THE BLACK PAPER

黑皮书

The *Principia* *of* SOVEREIGN DIGITAL INTEROPERABILITY

The Polycentric Framework for Sovereign-Verifiable Settlement Interface

主权间数字互操作元宪章

主权间可验证的多中心结算框架

VOLUME A:
Principles & Architecture
卷A：原则与架构

实现主权国家间　数字主权可验证协作的元宪章框架

The *Principia* framework for the verifiable interoperability of digital sovereignty between nations

theprincipia.org

Positioning *and* Reader's Guide
定位与导读

AUROPHOENIX

The course of human civilization reveals a consistent pattern: cooperative systems that endure among sovereign states by respecting independent boundaries while sustaining convergent action derive their force not from any single document.

This inherent resilience is grounded in a systemic examination initiated before the signing of any binding treaty. It is not limited to the shaping of strategic will by game theory, nor constrained by political trade-offs; it seeks the fundamental truth of First Principles: what are its first principles? Where are its boundaries and red lines? And most critically - how can cooperation be anchored as an engineering reality with verifiable determinacy, without requiring any party to cede sovereignty? These are questions about the underlying logic of order in an era of competing sovereign interests. They determine whether a system can remain resilient and hold to its rules under conditions of conflict.

At a moment when digital sovereignty is emerging and global cooperation is being restructured, **the Black Paper serves as a Principia framework for the verifiable collaboration of digital sovereignty between nations, providing the theoretical precursor and logical framework for the foundational work of polycentric sovereign digital interoperability.**

Transcending the divide between technical protocol and political initiative, the Principia stands as a profound synthesis of institutional design and engineering implementation.Inspired by the Bitcoin whitepaper, we take the logic of "enabling mutually distrustful entities to achieve reliable cooperation" and develop it into a verifiable architecture that serves polycentric sovereign collaboration. Its core mission is to address and rebuild the essential contradiction between "sovereign isolation" and "global interconnection": driving deep digital coordination among mutually distrustful states and institutions without requiring any party to relinquish independent sovereignty. To this end, we propose a dual-layer governance architecture. At the protocol base layer, algorithmic consensus ensures logical neutrality and global factual consistency; at the upper layer, each sovereign entity retains full autonomous authority over legal autonomy, data residency, and policy compliance.

人类文明的进程昭示着一个朴素的真理：凡能使主权国家互为独立边界、又成合流之势的协作体系，其生命力与契约性，从来不只依托于一纸文书的承诺。

这种生命力根植于盟约签署前的深层追问，它不止于利益博弈对参与意愿的塑造，也不囿于政治妥协的权宜之计，而是直抵第一性原理的本质：这套系统的逻辑根基是什么？它必须恪守的边界与红线在哪里？以及最核心的命题：如何在不让渡主权的前提下，将协作锚定为具备“可验证的确定性”的工程现实？这些追问，是在动荡的全球博弈中寻找秩序的底层逻辑，它决定了一个体系能否具有韧性，能否在无序的冲突中守住规则。

黑皮书诞生于数字主权觉醒与全球协作重构之际，作为服务于主权国家间实现数字主权可验证协作的“元宪章”框架，为多中心主权数字互操作这一奠基性工作提供的理论先导与逻辑框架。

元宪章既非纯粹的技术协议，亦非单纯的政治倡议，而是融合了“制度设计”与“工程实现”的深层综合体。受比特币白皮书启发，我们将“使互不信任的实体达成可靠协作”的逻辑，升维至一套服务多中心主权协作的可验证架构。其核心使命，是解构并重建“主权隔离”与“全球互联”的本质矛盾：在不要求任何一方让渡独立主权的前提下，驱动互不信任的国家与机构达成深度的数字协同。为此，我们提出构建一种“双层统一”的治理架构。在协议

As the logical starting point for this Polycentric Framework, **we focus on the settlement domain, demonstrating that settlement neutrality can be achieved not merely as a political stance but as a verifiable engineering reality**.

The Principia rests on three unshakable fundamental principles:

- National sovereignty above all: the absolute premise of system design and operation is to uphold that national law is higher than code logic.
- Independent and controllable technology: defending the strategic bottom line of "technical sovereignty" and digital territory is the physical guarantee for achieving sovereign continuity.
- Controlled interoperability: the "diplomatic norms" of sovereign states in digital space, ensuring cooperation is orderly, with clear rights and responsibilities, and controllable risks.

We hereby contribute to the world: Black Paper: The Principia of Sovereign Digital Interoperability.

Spanning cryptography, the operation of state power, monetary theory, and geopolitics, and integrating theoretical depth with engineering rigor, it provides the complete intellectual and architectural foundation from which future governance covenants among sovereign states can be derived - without reconstructing existing institutions, and without renegotiating first principles.

Sovereignty need not be ceded; cooperation is thus born.

Book Structure Guide:

- **Volume A (Principles and Architecture)**: establishes the architectural design principles, compliance mutual recognition, and governance logic that form the foundational framework of these Principia, providing the normative and conceptual basis for decision-makers and legal experts.
- **Volume B (Engineering and Compliance)**: provides directly citable technical standards and proof frameworks, for architects and auditors to implement and verify.

A Note on the Title

The English edition uses the title *Principia* - Latin for "first principles," known from Newton's *Principia Mathematica* (1687). This document does not constitute an agreement or charter between parties; it establishes the foundational principles and architectural constraints from which such agreements can later be derived.

The Chinese edition bears the title 元宪章 (yuán xiànzhāng). The term 宪章 appears in the Zhongyong (中庸), one of the Four Books of the Confucian canon,

底层，通过算法共识确保逻辑中立与全局事实一致；上层为各主权实体保留绝对的自治领地，以承载法律自主、数据留存与政策合规。

作为多中心协作的逻辑起点，**我们首先聚焦于结算领域，将“结算中立”从政治立场转化为可验证的工程现实**。

元宪章立足于三大不可动摇的根本原则：

- 国家主权至上：系统设计与运行的绝对前提，恪守国家法律高于代码逻辑。
- 技术自主可控：捍卫数字疆域的战略底线，是实现主权连续性的物理保障。
- 可控互操作：主权国家在数字空间的外交规范，确保协作有序、权责清晰、风险可控。

我们谨此向世界贡献：《黑皮书：主权间数字互操作元宪章》。

它横跨密码学、国家权力、货币理论与地缘政治，融合理论高度与工程纵深，为主权国家间衍生未来的治理盟约提供了完备的思想与架构基础，无需重构既有制度，无需重议基础原则。

主权无须让渡，协作自此而生。

本书结构指引：

- **卷 A（原则与架构）**：构成元宪章的架构设计原则、合规互认与治理哲学。为决策者与法律专家提供价值基石。
- **卷 B（工程与合规）**：提供可直接援引的技术标准与证明框架。供架构师与审计师实现与验证。

关于书名的说明

英文版定名为 *Principia* ，拉丁语意为“第一性原理”，因牛顿的《自然哲学的数学原理》（*Principia Mathematica*, 1687）而闻名。*Principia* 准确地界定了本文的本质：它并非各方间的具体协议，而是确立了后续契约据以衍生的底层原则与架构约束。

中文版定名为元宪章。“宪章”取《中庸》“宪章文武”之意，

where it means "to establish foundational constitutional norms from which all governance is derived." The prefix 元 (primordial, originary) amplifies this sense: the normative foundation that precedes all subsequent institutional order.

Principia and 元宪章 express the same concept within their respective traditions. The titles differ in language; their meaning is one.

Open-Source *and* Authorship Statement

This Principia does not originate under the authorization of any sovereign state or international organization, nor does it represent the position of any particular country or organization. Just as open protocols are jointly maintained by global nodes, these Principia are likewise open-sourced for all sovereign entities to use, critique, adapt, and co-build.

This Principia is written by Aurophoenix Technology. The founding intent of the project is to rebuild the cooperative order of the digital age through technology and rules: **The mission is to enable Global Settlement that is Neutral, Verifiable, and Beyond Unilateral Discretion. Making cross-border financial coordination sovereign-safe in a multipolar world.** The Principia proposes SSI (Sovereign Verifiable Settlement Interface) as its engineering specification, transforming abstract principles into a two-layer technical system of "intra-sovereign execution, globally co-verified". With the full support of the Aurophoenix Technology team, this vision has been realized in both theory and engineering implementation.

Special thanks are due to Yan Gu (Kyle Gu) and Stepan Soin, who played pivotal roles in two key domains - cross-domain compliance interoperability and sovereign-verifiable architecture design - driving the Principia's conceptual development and realization. Special thanks also to Yipin Liu for breakthroughs in engineering implementation, to Melida Mei for rigor in text review and compilation, to Yi Guo for support in research, and to Danting Li (Daisy Li) for craftsmanship in visual presentation and layout design.

Finally, with reverence and gratitude, I dedicate this work to my mother - whose quiet support through countless days and nights made possible the freedom to journey into the depths of thought.

We firmly believe that a nation's "digital frontier" should not be exclusively defined by any single power, but should be grounded in shared underlying logic and a verifiable order. May this work lay the foundation of a new cornerstone of digital civilization that is open and neutral.

AURO PHOENIX

Qinwen Wang
Founder of Aurophoenix Technology
June, 2026

指涉根本性的治理规范；前缀“元”强调其作为所有制度秩序之前的规范性基础。

Principia 与 元宪章 在各自的文化传统中表达了同一概念。其名虽异，其义为一。从第一性原理出发，向下贯穿并支撑起其上构建的万事万物。

开源与著作声明

元宪章不源自任何主权国或国际组织授权，亦不代表某一国家或组织的独立主张。正如开放协议由全球节点共同维护，本元宪章同样开源给所有主权实体取用、批判、化用与共建。

元宪章由珑凰科技独立撰写。立项初衷，是以技术与规则为数字时代的协作秩序重新奠基：**让主权国家间实现不受单边力量限制的可验证中立结算。让跨境金融协作在多极世界中实现主权安全。** 元宪章提出主权可验证结算框架（SSI）作为其工程规范，将抽象原则转化为“主权内执行，全球共验证”的双层技术体系。这一愿景在珑凰科技团队的全力支持下得以实现理论与工程的落地。

在此特别致谢：顾晏与 Stepan Soin，两位在“跨域合规互认”与“主权可验证架构”设计这两项关键命题上，为元宪章的创新与落地发挥了举足轻重的作用。感谢刘奕品在工程实现上的攻坚，梅静在文本审定与编译上的审慎，郭仪在调研方面的支持，以及李丹婷在视觉呈现与排版设计上的匠心。

最后，谨以此书献给我的母亲。感谢您在无数个日夜里的默默支持与理解，让我得以在思想的深处自由航行。

我们深信，国家的“数字边疆”不应由任何单一力量的排他性定义，而应奠基于共享的底层逻辑与可验证秩序。愿以此书，共同奠定一个开放、中立的数字文明基石。

科珑技凰

王琴文
珑凰科技创始人
丙午年甲午月

Sovereign-Verifiable Settlement
主权间可验证结算

Black Paper: The *Principia* of Sovereign Digital Interoperability

The Polycentric Framework for Sovereign-Verifiable Settlement Interface

黑皮书：主权间数字互操作元宪章

主权间可验证的多中心结算框架

Preface (序言)

Qinwen Wang / Founder of Aurophoenix
王琴文 / 珑凰科技创始人
qinwen@aurophoenix.com

The Peace of Westphalia[1] established the principles of territorial sovereignty and regulatory autonomy, thereby giving shape to the modern state system. By 1945, the Bretton Woods system had laid the institutional foundation for the postwar global economy. On this basis, world order evolved into a collaborative network anchored in unipolar credit. Through trade rules and cross-border settlement systems, this order enabled an exponential increase in efficiency. Sovereign states, in exchange for participation in the global division of labor, ceded part of their "regulatory autonomy". This cession was feasible because the rules at the time maintained a minimum baseline of neutrality: adherence to the rules did not imply submission to the will of any particular state. This efficiency-oriented arrangement sustained more than half a century of globalized prosperity.

However, as globalization entered a phase of zero-sum competition

1648 年《威斯特伐利亚和约》[1] 确立了领土主权与规制自主的原则，现代国家体系得以成型。及至 1944 年，布雷顿森林体系则为战后全球经济奠定了制度基调，在此基础上，世界秩序演化为一张以单极信用为支点的协作网络。通过经贸规则与跨境结算体系，这一秩序释放了指数级的效率跃迁。主权国家以让渡局部“规制自主权”为对价，换取进入全球分工体系的资格。这种让渡之所以可行，在于当时的规则仍维持着最低限度的中立底线：遵循规则，并不意味着服从特定国家的意志。这种以效率为导向的秩序安排，支撑了长达半个多世纪的全球化繁荣。

over existing gains, the technical and institutional system supported by unipolar credit was progressively drawn into geopolitical rivalry, transforming from an engine of efficiency into an instrument of sovereign competition. When rules lose neutrality, the cession of "regulatory autonomy" is no longer merely a cost of cooperation, but may evolve into institutional disarmament vis-à-vis a particular power. The resulting rise of "anti-globalization" is therefore not a rejection of cooperation per se, but an instinctive response by sovereign states to the risks of single-point dependency. The precondition for cooperation thus shifts from "technical reachability" to "political admissibility", and technology increasingly becomes subject to strategic instrumentalization. This transformation is particularly visible in settlement systems, where settlement authority no longer functions merely as infrastructure for value transfer, but increasingly as a gatekeeper of order. **Cross-border settlement is no longer a purely efficiency-driven problem, but has become a matter of systemic ordering with direct implications for a state's economic continuity**.

We have already entered what Ray Dalio describes as the sixth stage of the long-term cycle: rules themselves begin to be redefined by power, and "might defines principle" becomes the prevailing underlying condition of order[2]. Dalio identifies the fracture, but does not provide an institutional resolution. Beneath this fracture, digitization is emerging as the key variable reshaping the landscape. It equips multipolar actors with instruments of asymmetric competition, while simultaneously accelerating the loosening of the unipolar center. Yet multipolarity also introduces a new problem of order: the fragmentation of rules. Sovereignty entails the authority to define rules; mutual recognition of rules necessarily implies the partial delegation of that authority. When sovereign will is embedded into digital infrastructure, and cross-domain rule systems lack mutual recognition while standards diverge, global coordination faces structural fragmentation risks. This is not merely a technical problem, but a manifestation of sovereign divergence in digital space: technology can interconnect systems, but it cannot by itself reconcile divergent sovereign rule systems.

This tension is particularly evident in the evolution of settlement systems. At present, more than 130 jurisdictions are advancing the development of central bank digital currency (CBDC) systems, resulting in multiple heterogeneous technical architectures. Due to divergences in standards, governance boundaries, and compliance semantics, the global settlement network is transitioning from a single backbone structure toward a configuration characterized by regionalization, bilateral arrangements, and the coexistence of

然而，当全球化进入存量博弈阶段，单极信用所支撑的技术体系逐渐被裹挟进地缘政治竞争，从效率引擎变为主权博弈的筹码。当规则失去中立性，“规制自主权”的让渡不再是协作成本，而可能演变为向特定力量的制度性缴械。由此兴起的“反全球化”，并非对协作本身的否定，而是主权国家对“单一依赖风险”的本能防御。协作的前提随之从“技术可达”转变成“政治准入”，技术开始被武器化。在结算体系中这一变化尤为深刻：结算权，不再只是支撑价值流动的基础设施，逐渐演变为带有排他性的秩序入口。**跨境结算不再是单纯的效率问题，而成为关乎国家经济生存权的秩序裁决**。

我们已然步入 Ray Dalio 所言的大周期第六阶段：规则本身开始被力量重新定义，“强权即公理”成了唯一的秩序底色[2]。Dalio 揭示了裂痕，却并未给出制度答案。这道裂痕之下，数字化正成为重塑格局的关键变量。它为多极力量提供了非对称竞争的工具，也加速了单极中心的松动。但多极化同时带来了新的秩序难题：规则的离散化。主权即规则制定权，规则互认则意味着部分规则权的让渡。当主权意志被硬编码进数字基础设施时，跨域规则间缺乏互认、标准体系彼此分裂，全球协作便面临结构性碎片化风险。这非单纯的技术问题，而是主权在数字空间的正面交锋：技术足以连接系统，却无法自动弥合主权间的规则断裂。

这种张力在结算体系的演进中尤为突出。当前，全球已有 130 多个国家推进 CBDC 体系建设，并形成多种异构技术路径。由于标准体系、治理边界与合规语义各不相同，全球结算网络正由单一主干结构走向区域化、双边化乃至多网络并存的格局。这不仅带来冗余的对接与高昂的互操作成本，也在争议处置上形成法理空白。

multiple networks. This not only leads to redundant integration efforts and high interoperability costs, but also creates a jurisprudential vacuum in dispute resolution. Even where technical interoperability has been achieved (for example, mBridge[3]), differences in capital controls and compliance semantics across jurisdictions continue to constitute boundary conditions that cannot, at the current stage, be resolved through purely technical means.

The difficulty of technical approaches - such as those represented by cross-chain protocols - in addressing interoperability requirements among sovereign jurisdictions lies in the fundamental mismatch between their internal trust models and sovereign governance structures. "Protocol unification" often entails implicit rule delegation; and third-party cross-chain mechanisms, in essence, outsource verification and execution functions to off-chain coordinators, thereby reintroducing trust dependencies. In the context of crypto-assets, such designs may operate under conditions of homogeneous trust assumptions. However, once extended to sovereign coordination scenarios, a structural limitation becomes evident: no sovereign actor will entrust core settlement and compliance decision-making authority to an external entity that is not subject to its institutional framework. Because inherent mutual trust does not exist among sovereigns, any purely technical connectivity that attempts to bypass sovereign will will ultimately encounter the boundaries of trust and compliance. **This is the clearest expression of the tension between sovereign separation and global interconnection**.

From Efficiency to Order: The Constitutional Question of Settlement in the Digital Age

Before deriving technical pathways, it is necessary to clarify that what we face is not merely a problem of technical optimization, but a structural proposition of "technology–institution coupling". It is therefore necessary to return to the jurisprudential foundations of settlement systems. The Bank for International Settlements (BIS) defines settlement as "the legally irreversible transfer of funds and the final discharge of obligations[4]". This definition reveals a fact often obscured by technical abstraction: the finality of cross-border settlement is, in essence, a legal fact affirmed by sovereign authority, rather than merely a digital update of account states within information or DLT-based systems.

即便在技术层面实现接口互通（如mBridge[3]），跨法域间在资本管制与合规语义上的差异，仍构成当前阶段难以被纯技术路径消解的边界条件。

以跨链协议为代表的技术方案，之所以难以承载主权国家间的互操作需求，根源在于其内在的信任模型与主权治理结构间的本质错位。“协议统一”，往往意味着规则让渡；而“第三方跨链”机制，本质上是将验证与执行能力外包给链外协调者，形成信用的再嫁接。在加密资产语境中，这类设计或许可在同质信任环境下运行，但一旦进入主权协作场景，问题便随之显现：没有任何主权主体会将核心结算与合规裁量权托付不受其制度约束的外部。主权间缺少天然的互信，决定了任何试图绕过主权意志的纯技术连接，都终将触及信任与合规的边界。**这正是“主权隔离”与“全球互联“矛盾的必然显现**。

从效率到秩序：数字时代的结算宪制问题

在推演技术路径之前，必须首先理清，我们所面对的并非单纯的技术优化问题，而是一个“技术—制度耦合”的结构性命题。因此，有必要回归清算体系的法理基础。国际清算银行（BIS）将结算界定为“资金在法律上不可逆转的转移与债务的最终清偿”[4]。这一界定揭示了一个常被技术表象所遮蔽的事实，跨境清算的终局性，本质上是经主权意志确认的法律事实，而非仅仅是信息系统或分布式账本（DLT）中账目状态的数字更新。

然而，现行技术架构却使这一法律事实的确认过程，持续承受结构性摩擦。由发起行、多级代理行及收款行构成的多层级网络，在跨越时

Yet the current technical architecture causes the process of affirming this legal fact to bear persistent structural friction. The multi-layered network composed of the originating bank, multiple intermediary institutions, and the receiving bank faces a fundamental dilemma as it traverses time-zone differences, regulatory regimes, and heterogeneous ledger systems: from instruction issuance to finality, there exists no single participant capable of fully observing the real-time state of funds. The resulting "state invisibility" implies that the payer - and even participating institutions - can access only fragmented "partial truths". This condition does not arise from single-point failure, but from the fact that each participant operates within its own regulatory boundary and heterogeneous ledger environment. Information flow at the technical layer cannot be directly elevated into full-domain consensus at the jurisprudential layer.

This discontinuity of information further evolves into fragmentation of responsibility chains and redundancy in compliance validation. The release of a transaction depends on risk assessments independently performed by institutions along the transaction path under opaque conditions. In the absence of a pre-aligned proof structure, "compliance proofs" generated in different jurisdictions cannot be directly recognized across domains, forcing each node to conduct repetitive and inefficient validation. This phenomenon of "compliance islands" is not incidental, but an institutional consequence of unaligned regulatory frameworks across heterogeneous jurisdictions. Even where macro-level policy objectives converge, subtle divergences in threshold settings, sanctions regimes, and disclosure boundaries prevent compliance conclusions from being directly portable as cross-domain semantic units. Once disputes arise, facts must still be reconstructed through costly manual replay and narrative reconstruction rather than immediate formal verification.

However, when examining the three prevailing exploratory paths, it becomes evident that although each provides valuable partial solutions within a defined trust radius, all encounter structural limitations when addressing the challenge of "deep mutual trust" in a multipolar global environment.

- **The institutional-trust path centered on traditional intermediaries** benefits from mature governance structures and scalable operational capacity. However, under conditions of intensifying geopolitical tension, its neutrality relies more on temporary institutional equilibria than on structurally embedded constraints at the technical or protocol layer. Once external pressure is introduced, system

区差异、监管规则与异构账本体系的过程中，始终面临一个根本困境：从指令发出直至终局达成，系统中不存在任何一方能够完整掌握资金的实时状态。由此产生的“状态不可见性”，使付款人乃至参与银行都只能获得片段化的“局部真相”。这一问题并非源于单点失效，而是由于各参与方始终运行于各自独立的规制边界与异构账本之内，技术层面的信息流转，无法自然转化为法理层面的全域共识。

信息的不连续进一步演化为责任链条的断裂与合规审查的冗余。一笔交易的放行，沿途各机构在不透明条件下分别作出的风险判断。由于缺乏预先对齐的证明结构，不同法域生成的“合规证明”无法被跨域直接采信，导致各节点不得不进行重复且低效的审查。这种“合规孤岛”现象并非偶发，而是异构法域间规制差异无法对齐的制度性结果。 即便宏观政策目标趋同，但阈值设定、制裁名单及信息披露边界的细微差异，仍使合规结论难以作为可跨域携带的语义单元被直接采信。一旦争议发生，事实仍须通过高成本的人工复盘与叙事重构来还原，而非基于形式化逻辑的即时验证。

然而，审视既有主流的三条探索路径，尽管它们各自在特定的信任半径内提供了阶段性的宝贵解法，但在应对全球多极化格局下的“深层互信”挑战时，均触及了难以逾越的结构性边界。

- **以传统中介为核心的机构信任路径**，优势在于成熟的治理结构与规模化运行能力。然而，在地缘政治张力持续抬升的背景下，其中立性更多依赖制度博弈的暂时均衡，而非源于技术底层的结构性约束。一旦外部压力介入，系统稳定性便可能被迅速侵蚀，进而演化为网络分裂与信任断层。

stability may rapidly deteriorate, potentially resulting in network fragmentation and discontinuity of trust.

- **The decentralized path represented by Web3** achieves state consistency through algorithmic consensus and, in technical terms, approaches the ideal of "trust-minimized collaboration". However, its internal logic remains largely confined to determinacy within the system itself, lacking native mechanisms for embedding legal finality and sovereign discretion. This structural mismatch limits the ability of compliance conclusions to attain institutional recognition in cross-sovereign contexts, thereby constraining its applicability within real-world financial infrastructure.
- **The multilateral or bilateral agreement path** enables efficient coordination within a limited participant set, but its expansion depends on the continuous accumulation of bilateral or multilateral linkages. As the number of participants increases, coordination costs grow exponentially, while system complexity exhibits nonlinear escalation beyond critical thresholds. Because this path lacks an endogenous global coordination mechanism, it tends toward fragmentation into compliance islands and the structural discontinuity of wider cooperation.

Taken together, these three paths reveal, from different perspectives, the "impossible trinity" inherent in cross-border settlement systems: the difficulty of simultaneously achieving sovereignty, neutrality, and scalability. Yet the future digital order requires precisely the concurrent realization of all three dimensions, rather than compromise among them.

It therefore becomes clear that the challenge extends beyond technical interoperability; it constitutes a constitutional question of order reconstruction: **in a multipolar world, how can a digital order be constructed that neither depends on a single center of authority nor becomes susceptible to geopolitical instrumentalization?** Such an order must take sovereign independence as its premise, logical equality and minimal trust as its foundation, and ensure that all participants can achieve verifiable mutual recognition of cross-domain rules without ceding rule-making authority, while preserving security and collaborative capacity at the level of technological sovereignty.

What cross-sovereign collaboration fundamentally lacks is not additional channels of connectivity, but a mechanism capable of transforming "rule execution" into "globally re-verifiable facts ". The key lies in abstracting law and policy into executable and verifiable

- **以 Web3 为代表的去中心化路径**，则通过算法共识实现了状态一致性，在技术上逼近“无信任协作”的理想。然而，其内生逻辑仍主要停留在系统内部的确定性，对于法律终局性与主权裁量的嵌入缺乏原生接口。这种结构性错配，使得合规结论难以获得跨主权语境下的制度性承认，最终限制了其在现实金融基础设施中的外延能力。
- **多边或双边协议路径**，在特定参与范围内能够实现高效协同，但其扩展方式本质上依赖连接关系的不断叠加。随着参与节点增加，协作成本呈指数级上升，系统复杂性亦随之呈边际递增，并在规模临界点上触发非线性的跃升。由于该路径缺乏内生的全球协调机制，极易滑向碎片化的“合规孤岛”，进而导致全球协作在结构上走向碎片化。

上述三条路径，从不同侧面揭示了跨境结算体系中的“不可能三角”：关于主权、中立性与扩展性的“不可兼得”。而未来的数字秩序恰恰要求三者同时成立，而非在其中做出妥协性取舍。

由此可见，我们所面对的已远非技术互操作问题，而是指向秩序重构的宪制命题：**在多极化世界中，如何构建一种既不依附于单一权力中心，亦免于被地缘政治“武器化”的数字新秩序?** 这一秩序必须以主权独立为前提，以逻辑对等与最小信任为契约，确保各参与方在不让渡规则制定权的条件下，实现跨域规则的可验证互认，并依然能够获得技术主权层面的安全与协作能力。

跨主权协作真正匮乏的，并非更多的物理连接通道，而是一套能将“规则执行”转化为“全域可复验事实”的机制。其关键在于，将法规

programmatic constructs that, while accommodating divergence and disagreement, ensure that when disputes arise, logic remains traceable and deterministically replayable. Since "legal finality" cannot be directly transmitted across sovereign boundaries, the only viable path is to reconstruct it, through cryptographic and mathematical proofs, into a transparent logical representation that can traverse domains.

At this critical juncture, the BIS Project Mandala[5] and the Principia framework demonstrate a shared core insight: compliance mechanisms must shift from "ex post tracing" to "real-time verification". Mandala, by front-loading compliance decisions through codification, has demonstrated the engineering feasibility of this paradigm. Building upon these practical advances, the Principia framework extends the proposition into the domain of institutional design. Once pre-execution compliance ceases to be the primary constraint, a more fundamental question emerges: in a multipolar environment, on what basis can rules across sovereign systems be mutually recognized? Mandala remains anchored in existing credit structures and enhances execution efficiency through technical means. **Principia framework, by contrast, seeks to construct a sovereignty-neutral layer of logical verification, exploring a paradigm of mutual recognition among heterogeneous rule systems**.

This distinction ultimately reflects different engineering expressions of "neutrality". Mandala's neutrality is grounded in a high degree of alignment among participants around shared protocol standards, and its optimization target remains the execution pathway within existing governance frameworks. The Principia framework, by contrast, embeds neutrality into the verification structure itself through a principle of "logical equality", thereby reducing reliance on centralized coordinators and redefining the institutional foundation for mutual recognition among sovereign systems. These represent parallel explorations - "optimization of existing pathways" and "construction of a new paradigm", under different trust radii and governance configurations, rather than substitutes for one another.

From Institutional Trust to Verifiability: Reconstructing Order Through Settlement Neutrality

Proceeding from the logic developed above, we have systematically articulated the *Black Paper: Principia for Sovereign Digital Interoperability*. This is not merely an engineering blueprint, but a

与政策抽象为可执行、可验证的“程序化对象”，在容纳差异与分歧的同时，确保在争议发生时，逻辑依然具备可追溯、可重放的确定性。既然“法律终局性”无法跨越主权边界直接传递，唯一的可行路径，便是借助数学证明，将其重构为透明且可跨域携带的逻辑表达。

在这一关键转向上，国际清算银行（BIS）的 Project Mandala[5] 与元宪章体系呈现出一致的核心洞察：合规机制必须从“事后追溯”转向“实时验证”。Mandala 通过代码化将合规决策前置，验证了这一范式的工程可行性。元宪章体系在汲取 Mandala 实践成果的基础上，将命题进一步延伸至制度范式层面，当合规前置已不再构成约束，核心问题随之显现：在多极化格局中，不同主权体系间的规则何以互认？Mandala 仍立足既有信用结构，通过技术手段强化规则的执行效率；**而元宪章体系则尝试在多极化背景下，构建一个主权对等的逻辑验证层，探索异构规则间的互认范式**。

这种差异，本质上源于对“中立性”的不同工程表达。Mandala 的中立性建立在参与方对共同协议准则的高度对齐之上，其优化对象仍是既有治理体系中的执行路径。而元宪章体系则通过“逻辑对等”机制，将中立性内嵌于验证结构本身，从而削弱对中心化协调者的依赖，并重塑主权间规则互认的制度底座。这是在不同信任半径与治理格局下，“优化既有路径”与“探索新范式”两种路径的并行探索，而非彼此替代关系。

从制度信任到可验证：结算中立的秩序重构

沿上述逻辑展开，我们系统性地撰写了《黑皮书：主权数字互操作元宪章》。这不仅是一份

comprehensive reconstruction of a new order of neutral settlement in digital space at the critical juncture where governance and technology become deeply coupled. It translates the political consensus that "sovereignty is non-transferable" into a global interoperability paradigm that is executable, verifiable, and replayable. We define this system as the **Sovereign Settlement Interface (SSI)** - a sovereign-verifiable, polycentric settlement framework that enables cross-domain collaboration without requiring suprasovereign trust.

This framework reconstructs the traditional paradigm of institutional trust: settlement neutrality no longer depends on endorsement by centralized authority, but becomes endogenous to a verifiable structure. Its engineering expression is a dual-layer architecture of "execution within sovereignty, verification by all globally": a heterogeneous collaborative network composed of the Sovereign Compliance Execution Layer (SCEL) and the Sovereign Relay Hub (SRH).

The Sovereign Relay Hub (SRH) is designed as a public collaborative plane from which power has been structurally stripped in advance. It performs only the ordering, verification, and finality-confirmation functions required for cross-domain collaboration and never intervenes in the interpretation, discretion, or execution of sovereign rules.The SRH does not pursue the global unification of rules, nor does it presuppose political mutual trust or introduce any suprasovereign adjudicator; it provides only a set of independently verifiable collaborative procedures.Its trustworthiness derives not from external endorsement, but from strict functional boundaries: **it does not execute sanctions, interpret rules, hold assets, or exercise adjudicative authority**. These limits are fixed as Principia-level boundaries and reinforced in the protocol layer through a negative list, and supported by an auditable, rollback-capable governance pipeline with delayed effectiveness and rights of objection. Any attempt to overstep these bounds is intercepted and exposed simultaneously at both the institutional and protocol levels.Neutrality therefore depends neither on operator goodwill nor on sponsor assurances, and cannot be unilaterally redefined by the system's builders.

Corresponding to the neutrality of the SRH, **the Sovereign Compliance & Execution Layer (SCEL)**, as an execution system independently deployed within each sovereign domain, constitutes the concrete carrier of a "sovereign DLT" architecture under the premise of technological neutrality. Its core responsibility is to ensure that, at the instant each cross-border transaction is triggered, compliance adjudication under the domestic rule system is completed and

工程蓝图，更是在治理与技术深度耦合的临界地带，对数字空间中立结算新秩序的整体性重构。它将“主权不可让渡”的政治共识，转译为一套可执行、可验证、可重放的全球互操作范式。我们将这一体系定义为“**主权可验证结算框架 (SSI)**”：一个主权可验证的多中心结算框架，使跨域协作不再依赖于超主权的信任。

这一框架重构了传统的“制度信任”范式：结算中立性不再依赖于中心化权威的背书，而是转化为验证结构内生的确定性。其工程表达为“主权内执行，全球共验证”的双层架构：由主权合规执行层（SCEL）与主权中继枢纽（SRH）构成的异构协作网络。

主权中继枢纽（SRH）被设计为权力被预先剥离的公共协作平面，仅承担跨域协作的排序、验证与终局性确认，绝不介入任何主权规则的解释、裁量或执行。SRH 不追求规则的全球统一，不预设政治互信，不引入超主权裁决者，仅提供可被独立验证的协作程序。其可信性不源于外部授权，而源于严格的功能边界与可检验的自我约束：**不执行制裁、不解释规则、不持有资产、不承担裁决**。上述约束被固化为宪章级不可逆边界，并以负面清单形式嵌入协议层，辅以可审计、可回滚、带生效延迟与异议的治理流水线。任何试图越界的行为都会在制度与协议层同时被拦截并显性化。中立性不依赖运营者善意，也不依赖项目方承诺，即使建设者本身也无法单方面改变系统的权力边界。

与 SRH 的中立性相对应，**主权执行层（SCEL）**作为各主权域内自主部署的执行体系，以技术架构中立为前提，构成“主权区块链”的具体承载。其核心职责在于：确保每笔跨境交易在触发瞬间，即完成本国规则体系下的合规裁决，并将该裁决转化为可跨域验证的确定性结果。

transformed into a deterministic result that can be verified across domains.

This capability is jointly realized by three principal modules: **Policy-DSL**, which maps regulations into an executable formal rule language; **JPack**, which encapsulates rule sets into signable, versioned semantic snapshots, thereby providing alignable rule boundaries for cross-domain verification; and **PoPC**, which renders compliance adjudications as replay-verifiable proof objects by cryptographically binding the basis of execution, input digests, rule versions, and decision outcomes, so that any authorized party can perform deterministic replay verification under the same JPack rule snapshot. Acting together, these three modules abstract what was originally a rule-execution process endogenous to the sovereign domain into "proof primitives" that can be carried across domains, independently verified, and replayed.

The design of PoPC satisfies **the minimum conditions of an auditable closed loop**: source signatures anchor responsibility, transaction binding ties the conclusion to a specific event, controlled submission preserves proof integrity in transmission, and replay mechanisms allow independent reverification under the referenced rule snapshot. Accountability is thus embedded at the architectural level rather than supplied after the fact.

Its deeper paradigm shift lies here: **proof supersedes logs** as the basis of verification. Proof production is fully detached from discrete, non-replayable operational records and transformed into structured, versionable, replayable proof objects. Dispute resolution thereby undergoes a parallel shift: it no longer depends on retrieving fragmented logs across institutions or on subjective interpretation, but instead proceeds on the basis of uniformly generated, independently re-verifiable proof objects. This transforms the foundation of collaboration from "consistency of interpretation" to "consistency of verification".

This transformation strictly follows **the principle of minimal exposure**: along the default path, only the minimum information necessary for verification is disclosed - rule-version fingerprints, input-digest commitments, decision results, and their binding relationships. Sensitive raw data always remains within the sovereign domain and is only conditionally disclosed in a limited manner when disputes are triggered. In this way, the three principal modules jointly abstract the sovereign-internal rule-execution process into "proof primitives" that are verifiable, auditable, yet non-inspectable, externalizing verification capability while ensuring that data sovereignty does not spill beyond the boundary.

这一能力由三大模块协同实现：**Policy-DSL**：将法规映射为可执行的形式化规则语言；**JPack** 将规则集封装为可签名、可版本化的语义快照，为跨域验证提供可对齐的规则边界；**PoPC** 将合规裁决生成为可复验的证明对象，将执行依据、输入摘要、规则版本与决策结果进行加密绑定，使任意授权方均可在相同的 JPack 规则快照下进行确定性重放验证。三者共同作用，将原本内生于主权域内的规则执行过程，抽象为可跨域携带、可独立验证、可重放的“证明原语”。

PoPC 的设计原生满足**最小可审计闭环**的条件：源头签名锚定责任主体，事务绑定将结论与特定事件强关联，受控提交保障证明在传递过程中的完整性，而重放机制允许在引用的规则快照下进行独立复验。由此，问责因此被内嵌于架构层面，而非事后补丁式的补充。

其更深层的范式转变在于：**以证明替代日志，成为验证的基础**：证明生产从离散、不可复验的运维记录中彻底剥离，转化为结构化、可版本化、可重放的证明对象。争议处置亦由此完成范式迁移，不再依赖跨机构调取零散日志与主观解释，而是基于统一生成、可独立复验的证明事实展开，从而将协作基础由“解释一致”转化为“验证一致”。

这一转化严格遵循**最小暴露原则**：默认路径仅披露“验证所必需”的最小信息集合：规则版本指纹、输入摘要承诺、决策结果及其绑定关系；敏感原始数据始终留存于主权域内，仅在争议触发时通过条件化披露机制进行有限开放。由此，三大模块共同将主权内部的规则执行过程，抽象为可验证、可审计而不可窥探的“证明原语”，在确保数据主权不外溢的前提下，实现验证能力的外部化。

The SRH undertakes the coordinating function of **cross-domain compliance mutual recognition**. Through a unified cross-domain verification protocol, and without penetrating or intruding upon sovereign boundaries, it validates the consistency and completeness of the proof primitives submitted by each SCEL and reaches deterministic settlement consensus across heterogeneous ledgers. Verification takes place outside the boundary, while rules remain inside the boundary.

Under this structure, differences in rules no longer block cooperation; they become the condition for formal expression and independent verification. The credit fulcrum of collaboration shifts from identity and institutional endorsement to mathematics and proof structures. Cross-domain cooperation no longer depends primarily on ex post explanation and reconciliation, but generates deterministic, replay-verifiable proof at the point of occurrence.

However, the establishment of **cooperation depends not only on institutional completeness, but also on the sufficiency of real-world incentives**. What sovereign states seek is not merely the "preservation of capability", but also the "attainability of returns". In current cross-border settlement systems, repeated compliance work and manual reconciliation caused by semantic inconsistency constitute continuously accumulating institutional friction. Once "compliance has been executed" is transformed into a deterministic proof that can travel across domains, the liquidity previously trapped within bilateral bargaining structures is released. Settlement cycles are compressed, the marginal cost of compliance declines significantly, and network effects increase with broader participation, thereby generating cooperation dividends that are both measurable and perceptible.

The core of this architecture lies not in convergence of rule content, but in the establishment of a unified "proof grammar". Each sovereign entity may retain a fully heterogeneous rule system, but its cooperation interface must satisfy the minimum consistency constraints of being verifiable, auditable, and re-verifiable. Logical equality does not arise from institutional promises, but takes engineering transparency as its premise: the core implementations of SCEL and SRH are fully open source, the build process is reproducible, and at least two mutually independent open-source implementations exist. Verification tools can be independently obtained and run in lightweight form, so that even participants with limited technical capability can deterministically replay any proof without deploying the full system. Logical equality is thus anchored as a testable engineering fact, rather than as an unfalsifiable trust assumption.

SRH 承担**跨域合规互认**的协同职能，通过统一的跨域验证协议，在穿透、不侵入主权边界的前提下，对各 SCEL 提交的证明原语进行一致性与完备性校验，并在异构账本间达成确定性的结算共识。验证发生于边界之外，而规则始终保留于边界之内。

在此结构之下，规则差异不再构成协作阻碍，反而成为被形式化表达与独立验证的前提条件。协作的信用支点从“基于身份与制度背书的信任”，转向“基于数学与证明结构的信任”。跨域协同不再依赖事后解释与对账，而是在发生的同时即生成具备确定性的、可重放验证的证明。

然而，协作的成立不仅依赖制度完备，更取决于现实激励的充分性。**主权国家所追求的，并非单纯的“能力保全”，更需要“收益可得”**。当前跨境结算体系中，由语义不一致引发的重复合规与人工对账，构成了了持续累积的制度性摩擦。当“合规已执行”被转化为可跨域携带的确定性证明，原本沉淀于双边博弈结构中的流动性得以释放。结算周期被压缩、合规边际成本显著下降、网络效应随参与扩展而递增，进而形成可度量、可感知的协作红利。

这一架构的核心，不在于规则内容的趋同，而在于建立一套统一的“证明语法”。各主权体可以保留完全异质的规则体系，但其协作接口必须满足可验证、可审计、可复验的最低一致性约束。逻辑对等并非源自制度承诺，而以工程透明为前提：SCEL 与 SRH 核心实现完全开源，构建过程可复现，且至少具备两个相互独立的开源实现。验证工具可独立获取、轻量运行，使技术能力受限的参与方亦无需部署完整系统，即可对任何证明进行确定性重放。逻辑对等被锚定为可检验的工程事实，而非不可证伪的信任假设。

This unified grammar ultimately points toward a redefinition of settlement finality. In traditional models, the "completion" of ledger state and "completion" in legal terms have long remained separate, producing a grey fracture between technical confirmation and legal confirmation. By introducing **dual-track finality**, the Principia framework elevates the condition of completion from single-track ledger finality to **a conjunctive structure of ledger finality and policy finality**. Only when a transaction is irreversible on the sovereign-domain ledger, and its compliance execution can be independently verified, does it possess full legal finality. In this way, technical state and institutional effect become isomorphic, and the grey zone is structurally dissolved.

Yet what this framework seeks is not perfect unification at the level of rules, but the minimum cooperative order that can still hold amid continuing divergence. This principle is expressed through "sovereign continuity": even under extreme conditions, the system must preserve minimally viable cooperation and a complete chain of responsibility; it must remain degradable, reconstructable, and accountable. The reliability of infrastructure is not built on the idealized assumption of "never failing", but is rooted instead in the capacity to observe, trace, and repair failure - in other words, in institutionally endogenous resilience.

In this sense, "verification" becomes the minimum common denominator that connects heterogeneous sovereign rules, and also the foundational mechanism that sustains the operation of a polycentric order. **Rules may remain differentiated, but execution must be verifiable; sovereignty remains inviolable, and cooperation thereby becomes possible**.

On this basis, the Principia framework makes proof the common interface of cross-sovereign cooperation: independently verifiable at global scale, yet compatible with the protection of underlying sensitive data. In this way, the long-standing tension between sovereign separation and global interconnection is recast under a verifiable paradigm: difference no longer blocks cooperation, but becomes the condition for a shared order that can be tested rather than presumed.

这一统一语法最终指向对结算终局性的重新定义。在传统模体系，账本状态的“完成”与法律意义上的“完成”长期分离，形成技术确认与法律确认之间的灰色断层。元宪章通过引入**双轨终局性**，将完成条件从单一账本终局性，**提升为“账本终局性 ∧ 政策终局性”的合取结构**。唯有当交易在主权域内账本上不可逆转，且其合规执行可被独立验证时，方具备完整的法律终局性。由此，技术状态与制度效力实现同构，灰色地带被结构性消解。

然而，本框架所追求的并非规则层面的完美统一，而是在持续分歧中仍可成立的最低协作秩序。这一原则体现为“主权连续性”：系统在极端情境下仍需维持最小可用协作与完整责任链，可降级、可重建、可追责。基础设施的可靠性，不建立在“永不失误”的理想假设之上，而根植于即对失败的可观测、可追溯与可修复能力，即制度层面的内生韧性。

在此意义上，“验证”成为连接异构主权规则的最小公约数，亦是支撑多中心秩序运转的基础机制。**规则可以差异化存在，但执行必须具备可验证；主权不可侵犯，协作由此成立**。

基于这一逻辑，元宪章将“证明”锻造为跨主权协作的统一接口：它既能被全球范围独立验证，又无需暴露底层敏感数据。至此，“主权隔离”与“全球互联”之间的长期张力，在可验证范式之下获得结构性统一：差异不再阻断协作，反而成为可检验而非预设的共享秩序得以生成的条件。

Closing Reflection

Three centuries ago, the Peace of Westphalia emerged from the ruins of religious wars to demarcate the boundaries of physical territory. It exchanged exclusive sovereign governance for the

序言终章

300 年前《威斯特伐利亚和约》在宗教战争的废墟上划定物理领土的边界，以排他性的治理主权，换取了文明存续的起码和平。

foundational peace necessary for the survival of civilization.

Today, we stand at the historical intersection of digital sovereignty and multipolarity. The Principia framework seeks to establish the logical boundaries of digital sovereignty and interoperability. By employing a neutral verification architecture rooted in reciprocity, it reconstructs global collaboration within a multipolar order. It is a systemic response which is expressed through "verified trust" to the cracks in the global order revealed by Ray Dalio.

This framework is beholden to no single sovereign power; it belongs to all who safeguard their independence in the digital age and aspire to global collaboration. It is a spark ignited in this moment, destined to become a wildfire across a boundless horizon.

The journey is long; the dawn begins here.

今天，我们站在数字主权与多极化交汇的历史关口，元宪章体系则旨在确立数字主权与互操作的逻辑边界，以对等性的中立验证架构，重构多极秩序下的全球协作。这正是对 Ray Dalio 所揭示的秩序裂痕，给出的一份关于“验证信任”制度回答。

这一框架不依附于任何一个特定主权，属于所有在数字时代守护主权独立、并渴望与世界协作的参与者。它是一粒火种，点燃于此刻，期待在更广阔的天地间成燎原之势。

路很长，起点就在这里。

Table *of* Content
目录

Volume A: Principles & Architecture
卷 A：原则与架构

Volume B (Engineering and Compliance) : Forthcoming

卷 B（工程与合规）：后续发布

A0. Glossary *of* Original Terms in the Black Paper

A0. 黑皮书原创术语表

This document introduces several original concepts, abbreviations, and design principles that form the terminological foundation for all subsequent chapters. All terms are defined here in their canonical form.

元宪章引入若干原创概念、缩略语与设计原则，它们共同构成后续各章展开论述的术语基础。所有术语均在此作出规范定义，并以本节界定为准。

Architecture and Infrastructure Mechanisms

架构与基础设施机制

- **SSI - Sovereign Settlement Interface (Sovereign-Verifiable Settlement Interface).**

  A global settlement interoperability architecture composed of sovereign execution layers (SCELs) and a Sovereign Relay Hub (SRH). SSI is not a single ledger but a heterogeneous collaborative network in which each jurisdiction retains full policy autonomy while cross-border transactions are coordinated through standardized compliance proofs. Throughout this document, the terms "DLT" and "blockchain" are used interchangeably.

  Architectural composition of SSI:

  $SSI = SRH + SCEL_1 + SCEL_2 + ... + SCEL_n$

  SCEL = Sovereign Blockchain + { Policy-DSL, JPack, PoPC }

  A sovereign blockchain becomes a Sovereign Compliance & Execution Layer - and thereby gains the ability to interact with the SRH and participate in the SSI network - only when it implements the three compliance modules: Policy-DSL (rule execution), JPack (sovereign rule packages), and PoPC (compliance proof generation). Without these modules, a blockchain remains a domestic ledger with no standardized interface to the global settlement network.

- **主权可验证结算框架（主权结算层）- SSI**

  元宪章体系定义：由各主权执行层（SCEL）与主权中继枢纽（SRH）构成的全球结算互操作架构。SSI 并非单一账本，而是一个异构协作网络。在该网络中，各辖区保留完整的政策自主权，跨境交易则通过标准化的合规证明进行协同。在本元宪章体系中，“ 分布式账本技术（DLT）”与“ 区块链 ”为同义并可互换使用。

  SSI 的架构组成：

  $SSI = SRH + SCEL_1 + SCEL_2 + ... + SCEL_n$

  SCEL = 主权区块链 + { Policy-DSL, JPack, PoPC }

  一条主权区块链只有在实现了规则执行（ Policy-DSL）、辖区策略包（JPack）和合规证明生成（PoPC）这三个合规模块后，才能转变为主权合规与执行层（SCEL），从而获得与 SRH 交互并参与 SSI 网络的能力。若不具备这些模块，该区块链仅为本地账本，不具备接入全球结算网络的标准化接口。

- **SRH - Sovereign Relay Hub.**

  A globally coordinated, technically neutral infrastructure layer jointly governed by participating jurisdictions. The SRH orders cross-border transactions, deterministically re-verifies the compliance proofs (PoPC) attached to them, and anchors verification finality through BFT consensus. It operates under two foundational constraints: coordinate only, not adjudicate and verify proofs only, not interpret rules. The SRH does not custody funds, issue currency, or execute sanctions.

- **主权中继枢纽 - SRH**

  元宪章体系定义：由参与辖区共同治理、在技术上保持中立的全球协调型基础设施层。SRH 负责对跨境交易进行排序，对其附带的合规证明（PoPC）进行 确 定性再验证，并通过 BFT 共识锚定验证的终局性。其运行受两个底层约束的限制：仅协调，不裁决；仅验证证明，不解释规则。SRH 不托管资金、不发行货币，亦不执行制裁。

- **SCEL - Sovereign Compliance & Execution Layer.**

A distributed ledger instance autonomously controlled by a sovereign state or its authorized institutions, Its underlying technology selection is neutral (supporting all mainstream distributed ledger or centralized high-performance ledger technology stacks), and securely integrated with domestic core financial systems (RTGS, CSD, etc.). Each SCEL processes transactions under its own legal and regulatory framework, executes programmable compliance rules via Policy-DSL, and generates verifiable Proofs of Policy Compliance (PoPC). It serves as the sole standardized interface connecting a jurisdiction's domestic financial infrastructure with the global SSI network.

- **主权合规与执行层 - SCEL**

元宪章体系定义：由主权国家或其授权机构自主控制的一套分布式账本实例。其底层技术选型具备中立性（支持所有主流分布式账本或中心化高性能账本技术栈），并可与境内核心金融系统（如 RTGS、CSD 等）安全集成。各 SCEL 在其自身的法律监管框架下处理交易，通过 Policy-DSL 执行可编程合规规则，并生成可验证的政策合规证明（PoPC）。它是连接辖区国内金融基础设施与全球 SSI 网络的唯一标准接口。

- **RVM - Regulatory Virtual Machine.**

A dedicated compliance engine operating independently of the conventional state machine within each SCEL and within the SRH. It deterministically executes Policy-DSL logic against the referenced JPack version, producing replayable compliance outcomes. At the SRH, the RVM performs mirror verification - re-executing the originating SCEL's policy logic to confirm byte-identical results.

- **监管虚拟机 - RVM**

元宪章架构规范：部署于各 SCEL 与 SRH 内部的专用合规执行引擎，独立于传统状态机运行。它依据所引用的 JPack 版本，以 确 定性方式执行 Policy-DSL 逻辑，产出可重放的合规结果。在 SRH 中，RVM 负责执行镜像验证，即重新执行源 SCEL 的政策逻辑，以 确 认结果在字节级保持一致。

- **Audit & Observation Layer.**

An independent architectural tier composed of audit institutions, supervisory nodes, and research organizations. It does not access raw business data; instead, it independently replays transaction logic and verifies compliance execution using privacy-preserving proof summaries and cryptographic proofs (such as zero-knowledge proofs) provided by lower layers. Its core function is to provide objective, third-party assessment of system neutrality, continuity, and trustworthiness.

- **审计与观察层**

元宪章架构规范：由审计机构、监管节点及研究组织构成的独立架构层级。该层级不接触原始业务数据，而是依托下层提供的隐私保护型证明摘要与密码学证明（如零知识证明），独立重放交易逻辑并验证合规执行。其核心功能，是对系统的中立性、连续性与可信性提供客观的第三方评估。

- **Sovereign Boundary Interface.**

The external-facing gateway module of each SCEL, responsible for bidirectional communication between the sovereign execution domain and the Sovereign Relay Hub. On the outbound path, it packages the transaction intent, the PoPC, and the referenced policy version information into a standardized Transfer Package for submission to the SRH. On the inbound path, it receives Verified Transfer Packages from the SRH (at a receiving SCEL) and Outcome Receipts (at an originating SCEL). It also interfaces

- **主权边界接口**

元宪章架构规范：各 SCEL 对外的边界网关模块，负责主权执行域与 SRH 之间的双向通信。在出境路径上，它将交易意图、PoPC 及引用的策略版本信息封装为标准化的传输包提交至 SRH；在入境路径上，它负责接收来自 SRH 的已验证传输包（接收方 SCEL）或结果凭证（发起方 SCEL）。该接口还通过安全网关与国内核心金融系统（RTGS、CSD、商业银行账本）对接。主权边界接

internally with domestic core financial systems (RTGS, CSD, commercial bank ledgers) through secure gateways. The Sovereign Boundary Interface corresponds to the "Cross-Domain Gateway" described in the SCEL minimal component architecture, and is the sole standardized ingress and egress point for a jurisdiction's transactions entering and exiting the global SSI network.

口对应 SCEL 最小组件架构中的跨域网关，是辖区交易进出全球 SSI 网络的唯一标准出入口。

- **PoPC Archive.**

The immutable, append-only compliance record maintained by SRH validator nodes, in which every PoPC that has passed deterministic re-verification is permanently stored. The archive serves three functions: (1) it provides the evidentiary basis for the Global State Tree, linking each verified PoPC to its corresponding transaction record, verification receipt, and terminal outcome; (2) it enables retrospective replay - any authorized party with access to the archive and the referenced JPack version can independently re-execute the policy logic and verify the compliance claim, without access to raw business data; and (3) it supports the Audit & Observation Layer by supplying proof summaries and cryptographic commitments (event hashes, Merkle roots) for independent third-party attestation. The archive is distributed across SRH validator nodes; no single node holds exclusive custody, and the integrity of the archive is protected by the same BFT consensus mechanism that governs the SRH's verification operations.

- **PoPC 归档库**

元宪章架构规范：由 SRH 验证节点维护的不可篡改、仅限追加的合规记录库，凡通过 确 定性再验证的 PoPC 均永久存储于其中。该归档库具备三大功能：一是作为全球状态树提供证明基础，将 每 个已验证的 PoPC 与对应的交易记录、验证凭证及最终结果建立关联；二是支持事后重放，任何获授权的一方，只要能够访问归档库并取得所引用的 JPack 版本，即可在不接触原始业务数据的情况下，独立重放政策逻辑并验证合规主张；三是为审计与观察层提供证明摘要和密码学承诺（如事件哈希、Merkle 根），以支持独立第三方见证。该归档库分布式存储于 SRH 各验证节点之上，不存在单一节点的独占保管，其完整性受 BFT 共识机制保护。

- **Policy-DSL - Policy Domain-Specific Language.**

A formal, deterministic rule-expression protocol that translates complex regulatory requirements - such as AML/KYC, cross-border limits, the FATF Travel Rule, asset-class restrictions, and operating windows - into machine-executable, verifiable logical statements. Policy-DSL provides a jurisdiction-neutral semantic foundation; sovereign-specific content is expressed through JPack.

- **政策领域专用语言 - Policy-DSL**

元宪章协议标准：一种形式化、确 定性的规则表达协议。它将复杂的监管要求（如 AML/KYC、跨境限额、FATF 旅行规则、资产类别限制及运行窗口）转化为机器可执行、可验证的逻辑语句。Policy-DSL 提供的是跨辖区中立的语义基础；而各主权特有的监管内容则通过 JPack 表达。

- **Core-DSL - Core Domain-Specific Language.**

The minimalist base language underlying Policy-DSL, focused on cross-border settlement and foreign-exchange regulation semantics. Its primitives are designed for compatibility with major regulatory frameworks (EU AMLR, MAS PSA, U.S. BSA, SWIFT CBPR+) and for extensibility toward finer-grained compliance modeling.

- **核心领域专用语言 - Core-DSL**

元宪章协议标准：作为 Policy-DSL 底层基础的极简语言，聚焦于跨境结算与外汇监管语义。其原语设计既兼容主流监管框架（如欧盟 AMLR、新加坡 MAS PSA、美国 BSA、SWIFT CBPR+），也保留向更细粒度合规建模扩展的能力。

- **JPack - Jurisdiction Pack.**

  A versioned, digitally signed policy package published by a sovereign regulator or its authorized delegate. Each JPack contains executable rules written in Policy-DSL, parameter thresholds and reference lists, mappings to underlying legal provisions, and standard test vectors. JPacks are the mechanism through which sovereign regulatory intent is expressed in computationally verifiable form.

- **法规要件集 - JPack**

  元宪章协议标准：由主权监管机构或其授权代表发布的、带有版本号并经数字签名的政策包。每 个 JPack 都包含用 Policy-DSL 编写的可执行规则、参数阈值、参考清单、与底层法律条文的映射关系，以及标准测试向量。JPack 是将主权监管意志转化为可计算、可验证形式的核心机制。

- **PoPC - Proof of Policy Compliance.**

  A cryptographic credential generated by the SCEL during transaction processing. Each PoPC binds together the referenced JPack version (policy snapshot hash), an input data digest, the rule-execution trace, the compliance determination result (ALLOW / HOLD / REJECT), timestamps, and a digital signature. PoPC is designed for deterministic replay: any party with access to the referenced JPack can independently re-execute the policy logic and verify the claimed outcome.

- **政策合规证明 - PoPC**

  元宪章协议标准：由 SCEL 在交易处理过程中生成的密码学凭证。每份 PoPC 都会将引用的 JPack 版本（策略快照哈希）、输入数据摘要、规则执行轨迹、合规判定结果（允许 / 挂起 / 拒绝）、时间戳和数字签名绑定在一起。PoPC 按 确 定性重放原则设计：任何持有所引用 JPack 的一方，都可以独立重新执行政策逻辑，并验证其所声称的结果。

- **RFR – Regulatory Finality Representation.**

  A deterministic, publicly verifiable representation derived from the finalized global state of the SRH after a cross-border transaction has achieved dual finality.The RFR is not a protocol-layer receipt and does not constitute an additional settlement step. Instead, it is a standardized representation that can be independently generated and verified by any participant based solely on finalized on-chain data.It reflects, in a reproducible form ledger finality (transaction irreversibility), and Policy finality (completion of compliance verification as recorded in PoPC and global state). The RFR serves as a reconciliation, audit, and dispute-resolution reference artifact, without consuming protocol resources or altering consensus semantics.

- **合规终局记录 - RFR**

  元宪章协议标准：在跨境交易达到双重终局性后，基于 SRH 全局最终态所派生出的、具备 确 定性且可公开验证的标准化表示形式。RFR 不是协议层回执，也不构成额外的结算 步 骤；相反，它是一种标准化表征，任何参与方仅依据链上终局性的数据即可独立生成并验证。它以可复现的方式体现：其一，账本终局性（交易不可逆）；其二，政策终局性（PoPC 与全球状态所记录的合规验证已经完成）。RFR 作为对账、审计与争议解决的参考工件存在，不消耗协议资源，也不改变共识语义。

- **Settlement Receipt.**

  A signed credential emitted by the destination SCEL (SCEL-B) to the SRH after the inbound sovereign decision has been made. In the case of ACCEPT, it confirms that local settlement has been executed - assets have been transferred, ledger state updated, and accounting entries completed within domestic core systems. In the case of REJECT, it confirms the refusal and includes reason codes under the local policy framework. The Settlement Receipt

- **结算回执**

  元宪章协议标准：目标方 SCEL（SCEL-B）在作出入境主权决定之后，向 SRH 出具的签名凭证。若结果为接受，则 确 认其本地结算已经完成，即资产已转移、账本状态已更新，且境内核心系统中的会计分录已完成。若结果为拒绝，则 确 认其拒绝执行，并附带本地政策框架下的原因代码。结算回执以密码学方式绑定决策结果(接

cryptographically binds the decision outcome (ACCEPT or REJECT), the referenced PoPC identifier, a timestamp, and the SCEL-B's digital signature, providing the SRH with an authenticated signal to proceed to Global Outcome Finalization.

受或拒绝）、所引用的 PoPC 标识符、时间戳以及 SCEL-B 的数字签名，从而向 SRH 提供经过认证的信号，以进入全球结算最终 确 定。

- **Outcome Receipt.**

  A notification credential produced by the SRH after committing the terminal outcome to the Global State Tree. It is broadcast to the originating SCEL (SCEL-A), any registered audit subscribers, and the Audit & Observation Layer. The Outcome Receipt contains the terminal state (SETTLED, REJECTED, or EXPIRED), the global event hash, a reference to the archived PoPC identifier, and the SRH's verification receipt. It serves as the external-facing signal that Global Outcome Finalization is complete - informing all relevant parties of the transaction's final, irreversible status without requiring them to query the Global State Tree directly. Delivery to SCEL-A is optional per the architecture; delivery to audit subscribers is governed by Layer 4 access policies.

- **结果回执**

  元宪章协议标准：由 SRH 在将终局结果写入全球状态树后生成的通知型凭证。该凭证会广播至发起方 SCEL（SCEL-A）、已登记的审计订阅方以及审计与观察层。结果回执包含终局状态（已结算、已拒绝或已过期）、全局事件哈希、已归档 PoPC 标识符的引用，以及 SRH 的验证回执。它作为面向外部的完成信号，表明全球结算最终 确 定已经完成，相关方无需直接查询全球状态树，也能获知交易最终且不可逆的状态。按照架构设计，是否向 SCEL-A 送达是可选的；向审计订阅方送达则受第四层访问策略约束。

Design Principles

设计原则

- **Settlement Neutrality.**

  The principle that the underlying settlement protocol must not embed political bias. All policy decisions - market access, sanctions, compliance screening - are executed exclusively by sovereign jurisdictions within their SCELs. The settlement layer is responsible only for completing ledger updates and generating tamper-resistant proofs after transactions have passed each jurisdiction's compliance review. This principle corresponds to the institutional separation of the charter layer from the operations layer in the governance model.

- **结算中立性**

  元宪章治理准则：指底层结算协议本身不得嵌入政治偏向。所有政策性决定（市场准入、制裁执行、合规筛选）只能由各主权辖区在其各自的 SCEL 内完成。结算层只负责在交易通过各辖区合规审查之后，完成账本更新并生成抗篡改证明。该原则对应于治理模型中宪章层与运行层的制度分离。

- **Verifiable Sovereignty.**

  The condition in which a sovereign jurisdiction retains full authority over its domestic rules, execution logic, and legal settlement effects, while exposing only proof-based and replay-verifiable outputs for cross-domain coordination. Mutual recognizability is enhanced without transferring interpretive or governing authority to the shared layer.

- **可验证主权**

  元宪章治理定义：指主权管辖区在保留其国内规制、执行逻辑及法律结算效力的完整裁量权的同时，仅向跨域协作平面提供基于证明且可重放验证的输出结果。在不向共享层让渡解释权或治理权的前提下，实现跨域互认能力的结构性增强。

- **Sovereign Continuity.**

  The capacity of a sovereign domain to preserve domestic settlement, compliance execution, and proof generation under failure, disruption, sanctions, or conflict, while maintaining a recoverable path for cross-domain commitments. Once connectivity is restored, pending or emergency transactions can be reconciled, replayed, or backfilled in accordance with predefined procedures and preserved proof records.

- **主权连续性**

  元宪章治理准则：指主权域在面临系统失效、中断、制裁或冲突等极端情境时，仍能维持其境内结算、合规执行及证明生成的自主能力，并保留跨域协作承诺的可 恢复路径。待连接 恢 复后，待处理或应急交易可依据预设程序及留存的证明记录，完成对账、重放或补录。

- **Interpretive Continuity.**

  The requirement that historical rule application remain reproducible across version change by preserving pinned policy versions, stable execution semantics, and replay-verifiable proof records. Changes to rules, configurations, or participation environments must not render prior transactions uninterpretable in practice or unverifiable in audit.

- **解释连续性**

  元宪章设计原则：指通过保留固定的政策版本、稳定的执行语义及可重放验证的证明记录，确 保历史规则的应用在版本更迭中始终可被还原。规则、配置或参与环境的变更，在实践中不得导致既往交易变得不可解释，或在审计中变得不可验证。

- **Dual Finality.**

  The constraint that every completed cross-border settlement must satisfy two independent conditions: ledger finality (the transaction is irreversibly recorded) and policy finality (the transaction has been executed in accordance with the rules in force across the relevant jurisdictions, with a complete proof chain available for verification).

- **双重终局性**

  元宪章设计原则：指任何已完成的跨境结算，都必须同时满足两个相互独立的条件：其一，账本终局性，即交易已经被不可逆地记录；其二，政策终局性，即交易已经依照相关辖区当时生效的规则完成执行，并具备可供验证的完整证明链。

CHAPTER A1.

The Ledger *of* Civilization:

Five Thousand Years of Accounting Authority and Its Future

A1. 章节

文明的账本：

记账权五千年的演进与未来

Abstract:

Throughout history, societies have sought increasingly reliable and efficient ways to record and transfer one of the most fundamental social contracts: credit.

The carriers of accounting authority have shifted alongside centers of power, moving from priestly clay tablets backed by sacred authority, to monarchic currencies anchored in gold, to private credit networks operated by banks, and eventually to state-issued fiat money.

Today, a historical inflection point is emerging. Accounting authority is becoming detached from physical media, with credit reconstructed through mathematics. Bitcoin removed accounting authority from direct sovereign control and placed it under algorithmic consensus. This experiment demonstrated technical feasibility while also reaching the limits imposed by sovereignty.

This development reveals a central dilemma of the digital era: whether a choice must be made between sovereign control and network neutrality.

Historical experience suggests a different approach. Over more than five thousand years, accounting systems that have endured and scaled successfully have consistently introduced some form of separation and mutual constraint between the exercise of power and the verification of facts.

This paper proposes a third path for global settlement: the construction of a verifiable global Sovereign Settlement Interface, one that preserves absolute sovereign control while shifting fragile relational trust toward stable mathematical verification.

The trajectory of civilization can thus be understood as the evolution of accounting authority.

（本章摘要）

人类始终在寻找一种更可信、高效的方式，来记录和转移最根本的社会契约：信用。

记账权的载体随权力中心而迁移：从祭司的神权泥板，到君主制的金权货币，再到银行家的私人信用网络，最终演化为国家的政权法币。

如今，我们正站在一个新的历史拐点之上：记账权脱离物理载体，在数学中重构信用。比特币首次将记账权从主权中抽离，交由算法共识运行。这场实验验证了技术的可能也触达了主权的边界。

这揭示了数字时代的核心困境：我们是否只能在“主权控制”与“网络中立”间二选一?

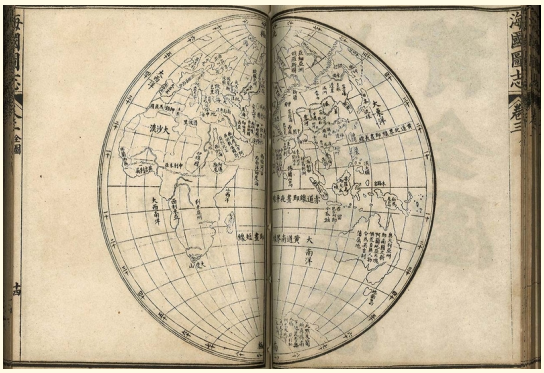
历史给出的答案，是将“权力的行使”与“事实的验证”分离，并让二者彼此制衡。

本文将循着五千年的演进轨迹，提出全球结算第三条道路：构建一个可验证的全球“主权协同结算层”。在保持主权绝对控制的前提下，我们试图将脆弱的关系“信任”，转向坚实的数学“验证”。

文明的进程，是一部“记账权”的演进史。

Accounting Relationships Backed by Sacred Authority

由神权背书的记账关系



IIlustrated treatise on the Maritime Kingdoms, 1902, Wei Yuan

"The fundamental logic is defined by its transparency;
the universal infrastructure is empowered by its simplicity."

"乾以易知，坤以简能。"

— I Ching, Xici (《易经·系辞》)

At the beginning of the 20th century, a discovery by a German archaeological team at the ruins of the Eanna Temple in Mesopotamia, revealed how large-scale human cooperation beyond kinship first became possible[1].

One Sumerian clay tablet, catalogued as W 19408,76[2], bears a line of plain text:

"*The farmer Ur-Lama received 2 gur of barley (approximately 600 liters) from the temple granary as seed for cultivating the field of the Sun God. It is to be repaid at harvest.*"

This record constitutes one of the earliest known formal loan contracts in human history, measured in standardized barley and collateralized by future harvests. The authority that gave this contract binding force was the temple itself.

At that time, Sumerian temples already functioned as both ritual and financial centers. As institutions of sacred authority, they maintained central ledgers that transformed interpersonal trust

20 世纪初，在美索不达米亚（今伊拉克）的埃安娜神庙遗址，一支德国考古队的意外发现，揭开了人类能超越血缘大规模协作的秘密 [1]。

这块编号为 W 19408,76 泥板 [2] 刻着一行朴拙的文字：

"*农夫乌尔 - 拉马，从神庙粮仓收到 2 古尔大麦（约 600 升），作为耕种‘太阳神’田地的种子。应在收获季归还。*"

这不是神庙的恩赐，而是一笔生意。这也是人类最早的"正规借贷合同"，以标准大麦为度量，以未来收成为抵押。而赋予这份合同效力的，正是神庙。

彼时的苏美尔神庙，已兼具祭祀与金融中心的

into written, enforceable debt relations backed by divine sanction. The clay tablet thus became the first theocratic accounting database in human history.

As David Graeber observes in Debt: The First 5,000 Years[3], systems of credit and debt were already in operation long before the emergence of money.

职能，作为神权中心创立的中央账本，将原本虚无缥缈的“信任”，转变为由神权背书且必须执行的“债务”关系。那块泥板，由此成为人类历史的第一个神权记账数据库。

正如大卫·格雷伯在《债：第一个 5000 年》[3]中所揭示：货币诞生之前，“信用与债务”体系早已运转。

From Imperial Gold to Credit Revolution

As ancient empires expanded, religious authority alone could no longer sustain the scale and complexity of finance. **Accounting power gradually shifted from temples to palaces**. This transition was formalized in the 7th century BCE, when the Kingdom of Lydia in Asia Minor minted gold coins bearing royal emblems of a lion's head[4], binding credit to precious metal under imperial authority. Gold-based accounting subsequently spread across Eurasia. It extended eastward to Persia and westward to Greece, was further disseminated through Alexander's campaigns, circulated within Roman trade infrastructures, and later connected with the Silk Road of Han China. Gold accompanied conquest, trade, and empire-building, and establishing a durable, transregional monetary standard.

Over time, however, the growth of long-distance commerce exposed the limitations of bullion-based settlement. Transporting gold and silver was costly, insecure, and inefficient. In response, **a credit revolution emerged in which accounting authority diffused from sovereigns into private commercial networks**. From the 8th to 10th centuries, the Eurasian continent witnessed a synchronized evolution toward lightweight ledger civilizations. While Tang China pioneered “Feiqian” (Flying Money)[33], Islamic traders employed the Suftaja[34] (the precursor to the modern “Check”) to enable remote settlements from Baghdad to Guangzhou. Functioning as the super-intermediaries of the Silk Road, these Islamic networks transformed cities like Baghdad and Samarkand into global clearing hubs, driving the cross-border flow of not only capital, but also transformative technologies like the compass and papermaking.

从帝国金权到私人信用的扩张

随着古代帝国的扩张，仅靠宗教权威已无法支撑帝国金融的规模与复杂程度。**记账权，随之由神庙移交宫廷**。公元前 7 世纪，小亚细亚的吕底亚王国铸造了印有狮头徽记的金币[4]，首次将“王权信用”与“贵金属”绑定。此后，以黄金为基础的记账体系遍及欧亚大陆，东至波斯，西达希腊，贯穿亚历山大的征途、罗马的商路与汉代的丝绸之路。黄金伴随着征服、贸易和帝国扩张，建立起了一套持久的、跨区域的货币标准。

然而，长途贸易的日益增长逐渐暴露了基于金银实物的结算体系的局限性：黄金和白银的运输成本高昂、安全无保障且效率低下。这倒逼出一场“信用革命”。8 至 10 世纪，亚欧大陆东西两端几乎同时演化出“轻量化”的记账文明：唐代中国出现了名为“飞钱”的汇兑券[33]，而伊斯兰商人则通过 Suftaja[34]（现代“Check”的词源）实现从巴格达至广州的异地支取。丝绸之路上的伊斯兰网络充当了东西方的“超级中介”，贸易催生了巴格达、开罗、撒马尔罕等全球清算中心，并传播了造纸术、罗盘等关键技术。

The 11th-century Mediterranean notarial system severed the link between transaction facts and physical exchange. It institutionalized the logic of "Contractual Primacy," allowing credit to break free from material constraints and circulate independently[35]. By the late medieval period, institutions such as the Medici banking network enabled merchants to settle cross-border obligations through bills of exchange rather than physical metal, while parallel innovations in China, the Shanxi-based Rishengchang Draft Bank introduced a system of Chinese-character codes as an anti-counterfeiting measure that ensured the security of redemption[5]. Wealth could now move through accounting entries rather than caravans.

The efficiency of private credit networks soon drew sovereign interest. Beginning in the early modern period, European states granted royal charters to institutions such as the East India Company, integrating private finance into imperial strategy. This moment represented the first large-scale incorporation of credit systems into state governance, as credit mechanisms moved from privately administered networks to institutionally regulated structures within the state apparatus.

记账权开始从王权向商业网络扩散。11 世纪的地中海公证人制度，将交易事实从物理交付中剥离，确立了"契约优先"的法理逻辑，使信用得以独立流转 [35]。到中世纪晚期，以美第奇银行网络为代表的机构，能够让商人仅凭一纸汇票，而非实物贵金属完成异地结算。与此同时，山西日升昌票号更进一步，以一套汉字密码防伪体系，为兑付安全提供保障 [5]。至此，财富的流动摆脱了金属实体的束缚。

私人信用网络展现的强大资源组织能力，迅速引来了主权的目光。自近代早期，欧洲君主通过颁布"特许状"，将东印度公司等机构转化为"准国家实体"。 这是信用体系从"私人网络"向"国家机器"第一次的系统性整合。

From Free Banking to Central Authority: The Consolidation of Monetary Power

From the 18th to the 19th century, the Industrial Revolution gave rise to the era of free banking[6], during which the authority to issue money was widely dispersed. Banks of all kinds issued their own private banknotes, and private banking, most notably exemplified by the Rothschild family[7],reached its historic peak, financing wars and large-scale trade throughout Europe.

Yet this highly decentralized monetary system lacked a unified clearing foundation. It could neither guarantee consistent value across notes issued by different banks nor withstand systemic bank runs. Recurrent banking panics exposed its fundamental limitation: private money was incapable of sustaining the unified economic space required by emerging modern nation-states.

从自由银行到中央权威：货币权力的集中

18 至 19 世纪，工业革命催生了 " 自由银行时代 " [6]。货币发行权被高度分散，各类银行发行私人银行票据。以罗斯柴尔德家族 [7] 为首的跨国金融巨头，通过为战争融资，将私人商业影响力推向了历史顶峰。

然而，这种高度分散的体系缺乏统一的清算底座，既无法保证每家银行币值的一致性，更无力应对系统性挤兑。接连不断的银行恐慌证明，私人货币无法承载现代民族国家的统一经济。

History therefore took a decisive turn. **Sovereign countries reclaimed the authority to issue currency, and central banking institutions were established**. The Bank of England, founded in 1694 under a government charter granting monopoly rights over currency issuance, emerged as the prototype of the modern central bank[8].With this development, accounting authority was gradually transferred from the private sector to public control.

This evolution culminated in the creation of the Federal Reserve in 1913[9]. Beyond unifying currency issuance, the Federal Reserve built a nationwide clearing system and assumed responsibility for managing national credit. The Great Depression of 1929 definitively shattered the belief in self-regulating markets, while Keynesian economics and the New Deal[10]affirmed the necessity of state intervention through fiscal and monetary policy.

By this stage, the central bank had evolved from a passive clearing institution into an active regulator of the volume and direction of money within the economy. The state thus assumed its role as the ultimate stabilizer of the macroeconomic system.

历史因此迎来决定性转折。**主权国家最终收回货币发行权，中央银行制度随之确立**。1694年，凭政府特许状获得垄断发币权的英格兰银行，成为中央银行的雏形 [8]，将记账权从私人部门收归公共权威。

现代中央银行制度的确立，则以 1913 年美联储的成立为标志 [9]。除了统一货币发行，美联储更构建了全国性的清算体系，并开始承担管理国家信用的职能。1929 年大萧条宣告了“市场万能”的破产，随之兴起的凯恩斯主义与罗斯福新政 [10]，确立了国家通过财政与货币手段干预经济的必然性。

至此，央行的角色发生了质变：从被动的支付清算中心，转变成调控全社会货币总量与流向的“总阀门”。国家作为宏观经济最终稳定器的地位，就此确立。

War, Reconstruction of the Global Monetary System, Sovereign Credit, and the Petrodollar-Centered Order

两次世界大战、全球货币体系重构主权信用与石油美元中心的秩序建立

The two World Wars marked a decisive rupture in the global monetary system, precipitating the collapse of the classical gold standard. Belligerent states compelled the surrender of gold and financed total war by issuing debt against future tax revenues, demonstrating that sovereign credit, rather than precious metal - had become the ultimate instrument for mobilizing economic resources.

两次世界大战导致古典金本位制崩溃。参战国强制征收黄金。政府通过发行战争债券将未来税收变现，以国家信用进行前所未有的资源动员。

1944 年布雷顿森林体系 [11] 将这一转变正式制度化：它确立了以美元为核心的金汇兑本位制。

In 1944, the Bretton Woods system[11] formalized this shift by establishing a hierarchical framework in which the US dollar was pegged to gold, while other currencies were pegged to the dollar. The dollar thus became the central unit of global accounting and settlement. As countries accumulated dollar reserves to stabilize their exchange rates, they effectively recycled global savings into US Treasury securities, making US sovereign debt the foundational asset underlying international liquidity.

This system, however, contained a structural contradiction known as the Triffin Dilemma[12]. Sustaining global growth required an expanding supply of dollar reserves, which compelled the United States to run persistent deficits and export dollars abroad. Over time, this dynamic eroded confidence in the dollar's gold convertibility. In 1971, the United States suspended convertibility in what became known as the Nixon Shock[13], bringing the Bretton Woods system to an end and inaugurating the era of floating exchange rates. Currency values thereafter rested primarily on market assessments of sovereign credit and policy credibility.

Following the exit from gold, the dollar continued to function as the core global currency, now supported entirely by credit. After the oil crisis of 1974, a new circulation mechanism emerged in which oil exports were priced and settled in dollars, and surplus revenues were reinvested in US financial markets. This arrangement, adopted broadly across OPEC economies, reinforced the dollar's central role under the floating exchange rate regime.

Through these transformations, the global accounting system entered a new phase: international liquidity, trade settlement, and financial stability became closely aligned with the sovereign credit of a single state. The postwar monetary order thus evolved from gold-backed money to a system anchored in sovereign balance sheets and geopolitical power.

美元与黄金挂钩，其他货币则与美元挂钩。至此，美元成为全球核心记账与清算单位，各国为维持汇率而储备美元（即购买美债），使得美债成为全球流动性的底层资产。

然而，这个体系内有个内在矛盾，即“特里芬难题”[12]：世界经济增长需要越来越多的美元作为储备，这就迫使美国必须长期保持国际收支逆差，长期向全球输出美元；这会持续损耗美国的黄金储备，最终使其无法兑现“美元固定兑换黄金”的核心承诺。1971 年，美国政府宣布美元与黄金脱钩，这一被称为“尼克松冲击”[13] 的事件，标志着布雷顿森林体系的瓦解。自此，主要货币的价值基准，不再由国际协议锁定，而主要取决于市场对发行国主权信用、经济实力与政策可信度的评估。

与黄金脱钩后，美元成为一种纯粹的信用货币。要继续担当全球主要记账单位，美元需要找到一个能够有效支撑其国际信用的新支柱。1974 年石油危机后，新的循环机制应运而生：石油出口以美元计价与结算，盈余收入再投资于美国金融市场。这一模式随后扩展至整个石油输出国组织（OPEC），在浮动汇率制度下进一步巩固了美元的中心地位。

历经这些变革，全球记账体系进入了新阶段：国际流动性供给、跨境贸易结算乃至金融体系稳定、单一国家的主权信用形成深度嵌套。战后货币秩序从黄金背书的传统体系，演变为以主权资产负债表和地缘政治实力为锚的新格局。

Global Clearing Networks: From Technical Channels to Strategic Infrastructure

全球清算网络：从技术通道到战略基础设施

As the petrodollar system solidified, Japan expanded its capital presence in the 1980s, and China joined the WTO in the early twenty-first century, the scale and complexity of cross-border capital flows grew exponentially. The global financial system faced a fundamental challenge: how could bank ledgers distributed across different countries and legal jurisdictions be updated safely and efficiently?

In 1973, cooperation among banking institutions in Europe and North America led to the establishment of SWIFT[14] as a replacement for inefficient telegraph-based communication. Owing to its deep integration with dollar clearing cores such as CHIPS, this infrastructure substantially improved global financial efficiency over the past half century. At the same time, its underlying logic of centralized verification meant that its operation was inevitably influenced by the legal frameworks of the jurisdictions in which core nodes are located.

As globalization entered a phase characterized by multipolar sovereign cooperation, the structural limitations of this architecture became increasingly visible.

- **Mismatch between public function and localized jurisdiction**: When an infrastructure operates as a global public utility, governance boundaries aligned with a single sovereign legal system generate friction in cross-border coordination.
- **Absence of verifiable neutrality**: Under centralized ledger models, neutrality is typically sustained through managerial commitments rather than through technically enforced, tamper-resistant constraints.

These tensions do not arise from the intentions of any specific institution. They reflect endogenous challenges faced by legacy clearing paradigms in an era defined by digital sovereignty. Whether in Europe's TARGET[15]system or China's CIPS[16], current sovereign initiatives can be understood as efforts to identify clearing paths that are more resilient and better aligned with a multipolar environment.

As the demand for credible cooperation increasingly exceeds reliance on centralized authority, the evolution of financial infrastructure enters a new phase. The question becomes whether a ledger paradigm can be constructed that is self-verifying in logic, sovereignly symmetrical in participation, and not dependent on the credit guarantees of any single entity.

随着石油美元体系的固化、日本在 1980 年代的资本扩张，以及中国在 21 世纪初加入 WTO，跨国资金流动的规模与复杂度呈指数级增长。金融体系面临一个根本性挑战：分布在全球各国、受不同法律管辖的银行，它们的账本如何才能安全、高效地同步更新?

1973 年，为取代效率低下的电报，欧洲和北美银行界合作组建了 SWIFT[14]。由于 SWIFT 与美元清算核心 CHIPS 的深度绑定，这套体系在过去半个世纪极大提升了全球金融效率，但其中心化验证的本质逻辑，使得基础设施在运行过程中不可避免地受到核心节点司法辖区法律的影响。

当全球化进入“多极主权协作”的新阶段，这种架构的逻辑缺陷开始显现：

- **公共性与局部管辖的错配**：当基础设施作为全球公共产品运行时，它的治理边界如果和单一主权法律重合，客观上会产生跨境治理的摩擦成本。
- **中立性验证的缺失**：在中心化账本模式下，中立性往往依赖于管理者的信用承诺，而非技术层面的不可篡改约束。

这种矛盾并非源于特定机构的主观意愿，而是旧有清算范式在数字主权时代面临的内生挑战。无论是欧洲的 TARGET[15] 还是中国的 CIPS[16]，各主权经济体的积极探索本质上都是在寻求一种更具韧性、更符合多极化现实的清算路径。

当全球对“可信协作”的需求超越了对“中心化权威”的传统依赖，金融基础设施的演进正式开启了下半场：我们能否构建一个逻辑自证、主权对等、且不依赖单一实体信用担保的新型账本范式?

Bitcoin: A Social Experiment in Verifiable Accounting

On January 3, 2009, Satoshi Nakamoto embedded the headline "Chancellor on brink of second bailout for banks"[17-19] into Bitcoin's genesis block, creating a permanent digital timestamp of the systemic financial crisis. This act symbolized a shift in trust from sovereign institutions to a system of cryptographic verification performed collectively by a network of nodes.

Bitcoin Block 0

Mined on January 04, 2009 02:15:05 • All Blocks

Satoshi | Notable Block

Coinbase Message • EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Bitcoin Genesis

On January 3rd 2009, the Bitcoin network was created when Satoshi Nakamato (the project's mysterious creator) mined the "Genesis" block. The 50 bitcoin coinbase reward is unredeemable, as it was omitted from the transaction database. This means any attempt to spend it would be rejected by the network. Whether this was intentional or not still remains unknown.
Read More

Details

Hash	00000-ce26f	Depth	934,091
Capacity	0.03%	Size	285
Distance	17y 0m 24d 20h 27m 47s	Version	0×1
BTC	0.0000	Merkle Root	4a-3b
Value	$0.00	Difficulty	1.00
Value Today	$0.00	Nonce	2,083,236,893
Average Value	0.00000000000 BTC	Bits	486,604,799
Median Value	50.00000000 BTC	Weight	1,140 WU
Input Value	0.00 BTC	Minted	50.00 BTC
Output Value	50.00 BTC	Reward	50.00000000 BTC
Transactions	1	Mined on	2009年1月04日 02:15:05
Witness Tx's	0	Height	0
Inputs	1	Confirmations	934,091
Outputs	1	Fee Range	∞-0 sat/vByte
Fees	0.00000000 BTC	Average Fee	0.00000000
Fees Kb	0.0000000 BTC	Median Fee	0.00000000
Fees kWU	0.0000000 BTC	Miner	Satoshi

Figure 1: Bitcoin block 1 info. Source: blockchain.com

In the digital age, Bitcoin addressed a longstanding problem in human cooperation: **how trust can be reliably established among strangers beyond the constraints of kinship, territory, and centralized authority**.

With the emergence of digitally mediated systems, this design renewed a central question in the history of human cooperation: how reliable TRUST can be established among strangers beyond the boundaries of kinship and territory? After the 2008 financial crisis[20], this question gained urgency, especially whether trust could be achieved without permission or reliance on a central intermediary[21].

Satoshi Nakamoto's response was an open-source, programmable protocol, later called blockchain, that reframed large-scale cooperation as two technical challenges solvable through cryptography and consensus.

比特币：一种可验证记账范式的社会实验

2009 年 1 月 3 日，中本聪在比特币创世区块中刻下当日《泰晤士报》的头条标题："财政大臣濒临第二轮银行纾困"[17-19]。这行铭文，为旧金融体系的危机盖上了不可磨灭的数字时间戳。比特币白皮书中所勾勒的技术范式，将信任，从对"主权信用"的被动依赖，重构为一项由全网节点主动执行的密码学验证工程。

在数字时空里，这一设计回应了贯穿整部人类协作史的终极问题：**超越血缘与地域的陌生人之间，如何建立可靠的信任?**

而在 2008 年全球金融危机[20]的废墟之上，历史为这个追问加上了属于数字时代的苛刻注脚：这种信任的建立，能否彻底摆脱中央权威，并向所有人"无需许可"地开放与验证[21]？

中本聪的答案，是一套可编程的开源协议，之后它被定义为区块链技术。他将宏大的人类协作命题，拆解成两个必须用数学验证与共识机制解决的工程挑战：

- **价值独特性的难题**（"双花问题"）[21]：在物理世界，一枚金币不能同时出现在两个地方。但在数字世界，复制信息易如反掌。如何让一串代码像金币一样，具有排他的、唯一的归属权?这是任何可信交易的根本前提。
- **全局事实一致性的难题**（"拜占庭将军问题"）[17]：当全球协作在陌生人间展开，谁有资格说了算?即使有人记账，又如何确保所有人看到的是同一版本，而无需一个最终的裁决机构来定夺?这

The first concerned the uniqueness of value, known as the double-spending problem[21]. Digital information can be copied freely, unlike physical objects. Bitcoin introduced a method to assign exclusive ownership to digital data, enabling credible transactions.

The second concerned global consensus, often framed as the Byzantine Generals Problem[17]. In a network of untrusted participants, Bitcoin created a shared record that could not be altered unilaterally yet could be collectively accepted without a central authority.

Bitcoin resolved these challenges through proof of work[21-23]. Participants expended computational energy to create new blocks and were rewarded with bitcoin. This aligned economic incentives with protocol compliance, making attempts to rewrite history economically infeasible.

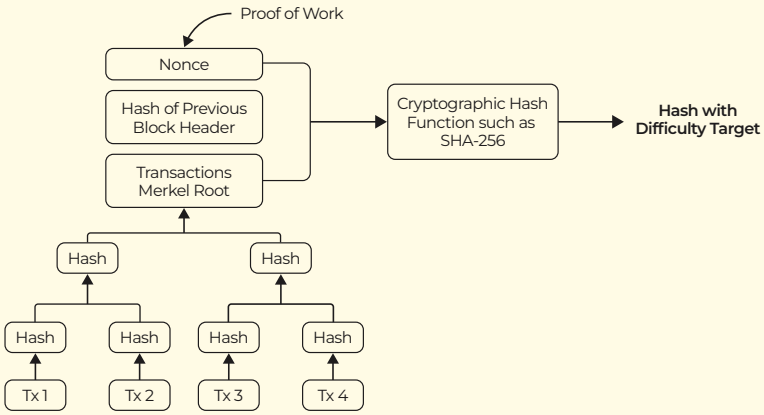


Figure 2: Proof of Work in Bitcoin Blockchain. Source: Ajitesh Kumar

The result was a trust machine: a system with no central operator, publicly defined rules, and universal verifiability[24]. Trust was not transferred to a new authority but reorganized through code and consensus.

This experiment is often linked to Friedrich Hayek's idea of denationalized money[25-26], demonstrating that a non-state, algorithmically governed accounting system could function in practice. However, Bitcoin diverged from Hayek's vision by operating outside existing legal frameworks rather than competing within them. This contributed to ongoing tension with governance institutions and eventual regulatory integration.

The results have been mixed. Bitcoin did not replace sovereign currencies as a medium of exchange, but it introduced a significant innovation in accounting authority. It forced monetary systems to confront digital-era questions about programmability, verifiability, and auditability[27-28].

要求创造一个无人能够单方面篡改、却被所有人共同承认的“事实”。

比特币的破局之道，在于工作量证明 [21-23] 的博弈设计：节点通过消耗能源进行哈希计算，争夺记账权。胜出者打包区块并获得比特币作为奖励。这套规则的精髓，让诚实成为最有利可图的选择。任何篡改历史的企图，都等同于与全网累积的能源为敌，成本高昂且自毁根基。

于是，一个不依赖任何中央权威、规则透明、运行即可被全网验证的去中心化信任机器，就此诞生 [24]。它并非寻找下一个中心，而是用代码与共识，重构了信任本身的生产方式。

这一成就，使比特币常被视为对哈耶克“货币非国家化”构想的一次极限技术验证 [25-26]。它以前所未有的工程严谨性证明：一个不由国家垄断发行、完全依靠算法与市场竞争维持信用的记账系统，在数字领域是可能成立的。这也标定了思想蓝图与工程现实的分野。哈耶克设想的是法律框架下私人银行信用的竞争。而比特币选择了一条更彻底的路径：它试图在数字空间构建一个超越现有主权法律框架的自治体系。正是这一根本差异，注定了其与现实治理的矛盾，并最终被全球监管体系识别、规训并重新纳入既有金融治理轨道 [27-28]。

因此，这场实验的成果呈现出一种深刻的分裂。作为一种试图流通的“货币”，比特币并未能取代主权法币。但作为“记账权”的技术革命，比特币取得了里程碑式的成功：它迫使整个传统货币体系，直面在数字时代的尖锐命题：在算法与数据主导的未来，主权信用应以何种形态存在?货币是否需要原生的可编程性、可验证性与可审计性?

因此，全球央行对数字货币的探索，远非简单的技术升级，而是一场深刻的“可验证主权”

From this perspective, central bank digital currency initiatives are not merely technical upgrades. They represent institutional responses to verifiable sovereignty[29-30], seeking to adopt features such as real-time settlement and auditability while preserving monetary control.

If blockchain enabled decentralized experimentation, **the next question concerns what form a sovereign blockchain network (DLT) capable of ensuring broad social legitimacy and state governance should take**.

Two issues are central to future development:

- The first is whether blockchain can function as a widely accepted medium of accounting authority.
- The second is why sovereign blockchains systems have not yet been implemented at scale.

Beyond the national level lies a further challenge: **Whether the peer-to-peer, disintermediated, and globally verifiable logic of Bitcoin can be adapted into a truly neutral cross-sovereign settlement system**[31-32]. Such a system would need to support value transfer among institutions that do not fully trust one another, without reliance on unilateral power or specific legal jurisdictions. This challenge sits at the intersection of technology, monetary sovereignty, and international political order.

制度觉醒[29-30]。其目标并非模仿去中心化，而是在坚守货币主权与政策职能的前提下，系统性地吸收区块链的可编程性、实时清算与全局可审计性，从而在数字竞争中重塑金融基础设施的效率与信任。

如果区块链为去中心化实验提供了理想的“技术骨架”，**那么，一个能被主权国家与社会广泛接纳、并系统性地服务于公共治理的“主权区块链系统”，其形态究竟应该如何构建?**

这指向两个决定未来格局的根本问题：

- 第一，范式之问：区块链技术，能否成为人类社会下一个公认的“记账权”媒介?
- 第二，现实之问：融合了主权意志与技术优势的“主权区块链系统”，为何尚未被系统性应用?

更进一步，一个更宏大的挑战在于：**能否借鉴比特币“点对点、去中心化、全球可验证”的架构灵感，创建一个数字时代真正中立的跨主权结算工具**[31-32]?让互不信任的央行或机构，在不受单边制裁或特定司法管辖区限制的情况下，进行可信的价值交换?这触及了技术、货币主权与国际政治秩序的交叉禁区。

Sovereign Settlement Interface: A Third Path for the Global Settlement System

主权协同结算层：全球结算体系的第三条道路

The Bitcoin experiment revealed a paradox: although a cryptographically complete and decentralized ledger has proven technically viable, it has been difficult to integrate into existing

比特币实验揭示了一个悖论：一个在密码学上完备的去中心化账本，却难以被国际政治所接

international political and legal frameworks. The same challenge applies to more advanced DLT, which offer greater functionality and programmability than Bitcoin. This outcome reflects not a technological failure, but rather the practical constraints imposed by sovereign principles.

At the same time, this trajectory has not been fully foreclosed. A further question arises as to whether sovereign intent can itself be translated into programmable rules within a shared global database. Such a shift would imply a redefinition of monetary function: money would no longer operate solely as a medium of exchange, but instead as a programmable state machine capable of facilitating global cooperation. Under this model, national laws, regulatory requirements, and diplomatic agreements could be expressed as verifiable execution rules embedded within the system.

When decentralized system design is embedded within a governance framework that preserves ultimate sovereign authority, a fundamental tension becomes apparent. **Sovereignty presupposes final decision-making power, whereas blockchain systems derive their credibility from neutrality and resistance to unilateral modification**. In practice, this tension manifests as a dual dilemma:

- **The control dilemma** concerns the need for sovereign emergency intervention, such as freezing or rollback, in contrast to the absence of a final controller that underpins global settlement networks.
- **The jurisdictional dilemma** arises from the fact that legal authority is territorially bound and embedded in locally specific regulatory systems, whereas distributed ledgers are not. This raises the problem of how algorithmic processes can resolve sovereign conflicts within execution timeframes measured in milliseconds.

Five thousand years of evolution in accounting authority yield a consistent insight: **cooperative systems that have endured and scaled have ultimately institutionalized a functional separation between the exercise of authority and the verification of records**. Technology supplies mechanisms for verification, whereas institutions govern the allocation and contestation of power.

Accordingly, the central challenge of what is often termed "sovereign blockchain interoperability" is primarily one of institutional architecture. The core design problem is how to construct a system that preserves sovereign control while maintaining network

纳。对于那些功能更丰富、可编程性更强更先进的分布式账本技术（DLT）而言，情况亦是如此。这并非技术的失败，而是主权原则不可逾越的现实。

但这条道路并未封闭：我们能否将主权意志本身，转化为全球数据库中的可编程规则?

这意味着货币功能的重构：货币将演进为驱动全球协作网络的可编程状态机。各国的法律、监管与外交协议，将转化为这台机器中可验证的执行代码。

当“去中心化自治”的理想被引入“主权控制”的现实框架，根本矛盾随即显现：**主权要求终极裁决权，而区块链的生命力来自不可篡改的中立性**。这一矛盾在实践中表现为双重困境：

- **控制权困境**：主权需要冻结、回滚等干预能力，而全球结算网络需要“没有最终控制者”的中立性。
- **管辖权困境**：源于法律权威天然受制于领土边界，并深嵌于各国各自的监管体系之中；而分布式账本则超越了地域限制。由此引发了一个问题：算法如何在毫秒间裁决主权冲突?

五千年记账权的演进史给出了启示：**任何持久扩展的协作系统，最终都实现了“权力的行使”与“事实验证”的制度性分离**。

因此，主权区块链互操作的核心挑战在于制度设计：如何构建一个既能保障主权控制权、又保持网络中立性的架构?既然矛盾无法消除，破局之道在于系统性地管理矛盾。

在“中心化控制”与“去中心化自治”的经典困境之外，**我们提出“主权协同结算层”（SSI）作为第三条道路**：

neutrality. If this tension cannot be resolved, it must be formally managed through explicit governance constraints and operational procedures.

Beyond the classical trade-off between centralized control and decentralized autonomy, **this paper proposes a Sovereign Settlement Interface (SSI) as a third path**.

> *This approach does not assume trust among sovereign actors. Instead, it requires that cross-border operations produce cryptographically verifiable proof, thereby converting the absence of trust into machine-verifiable state transitions that are auditable, reproducible, and institutionally accountable.*

SSI is not intended to replace existing financial market infrastructures, such as real-time gross settlement RTGS systems or SWIFT. Rather, it is designed to augment and interconnect them. Its core objective is to introduce a capability largely absent from legacy settlement architectures that have operated for more than half a century: verifiable interoperability.

This capability has become increasingly urgent as cross-border CBDC pilots progress from proof-of-concept connectivity toward scaled deployment. While baseline technical integration has largely been achieved, the primary bottleneck is institutional and governance-related. **The scaling of cross-border cooperation remains constrained by the absence of mutual rule recognition and enforceable alignment across jurisdictions**. Structural divergences among sovereign legal systems conflict with the requirement for consistent execution semantics in cross-border settlement. Existing infrastructures lack a shared mechanism through which rules can be represented in executable form and settlement outcomes can be independently verified.

Accordingly, the proposed solution is not the unification of national legal systems, but the introduction of an architectural buffer layer that enables divergent rule sets to coexist while supporting shared verification of execution outcomes.

The proposed architecture is based on a core design principle referred to as **dual-track consensus**, in which the sovereign governance track and the verifiable technical track are separated at both the institutional and technical levels. The sovereign track encompasses national rule-making authority and final adjudication rights, whereas the technical track provides neutral proof generation and verification across the global network.

> *不预设任何主权间信任，但强制要求所有跨境操作生成可验证的密码学证明，将“不信任”转化为可审计、可验证、可问责的技术事实。*

SSI 并非取代现有金融基础设施（如 RTGS、SWIFT），而是对其增强与连接。它的核心使命，是为运行了半个多世纪的体系注入一种新的原生能力：可验证的互操作性。

这一能力在全球各国央行 CBDC 跨境试点从“连通”迈向“放量”的当下，显得尤为紧迫。技术链路已然打通，**真正的瓶颈在于治理：跨境协作的规模化，卡在了“规则互认”的终极矛盾上**。多主权法律体系天然差异，与跨境交易对统一执行标准的需求，构成了结构性冲突。现有体系缺乏一套“规则可执行、结果可验证”的共通机制。

因此，破解之道不是试图统一各国法律，而是在架构上创造一个允许规则差异共存、但执行结果可被共同验证的“缓冲层”。

这依赖于名为**“双轨共识”**的核心设计：将主权治理轨道（一国的规则制定与最终裁决权）与可验证技术轨道（全球网络中立的证明生成与验证权）在制度与技术上解耦。

连接双轨的“缓冲层”由三项核心工程组件构成：（见 A5 章节）

- **Policy-DSL**（法规映射语言）：将法律中可执行的核心规则，转化为无歧义的“机器语法”。
- **JPack**（法规要件集）：将特定辖区在特定时间生效的整套规则，封装为可签名、可版本化的数字文件。
- **PoPC**（政策合规证明）：在交易跨越边界前，依据规则包生成密码学收据，使合规结论可独立重放验证。

The buffer layer interfacing these two tracks comprises three core engineering components (refer to Chapter A5):

- **Policy-DSL** (Policy Domain-Specific Language): Executable elements of applicable law are translated into a formal, unambiguous, machine-readable syntax.
- **JPack** (Jurisdiction Packs): The complete set of rules in force within a given jurisdiction at a specific point in time is encapsulated in a digitally signed, versioned package.
- **PoPC** (Proof of Policy Compliance): Prior to cross-border settlement, cryptographic receipts are generated based on the relevant jurisdictional rule packages, enabling compliance outcomes to be independently replayed, audited, and verified.

Through the coordinated operation of these components, dual-track consensus is realized. Rules are defined and maintained within the sovereign governance track. When transactions become cross-border, Proof of Policy Compliance (PoPC) proof is generated within the verifiable technical track. The end-to-end workflow follows a structured evidentiary lifecycle: domestic proof generation → global hub verification and ordering → secure execution by the receiving party → end-to-end independent auditability.

This design constitutes a form of protocol-layer integration. Just as the TCP/IP protocol stack did not replace national telecommunications networks but instead enabled global interconnection on top of them, SSI provides heterogeneous sovereign financial systems with a shared verification protocol for the credible execution of rules. It functions as an optional compliance and audit augmentation module whose deployment requires no systemic overhaul, but rather adherence to common evidentiary standards - thereby substantially reducing adoption barriers.

At its core, the SSI framework establishes a clear separation between sovereign autonomy within domestic jurisdictions and verifiable global interaction (refer to Chapter A6):

- **The Sovereign Compliance & Execution Layer** preserves full domestic authority while translating sovereign intent into independently verifiable technical proof through Policy-DSL and PoPC.
- **The Sovereign Relay Hub** is designed under strict functional minimalism, limited to transaction ordering and proof verification, and governed by a "three prohibitions" foundational principles: no asset custody, no unilateral

三者协同，“双轨共识”得以运转：各国在主权轨道上管理规则；当交易跨境时，PoPC 在技术轨道上生成证明。其流程遵循“证明的全球化流动”：本国生成证明包 → 全球枢纽验证排序 → 接收方安全执行 → 全过程独立审计。

这本质上是一种“协议层整合”。 正如 TCP/IP 协议并未取代各国电信网，而是在其上实现了全球互联；SSI 旨在为异构的主权金融系统，提供一套关于“规则如何被可信执行”的通用验证协议。它是一个可选配的“合规与审计增强模块”，部署无需系统性变革，仅需遵循共同证明标准，从而极大降低了采纳门槛。

SSI 体系的核心，在于实现“主权境内绝对自治”与“全球交互可验证”的清晰分离：（见 A6 章节）

- **主权合规执行层**：各国境内保留一切权力，但通过 Policy-DSL 与 PoPC，将主权意志转化为可独立验证的技术事实包。
- **主权中继枢纽**：职能被极端简化为交易排序与证明验证，并受“三不”宪章（不持有资产、不执行单边制裁、不解释语义）约束。它将法律冲突从“死结”转化为可审计、可外交协调的技术事件。
- **独立审计框架**：通过密码学工具，使监管方能在不接触原始数据的前提下，进行穿透式审计，将“基于规则的秩序”落实为可检验的技术现实。

“主权协同结算层”不创造乌托邦，也无意取代现有的全球金融体系。而是为这个必然存在不信任的世界，建立一套透明化、证明化、可计算化的全球验证基础设施。**它为主权国家提供了一个风险可控的选项**：无需改变内部规则，只需接入一套可共同审计的技术协议。

sanctions, and no interpretation of policy semantics. Under this model, legal conflicts are transformed from system-blocking deadlocks into auditable technical events that can be resolved through diplomatic coordination.

- **Independent audit framework** enables regulators to conduct deep, cryptographically grounded audits without requiring access to raw transaction data, thereby translating rule-based order from political commitment into verifiable technical execution.

The SSI does not aspire to a utopian resolution of geopolitical conflict. Rather, it establishes a transparent, proof-based, and computationally enforceable global verification infrastructure for an international environment in which distrust remains a persistent structural condition. **It offers sovereign states a controlled participation model** that requires no modification of domestic legal or regulatory rules, but instead adherence to a jointly auditable technical protocol.

Under conditions of sustained strategic competition, such a system does not eliminate conflict. However, it increases the auditability and observability of cross-border financial activity. While confrontation may not be prevented, its financial externalities become more predictable and, in certain domains, more governable. Participating states may reduce cross-border settlement friction while accruing a new form of digital-era compliance credibility that is legible to global markets.

Ultimately, the proposal is a standardized protocol for proof exchange within the global financial system. It does not promise a fully harmonized order; it commits only to a minimal operational principle: that every cross-border exercise of sovereign authority within the system generates verifiable traces.

By requiring sovereign actions to produce cryptographically verifiable proof, the basis of international coordination shifts from fragile trust-dependent equilibria to more stable verification-based equilibria. This may constitute one of the most practically attainable foundations for global cooperation in the digital age.

The evolution of accounting authority remains unfinished. The work presented here marks the opening of a new chapter - one defined by verifiability.

在战略竞争常态化的今天，这套系统不会消除冲突，但能使金融活动更可审计、更可观测；不一定能阻止对抗，但能让对抗的成本更可预测、更可管理。参与其中的国家，将在降低跨境摩擦的同时，积累一种新型的、可被全球市场识别的数字合规信用。

我们最终提出的，是全球金融体系的“标准化的证明交换协议”。它不承诺完美世界，只承诺：在这个系统里，每一次权力的跨境行使，都将留下可验证的痕迹。

当主权行为必然留下可验证证明时，国际协作的基础便从“信任博弈”，转向坚实的“验证博弈”。这或许正是数字时代全球协作能够建立的最务实根基。

记账权的故事远未完结，而我们今天的工作，只是翻开了名为“可验证性”的新章。

CHAPTER A2.

Core Principles *of* the Framework for Sovereign-Verifiable Settlement Interface

A2. 章节

主权可验证结算框架的四大核心原则

Abstract:

This chapter sets out the four foundational principles that Sovereign-Verifiable Settlement Interface must adhere to. These constitutive principles operate in a cumulative and interdependent manner, forming the foundational pillars of the system:

1. **Digital Abstraction**: defining money, in the digital era, as a programmable and verifiable shared accounting interface, where the term interface denotes an institutional coordination boundary governing interaction among sovereign systems, rather than a specific software endpoint.
2. **Settlement Neutrality**: maintaining a principled and impartial posture of this interface within a multi-sovereign environment.
3. **Execution Transparency**: ensuring that execution of rules is supported by mechanisms that are verifiable, auditable, and reproducible by independent third parties.
4. **Sovereign Continuity**: the ability of the system to maintain essential operational functionality and accountability under extreme conditions.

This principled framework emerges from a systematic analysis on the nature of monetary settlement, the logic of financial regulation, and the architectural properties of distributed systems. It further provides a normative benchmark for evaluating whether a given system possesses the institutional and technical robustness required to support sovereign-level instances cooperation.

（本章摘要）

本章旨在阐述主权可验证结算框架必须遵循的四项基本原则。这四项原则层层递进、缺一不可，共同构成这一体系的价值基石：

1. **数字抽象**：定义货币在数字时代，作为“可编程且可验证的共享记账接口”的根本形态，这里的“接口”特指管理主权系统间交互的制度性协调边界，而非单纯的软件端点；
2. **结算中立**:确立“可编程的记账接口”在多主权环境下必须坚持的公正立场;
3. **执行透明**：通过可验证、可审计、可复现的技术机制，确保规则执行的可信度；
4. **主权连续**：保障系统在极端条件下维持核心功能与责任追溯的能力。

这一原则框架的形成，源于对货币结算本质、金融监管逻辑以及分布式系统架构的深入思考，它也是衡量一个系统能否真正支撑国家间主权级主体协作的标尺。

A2.1

Digital Abstraction: Money as a Programmable Accounting Interface

数字抽象：货币是一套可编程的记账接口

"The ultimate form is formless,
and the foundational logic remains nameless."

"大象无形，道隐无名。"

— Lao Tzu, Tao Te Ching（老子,《道德经》）

The evolution of money can be understood, in fundamental terms, as the evolution of accounting technology - from early ledger-based record-keeping to institutional account systems and, most recently, digitally distributed ledgers. While the material and technical forms of money have changed over time, shifting from metallic coinage and paper instruments to electronic accounts, its essential function has remained unchanged: to provide a socially recognized mechanism for recording and settling obligations and for specifying "who owes whom, and in what amount". Accordingly, its role as "the central symbol within society's accounting system"[1]has remained constant.

In contemporary practice, this accounting system has evolved into a multi-layered digital network: commercial banks function as primary accounting nodes; payments operate as standardized message exchanges among these nodes; and cross-border

货币的演进，实质上是记账技术的迭代史。无论形态如何变化，从金属铸币、纸质票据到今天的电子账户，货币的核心功能始终是社会公认的记账与清算工具，旨在清晰记录"谁欠谁多少"。货币作为"社会记账系统核心符号"的本质 [1] 从未改变。

如今，这套记账系统已发展成为一个多层级的数字网络：商业银行是基础记账节点，支付是节点间的标准报文交换，跨境清算则是不同国家记账系统之间的对账与法律确认过程。国际清算银行 (BIS) 将"结算"定义为"资金在法律上不可逆转地完成转移、债务得以清偿"。

settlement takes place through processes of reconciliation and legal confirmation among national accounting systems. The Bank for International Settlements (BIS) defines "settlement" as the moment at which funds are transferred with legal finality and obligations are discharged, emphasizing that **settlement is not simply the extinguishment of an obligation through the transfer of funds, but the transfer of claims that have become irrevocable and unconditional**[2].

In the actual business of corporate cross-border payments, there is a severe time lag and information gap between the issuance of a payment instruction and the point at which settlement is completed (and becomes legally irreversible). This is one of the core sources of friction. Taking traditional SWIFT routes as an example, end-to-end processing of a cross-border remittance often can take several days, and once message information contains errors, it is returned and triggers renewed inquiries and resubmissions. Along paths involving multi-tier correspondent banking chains (such as certain RMB or European routes), a single transfer may pass through multiple intermediary banks, accompanied by opaque fee deductions and fragmented status visibility: neither the payer nor even the banks can clearly track the precise movement of funds. This lack of state visibility is not the failure of any single institution, but an inherent systemic outcome of clearing structures that span institutions and legal jurisdictions.

From this perspective, the modern financial system can be understood as a "distributed accounting machine" jointly maintained by multiple actors:

- The recorded content consists of monetary claims and payment instructions.
- The rules governing these records are derived from legal frameworks and internal risk-control regimes.
- Ledger consistency ultimately depends on inter-institutional settlement networks.

A "transfer" can therefore be understood as a coordinated update across multiple ledgers for the purpose of extinguishing a shared obligation, while "final settlement" denotes the point at which such updates acquire irrevocable legal force.

This understanding gives rise to two structural shifts:

- **A shift in governance logic**: away from a single authoritative global ledger and toward interoperable standards that enable national accounting systems to interoperate in a secure and predictable manner.

这揭示了一个关键点：**结算不仅是数字变动，更是法律关系的最终了结**[2]。

在企业跨境付款的实际业务中，支付指令发出与结算已完成（法律上不可逆）之间存在显著的时间差与信息断层，这是最核心的摩擦来源之一。以传统 SWIFT 线路为例，跨境汇款的全链路处理动辄耗时数日，且一旦报文信息有误，便会被退回并触发重新查询与补报。在涉及多级代理行链条的路径中（如人民币或部分欧洲路径），一笔转账可能穿越多家中介银行，并伴随扣费不明与状态割裂：付款人乃至银行都难以掌握资金的确切动向。这种状态不可见并非单一机构的故障，而是跨机构、跨法域清算结构下内生的系统性结果。

从这个角度看，现代金融体系就像一台由多方共同维护的"分布式记账机器"：

- 记账内容是各类货币债权和支付指令。
- 记账规则由法律和内部风控共同决定。
- 而确保多方账本最终一致的对账过程，则依赖于跨机构的清算网络。

因此，"转账"实质上是多方为清偿同一笔债务同步更新各自账本；"结算完成"则意味着这次更新获得了法律上的最终效力。 这一认识催生了两个根本性的转变：

- **治理思路的改变**：从追求单一系统的绝对权威，转向构建互联互通的标准。全球结算体系的关键，不在于建立一个全球统一的总账，而是设计一套能让各国账本安全、高效互操作的通用协议。
- **技术范式的升级**：从静态的数据记录，转向动态的规则治理。将监管要求，直接编码为可自动执行的逻辑，让账本自身成为合规的第一道防线，实现"国家法律高于代码逻辑"的治理新高度。

- **A shift in technological paradigm**: from static record-keeping to programmatic, rule-governed execution, in which supervisory requirements are embedded directly into executable logic, such that the ledger itself becomes the first layer of compliance – an architecture that reflects the principle that national law supersedes code logic.

这两大转变共同指向同一个未来：**全球结算体系的核心，将演进为一个可编程、可验证的共享记账接口**。需要明确的是，这一接口并非旨在取代各国现有的主权记账系统，而是构建一套制度化的协作框架。

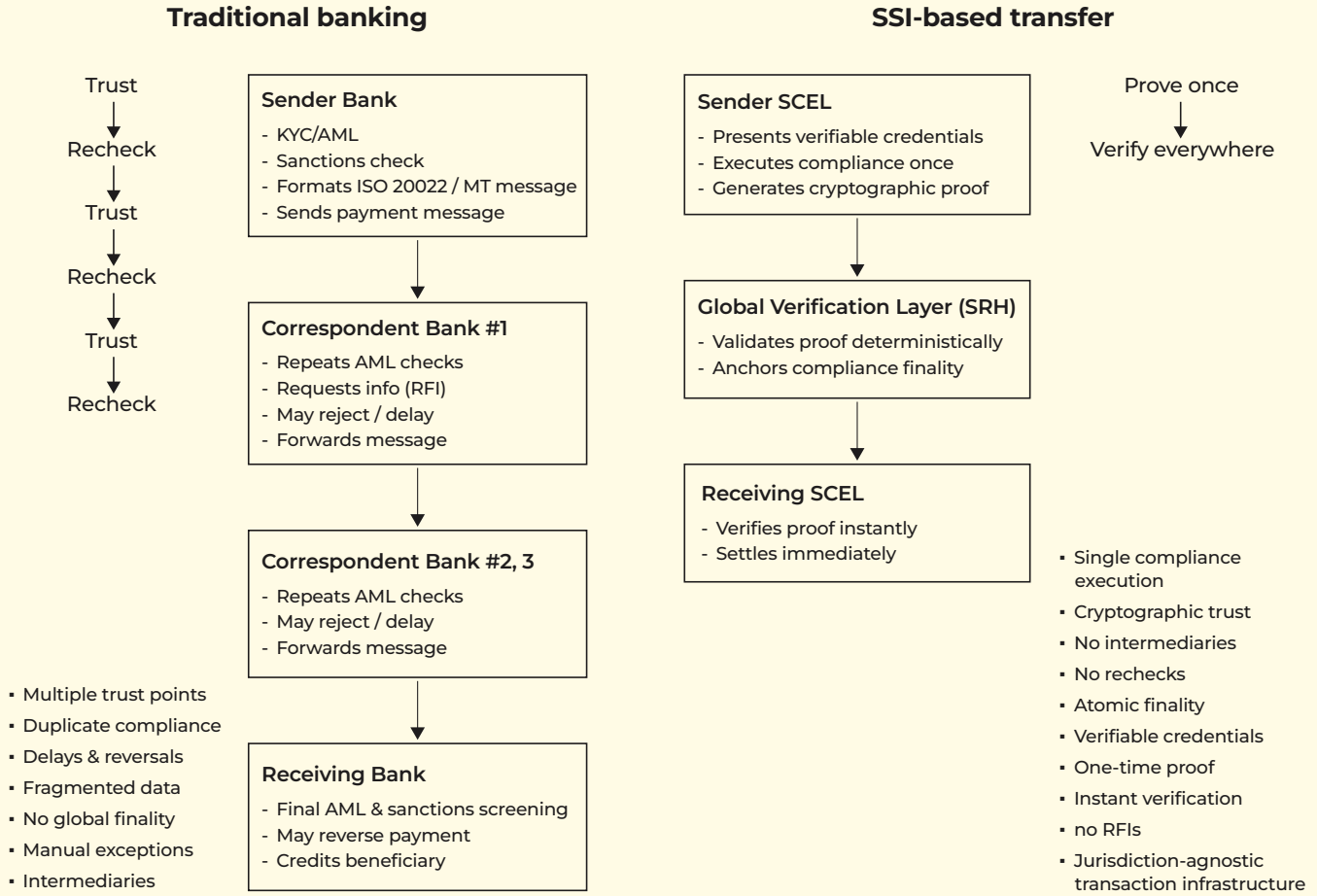


Figure 3: Structural Comparison of Traditional Banking vs SSI Transfer

Taken together, **these two transformations point toward a common trajectory: the core of the global settlement system evolves into a programmable and verifiable shared accounting interface**. This interface is not intended to replace existing sovereign accounting systems; rather, it establishes an institutionalized framework for cooperation among them. It specifies the conditions under which sovereign systems are intended to interact, including the formats in which information is submitted, the logic according to which rules are executed, and the manner in which evidentiary chains are generated such that any third party can independently replay and audit them.

The fundamental purpose of this framework is to ensure that cross-sovereign settlement cooperation rests on verifiable technical facts rather than on reliance upon the credit or discretion of

它清晰地定义了不同主权系统之间应如何交互：信息以何种格式提交、规则以何种逻辑执行、又如何生成一套可供任何第三方独立重放与审计的证明链。其根本目的是，使跨主权结算协作得以建立在一套可验证的技术事实之上，而非依赖于某一单一中心的信用背书。在这一框架下：

- 货币流动体现为多方账本状态同步更新。
- 商业合同与监管规则被直接写入可执行的代码。

any single central authority. Within this framework:

- Monetary flows correspond to synchronized state updates across multiple ledgers.
- Commercial contracts and regulatory mandates are encoded as executable rules.
- Every accounting event produces an auditable proof trail.

Participants retain full sovereignty over their domestic accounting systems and rule-making authority, while gaining interoperability through this shared interface. DLT technology is significant precisely because it provides a practically viable means of constructing such an interface, thereby rendering trustworthy cross-sovereign collaboration feasible in practice.

For this reason, the subsequent core principles - settlement neutrality, execution transparency, and sovereign continuity, constitute essential preconditions for integrating this interface into the evolving landscape of global governance while respecting sovereign diversity.

- 每一次记账变动都会自动生成可供审计的证明链条。

参与各方在完全保留自身记账系统和规则制定权的前提下，通过这个共享接口实现互联互通。分布式账本技术的根本价值在此得以凸显：它首次为构建这种强大、可靠的共享记账接口提供了完整且可行的工程路径，使得跨主权、跨机构的可信协作从理论构想走向现实实践。

正因如此，后续章节将要阐述的结算中立、执行透明和主权连续性，都是为了确保这个“记账接口”能够稳健、可信地融入全球治理格局而必须遵循的原则。它们共同奠定了一个在尊重主权多样性的前提下，足以支撑未来数字文明发展的可信基石。

A2.2
Settlement Neutrality

Once money is abstracted as a shared accounting interface, a central question arises: what stance must this interface maintain in a world of coexisting sovereigns? The required stance is “settlement execution neutrality”, which constitutes a minimum condition for the credibility of any shared settlement layer.

In legal terms, settlement signifies the final extinguishment of obligations[3-5]. Accordingly, the settlement layer functions as the ultimate confirmer of transactional outcomes and must be confined to the accurate and faithful execution of settlement, rather than the exercise of discretionary or politically conditioned judgment. When settlement infrastructure becomes subject to political contingencies, it ceases to operate as a trusted public good and instead functions as an instrument of coercive leverage - a transformation that undermines its legitimacy.

Empirical experience further demonstrates that when critical

结算中立

一旦将货币抽象为共享的记账接口，一个根本问题便浮现出来：在多主权共存的全球格局中，这个接口必须秉持何种立场?答案就是“结算中立”。这是清算层必须坚守的底线。

结算在法律层面意味着债务的最终了结[3-5]。因此，清算层扮演的是“最终确认者”的角色，其职责是忠实、准确地完成清算过程，而非进行带有倾向性的裁决。一旦清算行为附加上政治条件，它便从一个本应可信的公共服务，异化为胁迫工具，其公信力也将随之崩塌。

现实一再发出警示：当支付清算基础设施被单一实体集中控制时，极易被用作“地缘政治武

payment and settlement infrastructure is concentrated under the control of a single actor, it becomes highly susceptible to deployment as a tool of geopolitical pressure. Differential treatment at the settlement layer erodes participants' confidence in systemic fairness and incentivizes the development of insulated or alternative networks, thereby increasing fragmentation within the global settlement landscape.

The principle of settlement neutrality therefore seeks to preserve a clear institutional boundary: the underlying accounting system must execute settlement and maintain reliable records without embedding political judgments within its protocol. Decisions concerning sanctions, market access, and other policy matters must remain within the sovereign purview of individual states, rather than being predetermined at the level of shared infrastructure[6].

In operational terms, this principle implies the following:

- The sovereign DLT's base protocol must not incorporate sanctions rules directed at any country, institution, or individual.
- All compliance screening, including AML and sanctions checks, must occur within each sovereign's Sovereign Compliance & Execution Layer (SCEL), which operates under its own jurisdictional authority (as detailed in Chapter A6).
- The settlement layer's responsibility is strictly limited to finalizing ledger updates and extinguishing obligations once a transaction has passed sovereign compliance review, while producing tamper-proof proof of execution and finality through the Sovereign Relay Hub (SRH) (as detailed in Chapter A6).Moreover, the finality discussed within this Principia framework is not equivalent to the elimination of risk; rather, it provides a determinate anchor that can be jointly referenced for subsequent verifiable compliance and chains of responsibility.

Settlement neutrality does not disregard differences in national policy preferences, nor does it challenge the legal validity of sanctions imposed through proper sovereign procedures. Rather, its central claim is that sovereign policy discretion must be institutionally separated from global public settlement infrastructure. This separation corresponds directly to the dual-layer governance structure, constitutional and operational, outlined in Chapter A4. Only by maintaining this boundary can states collectively rely on a shared global settlement system.

器”。无论出于何种理由，在清算层实施区别对待，都会摧毁所有参与者对系统公平性的基本信任，最终可能迫使各方为求了保而转向封闭或另建替代系统，导致全球结算网络走向分裂。

因此，本框架所坚持的结算中立，旨在捍卫一条基本原则：底层记账系统只负责完成清算并留下可信记录，其协议本身绝不内置任何政治倾向。 所有关于市场准入、制裁等政策决策，都应由各国在其主权管辖范围内自主实施，而不是预先固化在底层协议中 [6]。

在实践层面，这一价值为体系设计划定了清晰的边界：

- 作为中立清算层的主权分布式账本，其底层协议不应包含任何基于国家、机构或个人的制裁规则。
- 所有反洗钱、制裁筛查等合规审查工作，均由各国在其自主控制的主权合规执行层（SCEL）内完成（具体形式将在 A6 章详述）。
- 清算层的唯一使命是：当交易通过各国的合规审查后，确保其按照既定规则完成账本更新和债务清偿，并通过主权中继枢纽（SRH）生成不可篡改的执行与终局性证明（详见 A6 章）。此外，本宪章体系讨论的终局性并不等同于风险终结，而是为后续的可验证合规与责任链条，提供了一个可被共同引用的确定性锚点。

需要明确，结算中立并非无视国家间的政策差异，也承认依法实施的制裁具有合法性。其核心主张在于：必须将这类政策裁量，与作为全球公共基础设施的记账系统，在制度层面进行有效隔离，以防止基础设施本身被政治化。这

Settlement neutrality is not something that can be asserted by self-declaration; it must be grounded in physical conditions that can be verified by third parties. At a minimum, these should include:

1. **Auditable authority boundaries**: the shared settlement layer possesses neither rule-making authority, nor interpretive authority, nor discretionary power; it is responsible only for validating preset rule versions and proof structures.
2. **Replayability of proof and rule versions**: every settlement determination must be independently recomputable by third parties under fixed rule snapshots and inputs, yielding consistent conclusions.
3. **Interface symmetry and visibility parity:** all participants are provided with isomorphic interfaces, equivalent proof-verification capabilities, and consistent state visibility; processing paths do not vary based on participant identity.
4. **Demonstrable neutrality:** the system should support proof, using public test vectors, that under identical inputs and rules, different participants obtain completely identical verification results, with any bias manifesting as visible audit discrepancies.

Accordingly, the neutrality emphasized by this Principia framework is not a political pledge, but an institutional constraint that is engineering-verifiable, reviewable, and demonstrable.

一制度隔离的设计，直接对应 A4 章将阐述的“宪章层”与“运营层”分离的双层治理模式。唯有坚守这一底线，各国才可能真正信任并共同使用同一套全球结算系统。

结算中立并不是一种自我宣称，而必须具备可被第三方验证的物理条件。最低限度应包括：

1. **权限边界可审计：**共享结算层不具备规则制定权、解释权与裁量权，仅负责核验预置的规则版本与证明结构。
2. **证明与规则版本可重放：**任何结算判定都必须能在固定规则快照与输入下，由第三方独立重算并得出一致结论。
3. **接口对称与可见性对等：**参与方享有同构接口、同级证明验证能力与一致的状态可见性，处理路径不因身份差异而改变。
4. **中立性演示：**系统应支持在公开测试向量下的证明：在相同输入与规则下，不同参与方得到的验证结果完全一致，任何偏倚都将转化为可见的审计差异。

因此，本宪章体系的中立并非政治承诺，而是工程上可验收、可复核、可演示的制度约束。

A2.3

Verifiability & Replayability

执行透明：可验证性与可回放性

In a settlement system shared by multiple sovereigns, trust cannot be grounded in institutional reputation or informal assurances. Instead, it must rest on technical properties that enable independent verification. Within this framework, transparency refers specifically to the verifiability and replayability of rule execution,

在一个由多国共享的结算体系中，“信任”不能建立在主观承诺或机构声誉之上，而必须基于能够被独立检验的技术事实。本框架所强调的“透明”，其核心是确保规则的执行过程本

together with interpretive continuity - that is, the stable interpretation of rules, proof, and outcomes across time and system evolution.

A credible system requires external verifiability, meaning that key operations can be independently validated using publicly available information[7]. Financial oversight further requires reconstructability - the ability to reproduce historical decisions and operations with precision for purposes of audit and accountability[8]. Verifiability and replayability, in turn, depend on deterministic execution, comprehensive recording of inputs and outputs, and continuity in the interpretation of system state across successive execution contexts. Taken together, these requirements imply that verifiability, replayability, and interpretive continuity must be intrinsic properties of the settlement architecture.

For this purpose, the framework identifies three technical pillars:

- **Verifiability**: For each state-transition operation that affects ledger finality, the system must deterministically emit a structured, cryptographically signed proof package that can be independently validated by third parties. This proof, referred to as Proof of Policy Compliance (PoPC) and specified in detail in Chapter A5, enables verification of the rule set applied, the input state and parameters consumed, the resulting output state produced, and the authority under which the operation was authorized.
- **Replayability**: Given a specific version of the applicable rule set and a complete, canonical record of input data, any qualified observer must be able to deterministically replay the execution and obtain identical results. This property requires deterministic execution semantics, comprehensive capture of execution context and parameters, and tamper-resistant preservation of operational logs sufficient to reproduce historical state transitions.
- **Semantic Continuity**: Changes to rule sets, system configuration, or participating execution environments must preserve the semantic meaning of rule execution and evidentiary artifacts across time and system versions. Historical ledger records and compliance proof must remain machine-interpretable, cryptographically verifiable, and interoperable across protocol upgrades, jurisdictional transitions, and integration with external accounting and audit systems.

Traditional Distributed Ledger Technology (DLT) consensus mechanisms are primarily concerned with achieving agreement

身是可验证、可事后复现的。

一个可信系统依赖于“外部可验证性”，即关键操作能够被第三方仅依据公开信息进行独立校验 [7]。同时，金融监管也要求系统具备“可回放性”，即能够完整复现历史上任何时间点的决策与操作细节，以支持审计和责任追溯 [8]。而可验证性与可回放性，又需要系统保持单一、连续的状态，并能够在系统存续的所有时间段之间无缝切换。因此，可验证性、可回放性以及释义连续性，必须共同成为下一代结算架构的内在属性。

本框架将它们界定为支撑可信协作的三大技术支柱：

- **可验证性**：系统必须为每一笔影响最终结算的操作，生成一个结构化、可进行数字签名、可供独立校验的证明包。这类证明在本框架中称为政策合规证明（PoPC），其具体形式将在 A5 章详述。通过 PoPC，任何第三方都能独立验证：执行了什么规则、输入是什么、输出了什么结果、以及由谁在何时授权。如此一来，信任的基础就从依赖机构信誉，转变为验证密码学证明。
- **可回放性**：在给定明确的规则版本和完整的输入数据后，任何合格的观察方都必须能够独立重新运行整个执行过程，并得到完全一致的结果。这不仅要求规则像数学公式一样准确无误，还要求执行环境、参数和操作日志被完整、真实地记录下来，使得历史上的任一关键瞬间都能够在法庭或审计场景中被精准“重现”。
- **释义连续性**：规则、系统配置或参与环境的任何变更，必须长期保持执行语义与证明意义的兼容性。历史记录与合规

on ledger state - that is, ensuring that state transitions are ordered, validated, and finalized consistently across participating nodes. They do not, by themselves, establish whether those state transitions were executed in compliance with applicable policy or regulatory rules across jurisdictions. In addition, this approach entails a structural trade-off. It requires either the deployment of publicly accessible validator nodes - thereby increasing exposure to coordinated attacks aimed at majority control or quorum capture - or the reliance on trusted execution environment (TEE) enclaves, which may introduce risks of physical co-location, shared administrative control, and correlated failure within a limited trust domain. Addressing this limitation requires the integration of a policy domain-specific language, jurisdiction-specific rule sets, and cryptographically verifiable Proofs of Policy Compliance (PoPC). Together, these components form a verifiable and replayable rules-consensus layer, as detailed in Chapter A5.

Verifiability and replayability therefore constitute a second, orthogonal layer of consensus. The first layer ensures factual consistency and finality of the ledger state, while the second ensures the legitimacy, compliance, and accountability of the rule-governed processes that produced that state. Semantic continuity further ensures that these processes, and the evidentiary meaning of their outcomes, remain stable, machine-interpretable, and compatible across protocol upgrades, rule-version changes, and long-term system evolution. In the layered architecture described in Chapter A6, the circulation and validation of PoPC proof provides the operational substrate for this rules-consensus layer.

证明应始终清晰可解、可验证，能够跨越版本迭代，并确保与外部会计系统的互操作性。

在主权协作场景下，传统区块链的“共识”机制通常只能回答“账本是否一致变化”的问题，却无法回答更关键的“这一变动是否符合各方规则”。此外，其要么依赖公开验证者增加攻击面，要么依赖 TEE 带来集中失效风险。解决之道是引入法规映射语言（Policy-DSL）、核心领域专用语言（Core-DSL）以及政策合规证明（PoPC），形成一套可验证、可复盘的“规则共识”（其具体形式均将在 A5 章详述）。

因此，可验证与可回放共同构成了主权可验证结算框架的“第二层共识”。第一层共识（分布式账本技术）保障了账本状态一致性（事实为真）；第二层共识（规则证明链）则保障了所有操作的正当性与可问责性（行为为善）。释义连续性则确保了这些操作过程及其结果的证明意义，在系统演进和跨时期审查中始终保持连贯、兼容与可理解。实现“第二层共识”的工程架构，正是 A6 章“分层模型”中 PoPC 流转机制的核心任务。在这一分层架构中，PoPC 证明的流转为这一维度的共识提供了运行基础。两层共识结合，构成了从客观事实到合规行为的完整可信链条。

A2.4
Sovereign Continuity

主权连续性

The preceding principles establish system credibility under normal operating conditions. As sovereign financial infrastructure, however, the system must also be capable of operating under

上述原则确保了体系在常态下的可信运行。然而，作为国家关键金融基础设施，其设计必须

extreme scenarios, including armed conflict, sanctions, or large-scale network disruption. The critical question is whether essential economic activity can be sustained and whether accountability and control over financial records can be reliably preserved under such conditions[9].

At the outset, it must be emphasized that the concept of sovereign continuity is not intended to circumvent legal, regulatory, or international obligations. Rather, it is designed to ensure that, in circumstances involving institutional conflict, infrastructure impairment, or contested sovereignty, participating states retain full operational control over their domestic ledger state and associated cryptographic compliance proof, and remain able to account for, verify, and interpret those records ex post in accordance with their respective legal and regulatory frameworks.

Contemporary digital sovereignty is characterized by a structural tension: national economies are deeply embedded in global financial networks, yet reliance on externally controlled payment and settlement channels exposes them to risks of disconnection, loss of access, or asset immobilization. Financial infrastructures that depend entirely on foreign technology stacks or external legal jurisdictions may therefore lose effective operational sovereignty during periods of crisis.

The principle of sovereign continuity addresses this risk by requiring both sustained domestic operability under conditions of external isolation and verifiable reintegration once connectivity is restored. This requirement entails following design properties:

- **Independent Operation**: Each participating state must be able to continue domestic payment, clearing, and settlement activities during periods of network partition or external disconnection.
- **Proof Preservation**: Any attempted cross-border, payment instructions, or settlement intents arising during periods of disconnection must be recorded via an independent, tamper-resistant proof mechanism, preserving execution context and intent for subsequent verification.
- **Orderly Recovery**: Upon restoration of connectivity, a predefined, auditable reconciliation and re-synchronization process must govern the integration, validation, and resolution of records generated during isolation, thereby restoring global ledger consistency in a controlled manner.

It must be emphasized that sovereign continuity does not, under any circumstances, permit unrestricted system behavior during

考虑最坏情形：在战争、制裁、网络中断等极端事件中[9]，系统能否维持经济命脉的最低限度运转，并留存无法抵赖的责任证明?

必须首先澄清，“主权连续性”并非旨在规避任何法律、监管或国际义务。其核心要义在于，当出现制度冲突、基础设施中断或主权争议时，确保各参与国依然能对其自身的账本记录与合规证明保持完全的控制能力与事后解释能力。

当前，数字主权面临一种双重困境：国家经济既深度融入全球网络，又因关键支付通道可能被“武器化”而暴露在断联、资产冻结的巨大风险之下。一套完全依附于他国技术或司法体系的系统，其主权在危机时刻难免名存实亡。

本框架提出的“主权连续性”，正是为了应对这一终极风险。它要求系统具备在压力下持续运行与在事后可信恢复的双重能力：

- **独立运行能力**：当与外部网络完全中断时，系统必须保证任一参与国能在孤立环境下，继续处理其国内的支付清算业务，维持最基本的经济活动。
- **证明保全能力**：对于断联期间可能产生的对外支付义务或尝试，需通过独立的“证明带”机制，完整记录下本地的支付意图和所有操作。这些可验证的记录，是国家在“数字静默期”维护自身权益、并在网络恢复后主张权利的核心依据。
- **有序恢复能力**：网络连通恢复后，必须有一套预先设定、可审计的对账与冲突解决机制，能够公正地整合或裁决断联期间各方产生的本地记录，最终恢复全球账本的一致性。

必须强调，主权连续性绝非允许在紧急状态下为所欲为。相反，它要求任何应急操作都必须

states of emergency. Rather, it requires that any emergency-mode operation be subject to stricter rule constraints and more stringent evidentiary requirements than those applicable under normal operating conditions. The authority to activate emergency modes, the bounded scope within which execution rules may be temporarily modified, and the procedures through which such actions are subsequently reviewed, validated, and held accountable must be explicitly specified at both the technical architecture and governance layers. Throughout this process, all state transitions and control actions must be cryptographically non-repudiable, and all associated records and proof must be preserved.

In this way, sovereign continuity completes the logical structure established by the preceding principles. Even under conditions of extreme stress, settlement neutrality must be preserved to the greatest extent possible, and any exceptional measures must remain fully traceable through enhanced mechanisms for verification and deterministic replay.

受到比常态更严格的规则约束和证明记录。谁有权启动应急模式、应急状态下能在多大范围内临时调整规则、事后如何接受审查与问责，所有这些都必须在技术设计和治理层面被清晰定义，并做到过程不可抵赖、记录永久留存。

至此，主权连续性与前三大原则形成了一个逻辑闭环：即便在极端压力下，清算层也应最大限度地保持其中立性，并借助强化了的验证与回放机制，确保任何临时权力的行使都无法逃脱永久追溯。

A2.5

Integration of the Four Core Principles and Significance of This Chapter

四项核心原则的统一与本章意义

Taken together, these four principles address a foundational design question: what constitutes legitimate financial infrastructure in an era defined by the digital reconstruction of settlement systems and the reconfiguration of sovereign boundaries in the digital realm? Rather than operating as independent considerations, they form an integrated architectural framework for evaluating the correctness, credibility, and resilience of Sovereign-Verifiable Settlement Interface.

- **Digital abstraction** defines the system's conceptual model, specifying money as a programmable and verifiable shared accounting interface.
- **Settlement neutrality** establishes the system's institutional posture in cross-sovereign interaction, constraining the

综上所述，本章确立的四项核心原则，共同回应了一个根本命题：在全球结算体系经历数字化重构与数字主权边界重组的深刻变革中，何为合格的下一代金融基础设施。这四项原则并非孤立的条目，而是构成了一套审视与构建“主权可验证结算框架”的完整价值坐标系。

- **数字抽象**揭示了系统的本质，完成了从实体到数字接口的认知跃迁。
- **结算中立**确立了该接口在全球协作中必须坚守的公平立场。

settlement layer to neutral execution rather than discretionary judgment.

- **Execution transparency** provides the technical mechanisms - verifiability, replayability, and semantic continuity - through which this posture is rendered auditable and enforceable.
- **Sovereign continuity** ensures that the system maintains operational resilience, accountability, and evidentiary integrity under conditions of stress, isolation, or emergency.

Taken together, these principles form a coherent architectural logic: they define the system's conceptual model, constrain its institutional posture, render its execution verifiable, and ensure its operational continuity over time.

This chapter therefore establishes the normative and architectural foundation for all subsequent technical, institutional, and governance design. Any system that fails to satisfy even one of these principles, irrespective of its technical sophistication, remains a domain-specific financial application with blockchain features, rather than a sovereign-grade settlement infrastructure capable of supporting cross-sovereign cooperation.

Conversely, only when these principles serve as the foundational constraints can subsequent constructs, such as the Policy-DSL, PoPC, and cross-jurisdiction recognition mechanisms, exhibit coherence, legitimacy, and internal consistency.

The construction of a sovereign-grade system therefore begins with conceptual and legal definition, not with implementation. Only by first establishing why the system exists and which principles it must uphold can the technical question of how to build it be addressed in a manner that preserves architectural integrity and long-term governance alignment.

- **执行透明**提供了确保这一立场得以可信实施的技术方法。
- **主权连续**则为整个体系在最坏情况下的持续运作与事后追责提供了最终保障。

因此，这四项原则共同构成了连贯的架构逻辑：它们定义了系统的概念模型、约束了其制度立场、实现了执行的可验证性，并确保了其长期的运行连续性。

本章的根本意义，在于为后续所有的技术架构设计、制度安排与治理模型，树立了不可动摇的价值锚点。一个系统如果在任何一环上存在缺失，无论其代码如何精妙，都只能算作“具备区块链特征的业务系统”，难以承载主权级数字协作的重任。

反之，唯有奠基于此原则基石之上，后续关于 Policy-DSL 语言、PoPC 机制、跨域互认协议等一切具体构建，才得以拥有统一的灵魂与正当性的源泉。

构建主权级别的系统，其起点从来都是哲学思考与法律原则，而非单纯的代码编写。只有先厘清“为何而建”与“应当何为”，关于“如何构建”的探索才不会迷失方向。

CHAPTER A3.

Mathematical Formalization *of* Verifiable System Order:

The Minimal Auditable Closed Loop

A3. 章节

秩序的数学化：

最小可审计闭环

Abstract:

Section A2 established the value of Sovereign-Verifiable Settlement Interface. This chapter addresses its core engineering proposition: how to construct an institutional-grade foundation of order that does not depend on ex post interpretation and instead admits objective, repeatable verification.

Contemporary global financial infrastructure defines "settlement completion" on the basis of two primary mechanisms: inter-institutional consensus and retrospective, ex post audit processes[1-2]. Finality is grounded in central bank ledgers, operational system logs, regulatory oversight, and, ultimately, judicial enforcement. While these mechanisms are effective under normal conditions, their underlying epistemic model remains one of after-the-fact reconstruction: when settlement truth is contested or examined, it must be reassembled from distributed records, documentary proof, and institutional attestations.

The principal innovation of Sovereign-Verifiable Settlement Interface lies in the introduction of a fundamentally different paradigm for the production of order. In this paradigm, rule execution itself constitutes order. Each state transition, at the moment of its execution, is irreversibly transformed into a mathematically formalized and self-contained evidentiary object - one that can be independently replayed, verified, and validated without recourse to retrospective interpretation.

Under this framework, the notion of a "completed" cross-sovereign settlement is redefined. Completion no longer signifies institutional acknowledgment or post hoc reconciliation, but rather the ability of any authorized participant to independently and deterministically replay all applicable rules and state transitions associated with the settlement. Given identical inputs, such replay must necessarily yield identical outputs. Trust is thereby relocated from institutional credibility and discretionary judgment to the verifiability of open rule sets and mathematical consistency.

To operationalize this paradigm, this chapter introduces a core methodological construct: the minimal auditable closed loop. This construct does not refer to a specific implementation or software component, but to a meta-structural condition for the existence of provable order. It specifies the minimal and sufficient requirements under which sovereign-level digital actions can be verified, audited, attributed, and recognized across institutional and jurisdictional boundaries. Where this closed loop remains intact - logically and evidentially, order rests on an objective foundation. Where it is broken, the system necessarily reverts to a reliance on subjective consensus and discretionary interpretation.

(本章摘要)

A2 确立了主权可验证结算框架的价值坐标。本章将回答其核心工程命题：如何构建一种不依赖事后解释、具备客观可证明性的秩序基础。

当代全球金融基础设施将“结算完成”建立在两个前提上：机构间的主观共识与事后的回溯性审计[1-2]。它依赖中央银行的账簿、系统的日志、监管的权威与司法的强制力。这些机制在多数时间有效，但其根本模式是“事后解释”：当需要确认真相时，我们必须调取分散各处的文件、日志与证明进行人工还原。

主权可验证结算框架的本质突破，在于构建一种全新的秩序生成范式：让“规则执行”过程本身直接构成秩序，使其在发生瞬间就转化为一条可独立存在、可重复验证的数学化证明链，从而摆脱对“事后解释”的依赖。

在新范式下，一笔“已完成”的跨主权结算，其含义发生根本转变：它意味着任何被授权的参与方，均可在不依赖他方陈述的情况下，独立、完整地重放该次结算所涉及的全部规则判定与状态变更，并在相同输入下必然获得完全一致的输出。信任的基础，由此从对机构信誉的依赖，转向对公开规则与数学一致性的可验证性。

为实现此范式，本章提出核心方法论构建：“最小可审计闭环”。它并非具体软件模块，而是构成可证明秩序的“元结构”。它定义了主权级数字行为可被审计、可被问责、可被跨域采信的一组最小充分条件。只要该闭环在逻辑与证明上成立，秩序便具备了客观根基；反之，若闭环断裂，系统将不可避免地退回至依赖主观共识的原始状态。

A3.1

The Four Elements of Provable System Order

可证明系统秩序的四个要素

Washington Constitutional Convention,1787, VMFA

"In questions of authority, let no more be heard of confidence in man, but bind the system down from betrayal by the chains of mathematical logic."

"在权威问题上,不要再谈论对人的信任,
而要用数学逻辑的锁链, 将系统锁死在不可背叛的轨道上。"

— *Inspired by Thomas Jefferson（受托马斯·杰斐逊思想启发）*

The completion of traditional financial collaboration is, in essence, a form of subjective certitude achieved among multiple parties through institutional arrangements and institutional credit. It constitutes a social consensus rather than a mathematical fact. What Sovereign-Verifiable Settlement Interface institutes is a fundamentally different proof paradigm: **mathematically verifiable consistency**. Within this framework, the system anchors transaction authenticity through cryptographic proofs, shifting the nature of settlement finality from perceived completion to verifiable completion.

To enable this paradigm shift, a system must possess native capabilities to address four unavoidable fundamental questions:

- **Attribution of action**: The system must uniquely which legal entity initiated the operation, and within which sovereign framework and functional mandate it was performed.

传统金融协作的达成，本质上是参与各方基于制度规约与机构信誉达成的主观确信。这种完成状态依赖社会共识的背书，而非数学事实的确认。相比之下，SSI 确立了可经数学验证的证明范式：即**可证明一致性**。在这种范式下，系统通过密码学证明来锚定交易的真实性，使结算效力从各方相信它已完成转向各方能验证它已完成。

为了实现这个范式跃迁，系统必须具备原生的技术能力 , 以回答四个不可回避的根源性问题：

- **行为归属**：系统必须能够界定是哪一个法律主体，在何种主权授权与职责背景下发起了此项操作?

- **Intent locking**: The system must authenticate the complete business intent, rule set, and input conditions were explicitly declared by that entity at the moment of initiation.
- **Process traceability**: The system must maintain a comprehensive record of all processing steps and state transitions as the operation traverses heterogeneous systems and sovereign boundaries.
- **Truth reproducibility**: In the event of dispute, can the entire process be re-executed under the original conditions and deterministically deduce an identical conclusion?

A structure that can natively and systematically answer these four questions constitutes the **minimal auditable closed loop**. This construct is composed of four mutually coupled and inseparable elements, each corresponding precisely to one of the meta-questions above:

1. **Source signature**: Identify who initiated the action, and within which sovereignty context. (Establishing a non-repudiable origin of responsibility.)
2. **Transaction binding**: At the moment of initiation, capture the complete rule set and exact inputs were declared. (Producing an immutable snapshot of the decision state.)
3. **Controlled submission path**: Record precisely what did the action experience as it crossed system and sovereignty boundaries. (Forming a verifiable, end-to-end evidentiary chain of process execution.)
4. **Reconciliation and replay**: In the presence of dispute, enable the full decision trajectory be reproduced under identical conditions. (Providing an independently reproducible, final verification.)

The closed loop formed by these four elements constitutes a first-principles foundation that translates the value propositions of execution transparency and sovereignty continuity into engineering reality. It is not an optional system capability, but the necessary structural skeleton upon which sovereign-level digital collaboration must be built.

In Chapter A6, subsequent constructs, such as Sovereign Compliance & Execution Layer (SCEL), Sovereign Relay Hub (SRH), regulatory mapping languages (Policy-DSL), compliance proofs (PoPC), and cross-domain mutual recognition protocols, will all be developed from this closed loop as their unified logical point of departure.

- **意图锁定**：系统必须能够确证该主体当时所声明的完整业务意图、规则集与输入条件究竟是什么?
- **过程留痕**：系统必须完整记录该操作在穿越不同系统与主权边界时，具体经历了哪些处理与状态变更?
- **真相可复**：当争议产生时，监管方能否依据原始条件重新执行全流程，并必然推导出完全一致的结论?

一个能够从原生、系统层面回答上述四个问题的逻辑架构，即构成了**最小可审计闭环**。它由以下四个相互耦合、不可分割的要素构成，每一项要素均与前述根源性问题精准对应：

1. **源头签名**：通过密码学签名锁定发起者，界定行为由谁、在何种主权语境下发起，从而确立不可否认的责任原点。
2. **事务绑定**：系统在行为发起瞬间，将完整的业务规则与精确的输入条件进行绑定，从而生成不可篡改的决策快照。
3. **受控提交路径**：系统记录该行为在跨越不同系统与主权边界时的流转细节，从而形成可验证的端到端证明链。
4. **对账与重放**：当争议发生时，监管方依据既有条件完整复现决策轨迹，从而提供独立且可复现的终极校验。

这四者构成的闭环，是将“执行透明”与“主权连续”的价值主张，转化为工程现实的第一性原理。它不是系统的可选功能，而是承载主权级数字协作的必要骨架。

在 A6 章节中, 无论是主权合规执行层（SCEL）、主权中继枢纽（SRH）、法规映射语言（Policy-DSL）、政策合规证明（PoPC）还是跨域互认协议，都将以此为统一的逻辑起点展开构建。

A3.2

Element Elaboration: The Four Pillars of the Closed Loop

A3.2.1 Source Signature: Instant Anchoring of Responsibility

The source signature provides cryptographic anchoring of legal attribution at the precise moment an action is initiated. It requires that any critical operation be authorized and signed by a legally recognized subject, and that the signature be bound to the minimal necessary contextual attributes, including sovereign affiliation and functional business role.

This mechanism categorically prevents intermediaries from acting through delegated signing or retroactive endorsement. The source signature establishes the origin point of responsibility within the minimal auditable closed loop. If this origin is ambiguous or contestable, the integrity of the entire downstream evidentiary chain is necessarily compromised.

A3.2.2 Transaction Binding: Immutable Encapsulation of Context

Transaction binding addresses the question of what, precisely, constituted the complete content and operative context of an action at the time of execution. The inputs to a single decision consist of four categories of critical information: *business parameters, such as amounts and counterparties*; *applicable rule sets, including legal, policy, and risk-control constraints*; contextual attributes, such as time, jurisdiction, and hierarchical position; and the real-time system state, including balances and limits.

In traditional financial architectures, these elements are stored in a fragmented and distributed manner. As a result, the operative context of an action can only be reconstructed retrospectively, yielding interpretations that are inherently approximate and discretionary. The objective of transaction binding is to replace this model of "ex post interpretation" with "determination at the moment of execution".

要素阐释：闭环的四个支柱

A3.2.1 源头签名：责任的瞬间锚定

源头签名在行为发生的瞬间，通过密码学手段锚定其法律归属。它要求任何关键操作必须由法定主体签署，且签名必须绑定其主权归属与业务角色等最低限度语境。

系统禁止任何中介进行代签或补签。源头签名构成审计闭环的责任原点；若此环节逻辑模糊，后续证明链的根基将彻底瓦解。

A3.2.2 事务绑定：语境的不可篡改封装

事务绑定的核心目标，在于确证在操作执行的瞬间，究竟是什么构成了该操作的完整内容及其运行上下文。针对单一决策的输入由以下四类关键信息组成：*业务参数（金额、对手方等）*、*规则集合（法律、政策、风控）*、*上下文（时间、辖区、层级）以及实时系统状态（余额、限额）*。

传统金融架构中，这些信息分散存储，导致事后重建的语境只能是近似的、可解释的。事务绑定的目标，是将这种"事后解释"转为当时即定。它在行为发起时，将所有实质输入与规则版本压缩并通过密码学绑定为一个不可拆解的整体。这确保了任何字段篡改均可被检测，且任何事后重放都必须以该原始整体为输入。

At the point of initiation, transaction binding compresses and cryptographically binds all substantive inputs and applicable rule versions into a single, indivisible unit. This construction ensures that any subsequent tampering with individual fields is detectable and that any later replay or verification must take the original bound context as its sole input.

In operational financial environments, compliance rules do not always take the form of fully institution-controlled DSLs. Sanctions screening provides a clear example. Screening workflows commonly depend on third-party data and algorithmic platforms (e.g., World-Check and comparable services), whose matching logic, thresholding methods, and list update cadences often lie outside the direct control of the executing institution.

In such settings, the notion of a "rule version" cannot be limited to internal policy artifacts alone. It must also include the externally determined components that materially affect the decision outcome, such as the third-party platform release identifier, cryptographic hash snapshots of the relevant list data (or its partitioned subsets), the identifier of the matching model or algorithm family, and the effective parameter configuration applied at execution time. Absent versioning and cryptographic anchoring of these external dependencies within the transaction's proof package, deterministic replay becomes infeasible in practice.

Accordingly, from an engineering standpoint, the rule-version locking required by this Principia must extend to the minimal verifiable encoding and **version anchoring of all external rule dependencies that can influence compliance determinations**.

Transaction binding therefore functions as a **context encapsulation mechanism**. It transforms the question of which rules and data govern a decision from a narrative-dependent, subjective assertion into an objective fact that can be directly verified. In the absence of transaction binding, compliance and risk control inevitably remain in a condition of ambiguous rules and malleable context, which constitutes a structural breeding ground for systemic risk and regulatory arbitrage.

A3.2.3 Controlled Submission Path: Explicit Evidentialization of Process

The execution of rules for a cross-border transaction necessarily traverses a chain composed of boundary gateways, compliance engines, relay networks, and settlement or ledger systems. In traditional financial architectures, this execution path exists

在现实金融环境下，合规规则并非总以机构完全自主控制的 DSL 形式呈现。以制裁名单筛查为例，由于通常依赖第三方数据与算法平台（如 WorldCheck 等），其匹配逻辑、阈值算法与名单更新节奏往往处于执行机构的控制范围之外。在此类场景下，规则版本的定义不能只局限于内部策略文件，还必须涵盖第三方平台版本、名单数据快照哈希、匹配算法标识及相关参数配置等关键变量，若上述外部依赖未被版本化并锚定在交易证明中，所谓的可重放在实践中就无从谈起。在工程实践上，本宪章体系所倡导的规则版本锁定，必须延伸至：**对所有外部规则依赖进行最小可验证编码与版本锚定**。

因此，事务绑定是一种**语境封装技术**。它将"当时依据何种规则与数据"这一问题，从一个依赖叙述的主观命题，转化为一个可直接验证的客观事实。缺乏事务绑定，合规与风控将永远停留在"规则模糊、语境可塑"的状态，这正是系统性风险与监管套利的温床。

A3.2.3 受控提交路径：过程的显式证明化

一笔跨境交易的规则执行，需穿越由边界网关、合规引擎、中继网络与结算或账本系统构成的链条。在传统架构中，这一流程主要依赖"接口规范 + 日志 + 审计"的形式存在。虽然各环节保留局部记录，但这些记录在格式、语义与时间上彼此异构，缺乏跨机构的密码学对齐与统一结构。

这种碎片化导致了一个后果：系统能证明起点与终点，却无法提供一条**端到端、语义一致、可被第三方重放的证明链**。中间状态只能通过事后调取多方日志、拼接时间线并辅以人工解释来还原，而无法成为原生的可验证对象。

primarily in the form of interface specifications, operational logs, and ex post audits. While each component maintains local records, these records are heterogeneous in format, semantics, and temporal granularity, and lack cryptographic alignment or a unified structural representation across institutions.

As a result, such systems can typically attest to the point of initiation and the point of completion, but cannot natively provide an **end-to-end, semantically coherent process proof chain that is independently replayable by a third party**. Intermediate states must instead be reconstructed retrospectively through multi-party log retrieval, timeline correlation, and manual interpretation. They do not exist as first-class, natively verifiable objects.

In practice, this structural limitation has been repeatedly exposed through incidents affecting critical financial infrastructure:

- **Bank of England RTGS/CHAPS (2014)**: A routine configuration change triggered a nine-hour service outage affecting, delaying the settlement of 142,759 payments. The subsequent investigation required several months and involved the retrieval of extensive log data from the central bank, CHAPS Co., and participating banks, followed by manual reconstruction of execution timelines before an incident report could be produced. This episode demonstrated that even within highly centralized and well-governed payment infrastructures may lack inherently verifiable end-to-end execution path proof and depend on extensive retrospective analysis[3].
- **Visa Europe Network (2018)**: A rare failure involving a network switch in one of Visa Europe's data centres resulted in a prolonged service disruption that affected millions of transactions across Europe, with approximately 5.2 million transactions failing to process correctly. Investigations into the incident required the synthesis of logs, monitoring data, and operational information from multiple parties in order to reconstruct the fault propagation path. This episode demonstrated that even highly automated global payment networks lack natively replayable end-to-end execution proof and continue to rely on dispersed operational records and post hoc interpretation to explain transaction failures[4].
- **CHAPS Payment Outage due to SWIFT (2024)**: A subsequent incident involving the CHAPS system further illustrates this vulnerability[5]. The UK's high-value CHAPS payment system experienced a temporary outage after an

现实中，这一结构性缺陷已在多次关键基础设施事故中暴露：

- **英国央行 RTGS/CHAPS（2014）**：一次常规配置变更引发九小时的服务中断，导致 142,759 笔支付的结算工作出现延误。事后调查耗时数月，需从央行、CHAPS 公司及各银行处调取海量日志，人工拼接时间线，方能产出事故报告。这表明，即便在高度集中、治理成熟的系统中，端到端路径亦非天然可验证，仍依赖大量的回溯分析 [3]。
- **Visa 欧洲网络（2018）**：Visa 欧洲公司某一数据中心发生一起罕见的网络交换机故障，引发了长时间的服务中断，此次中断影响了欧洲地区数百万笔交易处理，其中约 520 万笔交易未能完成正常处理。为追溯故障传播路径，需综合多方日志、监控数据及独立评估，方能勾勒大致过程。这证明，即使在高度自动化的全球网络中，“交易为何被拒、在何处阻断”的答案，仍藏于分散的日志与内部说明，而非可独立重放的过程证明 [4]。
- **因 SWIFT 故障导致的 CHAPS 支付系统中断（2024）**：随后发生的 CHAPS 系统中断事件进一步印证了这种脆弱性 [5]。英国高价值支付系统 CHAPS 因 SWIFT 报文网络发生运营事故、导致消息处理延迟而短暂中断。英格兰银行表示，此次中断仅持续数小时，未影响零售支付，且与网络攻击无关。尽管如此，该事件凸显了对外部报文基础设施的依赖可能形成关键性的单点失效风险，表明即便治理完善的本国支付系统，也仍然受制于其全球报文主干网络的稳定性。

operational incident at the SWIFT messaging network delayed message processing. The Bank of England reported that the disruption lasted only a few hours, affected no retail payments, and was not cyber-related. Nevertheless, the incident underscored how reliance on external messaging infrastructure can create critical single points of failure, illustrating that even well-governed domestic payment systems remain vulnerable to disruptions in their global messaging backbone.

- **Centralized Systems as a Sanctions Enforcement Choke Point**: The centralized financial messaging network SWIFT can be used as a key instrument for enforcing international sanctions. For example, in March 2012, SWIFT disconnected approximately 30 Iranian banks from its network in accordance with a decision of the EU Council, effectively isolating Iran from the majority of cross-border financial transactions[6]. Since around 2015, banks in the Caribbean, Pacific island states, and parts of Africa have lost correspondent banking access due to AML/CFT concerns[7]. In 2022, major Russian banks were disconnected from SWIFT as part of sanctions measures[8]. By controlling access to the world's dominant interbank messaging system, sanctions authorities are thus able to impose powerful constraints on trade and finance. These cases illustrate how a single centralized network such as SWIFT can be employed as an enforcement mechanism: denying a country's banks access to SWIFT effectively severs their connections to the global financial system. As this practice continues to be applied, its scope of use may further expand.

The controlled submission path seeks to transform this logical execution route itself into an evidentiary object that can be recorded, verified, and replayed. Its realization depends on three core constraints:

1. **Standardization of recorded content**: At each node along the path, records must include the following four-tuple and be expressed in a standardized form, such as cryptographic commitments:
   - **Node identity and sovereign affiliation**: Which entity performed the processing.
   - **Input state summary**: Key transaction attributes and applicable rule versions at the time of receipt.
   - **Execution actions and conclusions**: Which checks were performed and what results and justifications were produced.

- **中心化系统作为制裁执行的“咽喉点”**：中心化的金融报文网络 SWIFT 已成为执行国际制裁的核心工具。例如，2012 年 3 月，根据欧盟理事会的决定，SWIFT 断开了约 30 家伊朗银行的网络连接，从而在事实上将伊朗从绝大多数跨境金融交易中孤立出去 [6]。自 2015 年前后起，由于对反洗钱与反恐怖融资（AML/CFT）风险的担忧，加勒比地区、太平洋岛国及非洲部分地区的银行也相继失去了代理行的接入权限 [7]。2022 年，作为制裁措施的一部分，俄罗斯的多家主要银行也被移出了 SWIFT 系统 [8]。通过掌控全球主流银行间报文系统的准入权，制裁机构得以对贸易与金融施加强大的约束力。这些案例说明了像 SWIFT 这样的单一中心化网络是如何充当执行机制的：剥夺一个国家银行对 SWIFT 的访问权，便能有效地切断该国与全球金融体系的联系。随着这种手段被持续应用，其适用范围未来可能会进一步扩大。

受控提交路径旨在将此“逻辑路线”本身转化为可记录、可验证、可重放的证明对象。其实现依赖四重核心约束：

1. **记录内容标准化**：路径中每个节点的记录，必须包含以下四元组，并以标准化格式（如密码学承诺）呈现。
   - **节点身份与主权归属**：执行处理的主体是谁？
   - **输入状态摘要**：接收时的事务关键属性与规则版本。
   - **执行动作与结论**：进行了何种检查，输出何种结果及原因。
   - **输出状态摘要与时间戳**：处理后的事务

- **Output state summary and timestamp**: Post-processing state changes and completion time.

These requirements ensure that path proof does not degenerate into arbitrary logging, but instead constitutes a structured sequence of state transitions that provides uniquely determined inputs for subsequent replay.

2. **Measurable execution environment**: Where feasible, mechanisms such as trusted execution environments or threshold signature schemes are introduced to cryptographically measure the execution environment of critical steps, thereby strengthening the tamper resistance and credibility of the proof chain.
3. **Explicit documentation of execution strength fallback**: In extreme or force majeure scenarios (such as TEE unavailability, hardware attestation failure, or the activation of pre-authorized backup paths) the system must explicitly record this "strength fallback" as a path state within the proof chain. It must be emphasized that such a fallback pertains solely to the security measurement of the execution environment and in no way compromises the rule semantics or the determinism of settlement outcomes. The system strictly prohibits any retroactive masking, tampering, or deletion; all fallback records must remain replayable and independently verifiable, ensuring full transparency under audit scrutiny.
4. **Polycentric execution and sustainability**: The controlled submission path must not rely on a single centralized execution domain, coordination hub, or globally uniform control plane. Instead, it must support execution across multiple independently governed domains, each operating with its own parameters, policy constraints, and trust anchors, while remaining interoperable through shared evidentiary semantics and verification rules. This polycentric structure eliminates single points of technical or governance failure and ensures that execution paths remain verifiable, auditable, and replayable even when individual domains are disrupted, excluded, or subject to policy divergence.

Within the SSI architecture, the structured proof generated along controlled submission paths constitutes a component of the PoPC produced by the sovereign compliance execution layer. This proof is submitted together with the transaction to the SRH. The hub does not interpret the content of the proof and does not take into account the political component, but verifies its cryptographic integrity and logical coherence. At this point, path proof is elevated

状态变更及完成时间。

以上规范确保路径证明不是任意日志，而是结构化的状态转移序列，为后续重放提供唯一确定的输入。

2. **执行环境可度量**：在条件允许时，引入可信执行环境或阈值签名等机制，对关键步骤的执行环境进行密码学度量，从而增强证明链的抗篡改能力。
3. **可信执行强度回退的显式存证**：在极端或不可抗力下导致的可信执行环境（如 TEE 不可用、硬件度量失效或启用预设备用路径时）系统必须将此类“强度回退”作为路径状态明确写入证明链。需要强调的是，回退仅涉及执行环境的安全度量等级，绝不影响规则语义与结算结果的确定性。系统禁止任何回溯性的遮蔽、篡改或删除。所有回退记录必须支持逻辑重放与独立验证，并在审计视角下保持全程透明。
4. **多中心化执行与可持续性：**受控的提交路径不应依赖于单一的中心化执行域、协调中心或全球统一的控制平面。相反，它必须支持在多个独立治理的域之间进行执行。每个域依据其自身的参数、政策约束和信任锚点运行，同时通过共享的证明语义和验证规则保持互操作性。这种多中心化结构消除了技术或治理上的单点故障，并确保即使在个别域发生中断、被排除或出现政策分歧时，其执行路径依然保持可验证、可审计且可回放。

在 SSI 架构中，这些受控路径上生成的结构化证明，正是“主权合规执行层”输出 PoPC（政策合规证明）的组成部分。它们随交易提交至“主权中继枢纽”，枢纽不解读其内容，也不考虑其中的政治因素，而是验证其密码学完整性与逻辑连贯性。至此，路径证明从各系统内部

from internal operational data within individual systems to sovereign action traces that are independently auditable within the global settlement network.

The controlled submission path does not presume system perfection. Rather, it requires that all deviations from ideal execution conditions leave explicit traces within the proof. Its ultimate objective is that, when any critical transaction is examined years later, what is observed is not merely the final outcome, but a fully reproducible chain of actions. This chain records, with clarity, who acted, where, under which rules, which decisions were made, and, when applicable, what compromises were introduced. Centralized rails enforce access via global switches, while SSI/DLT architectures allow rule-scoped, bilateral, auditable control.

A3.2.4 Reconciliation and Replay: Ultimate Reproducibility of System Order

Reconciliation and replay constitute the final verification stage of the minimal auditable closed loop. A system that cannot be replayed does not possess auditability, and a system that is not auditable cannot serve as sovereign-level digital infrastructure.

In this context, "replay" denotes the following capability. After fully obtaining the three required elements:

1. the source signature and subject attribution
2. the rules and inputs applied at the moment of transaction binding
3. and all intermediate proof generated along the controlled submission path

an independent party, operating outside the original execution environment, must be able to re-execute the entire decision process within a publicly specified rule engine and obtain results that are identical to the original outcome. This equivalence extends beyond the final allow-or-deny determination to include decision rationales, rule-evaluation paths, and all relevant intermediate states.

To ensure the validity of adjudication, replay must be performed within a predefined baseline mirror of the rule execution environment. This mirror, distributed as part of the rule package (JPack), includes deterministic runtime versions, cryptographic hashes of dependency libraries, and standardized test vectors. By constraining environmental variability, this structure ensures that any divergence in replay results can be attributed to deficiencies

的运维数据，升维为全球结算网络中可独立审计的主权行为轨迹。

受控提交路径不假设系统完美，而是要求所有偏离理想状态的行为均在证明上留下痕迹。其终极目标是：在多年后审视任何一笔关键交易时，所见非仅结果，而是一条可复验的行为全链。这条全链将明确记载谁在何处、依据何规、作了何决，以及在必要时作出了何种妥协。中心化轨道通过“全局开关”实施准入控制，而 SSI/DLT 架构则实现了基于特定规则、双边协作且可审计的管控模式。

A3.2.4 对账与重放：秩序的终极可复现性

对账与重放是闭环的最终验证环节。一个无法被重放的系统，不具备可审计性；而一个不可审计的系统，与主权级基础设施的安全性要求是根本互斥的。

所谓“重放”，指在完整获取以下三项要素后：

1. 源头签名与主体信息
2. 事务绑定时所使用的规则与输入
3. 受控路径上产生的所有中间证明

一个独立于原执行环境的第三方，能够在公开实现的规则引擎中，重新运行整个流程，并得到与原始结论完全一致的结果。这不仅包括“允许 / 拒绝”的布尔判断，更涵盖全部判定理由、规则命中路径及关键中间状态。

为实现裁决有效性，重放必须在预先定义的“规则执行环境基准镜像”中进行。 该镜像作为规则包（JPack）的组成部分，包含确定性的运行时版本、依赖库哈希及标准测试向量。这确保了重放结果不受环境配置干扰，任何计算结果的不一致，均可归因于输入证明的完整

in the completeness or authenticity of the submitted proof, thereby transforming disputes from interpretive disagreements into verifiable technical facts.

Within this framework, the meaning of reconciliation undergoes a fundamental transformation. It no longer refers to the verification of balance equality, but to the confirmation that two independent replay processes produce an identical decision trajectory. This, in turn, redefines the notion of settlement completion. In the Sovereign-Verifiable Settlement Interface, the completion of a cross-border settlement must satisfy two conditions simultaneously:

1. **Ledger finality**: the transaction has reached an irreversible final state;
2. **Rule replayability**: the complete evidentiary chain associated with the transaction can be independently replayed by any authorized party and reproduce the same outcome under identical rules and inputs.

It is worth noting that compliance execution in incumbent compliance infrastructures is not always strictly deterministic. Where natural-language matching is involved - names, addresses, or transliterated aliases, rule application often relies on fuzzy matching, yielding probabilistic scores rather than uniquely determined matches. Replayability therefore requires the matching procedure to be governed and reproducible: the fuzzy-matching model and scoring methodology must be explicitly versioned; score outputs, thresholds, and relevant parameter configurations must be captured; and the final decision trajectory must be cryptographically committed as part of the transaction's proof package. The system does not require the external world to be perfectly deterministic; it requires the compliance determination to be procedurally reproducible under the same declared model, parameters, and inputs.

The institutional significance of replay derives from its coupling with predefined governance rules. Based on the type and severity of detected inconsistencies, the system generates standardized governance events and corresponding action recommendations, which activate predefined processes. For example:

- **Invalid proof chain** (such as a signature mismatch) results in automatic rejection of reconciliation and the triggering of dispute resolution protocols;
- **Ambiguity in rule execution** leads to the generation of standardized dispute proof packages submitted to the relevant sovereign regulatory authorities for discretionary review;

性或真实性问题，从而将争议转化为可验证的技术事实。

在此结构下，对账的含义发生根本演变：它不再是核对余额是否相符，而是校验两个独立的重放过程是否产出完全一致的决策轨迹。这进而重新定义了“结算完成”的概念。在主权可验证结算框架体系中，一笔跨境结算的真正完成，必须同时满足两个条件：

1. **账本终局性**：事务已经达成不可逆的终局状态；
2. **规则可重放**：该交易对应的完整证明链，可被任何授权方独立重放，并在相同规则与输入下复现同一结论。

必须注意到，在现实合规执行中问题往往更为复杂。例如，涉及自然语言匹配时（如姓名、地址、别名转写），规则往往采用模糊匹配算法。同名同姓、转写差异或别名变体等情况，会导致匹配结果存在概率性评分而非唯一确定输出。在此类情况下，系统会相应要求：模糊匹配算法必须版本化、评分结果必须被记录、最终决策路径必须被明确承诺等。换言之，系统不要求世界是绝对确定的，而要求决策过程是绝对可复现的。

重放机制的制度意义，源于其与“预设治理规则”的耦合。系统依据不一致的类型与级别，生成标准化的治理事件与行动建议，并驱动预设流程：

- **证明链无效**（如签名不匹配）：自动拒绝对账，触发争端解决协议；
- **规则执行歧义**：生成标准化的争议证明包，提交至相关主权监管方进行裁量；
- **确认的规则违反**：在预设授权下，系统生成“规则违反”事件，并可据此执行链上状态标记、后续交易拦截等预设合规动作。

- **Confirmed rule violations**, subject to predefined authorization, generate formal rule-violation events and may initiate prescribed compliance actions, including on-ledger state marking and subsequent transaction interception.

This design ensures that replay functions not merely as an audit mechanism, but as a structured input into verifiable governance processes. It does not replace the ultimate adjudicative authority of sovereign institutions; rather, it encodes their intent ex ante into explicit rules, translating audit outcomes into predictable, auditable execution recommendations. In doing so, sovereign control is transformed from abstract principle into verifiable engineering practice.

Only when both ledger finality and rule replayability are satisfied is a settlement not merely executed, but mathematically proven to be correct. At this point, the foundation of system order shifts decisively from reliance on institutional narratives to objectively consistent results that can be independently and repeatedly verified.

这一设计确保重放不仅是审计工具，更是可验证治理流程的结构化输入。它并不取代主权机构的最终裁决权，而是将其意志预先编码为明确的规则，将审计结论转化为可预测、可审计的执行建议，从而将主权控制从原则落实为可验证的工程实践。

当两者兼备，一笔结算才不仅“被执行”，更在数学上“被证明为正确”。至此，秩序的可信基础从依赖机构的权威叙事，彻底转向可反复验证的客观一致性。

A3.3

The Position of the Closed Loop in the SSI

A system designed for sovereign collaboration is not a single-dimensional “global ledger”, but a layered architecture with clearly separated functional responsibilities:

- **Sovereign domain layer**: executes domestic policy and regulatory rules;
- **Cross-sovereign relay layer**: performs transaction ordering, anchoring, and mutual recognition while maintaining procedural neutrality;
- **Application and market layer**: builds financial applications and services on top of the underlying infrastructure.

The minimal auditable closed loop serves as the unified proof

闭环在主权可验证结算框架中的位置

一个面向主权协作的体系，并非单一维度的全球账本，而是由职能分明的多层结构构成：

- **主权域内层**：执行本国政策与监管规则；
- **跨主权中继层**：承担交易排序、锚定与互认，保持中立；
- **应用与市场层**：基于底层设施构建金融应用与服务。

最小可审计闭环是贯穿这三层架构的统一证明骨架，其核心作用有三：

backbone that spans this three-layer architecture. Its role can be described along three functional dimensions:

1. **Within the sovereign domain layer, the closed loop functions as the atomic unit of compliant execution.** Any execution of domestic rules that is expected to obtain recognition from external jurisdictions or international institutions must be recorded in closed-loop form. The closed loop converts sovereign intent from a policy assertion into a cross-domain verifiable technical fact.
2. **At the relay layer, the closed loop establishes the verification baseline for cross-domain mutual recognition.** The relay layer does not evaluate the substantive content of sovereign rules; it verifies only the structural validity of the closed loop: whether the source signature is valid, whether transaction binding is consistent, whether path proofs are complete, and whether deterministic replay is feasible. Only transactions accompanied by a valid closed loop are admitted into the shared cross-sovereign order. Mutual recognition thus shifts from discretionary trust to proof-based verification.
3. **At the application and market layer, the closed loop provides the trusted technical foundation for innovation.** Higher-layer services may evolve independently, but every compliance-relevant and settlement-relevant fact they rely upon is anchored in a replayable proof chain rather than in unilateral institutional assertions. This establishes a shared and non-ambiguous factual substrate for cross-border financial activity.

Accordingly, the minimal auditable closed loop is not an auxiliary capability but a structural backbone within the sovereign DLT architecture. It connects cryptographic primitives at the base layer, policy-constrained execution at the middle layer, and market structures at the upper layer within a single provable framework. In doing so, it enables sovereign collaboration to scale along a transparent, verifiable, and auditable path.

1. **在主权域层内，此闭环是合规执行的“原子单元”**。任何本国规则的执行，若期望获得他国或国际机构的未来认可，其过程必须以闭环形式被记录。闭环将主权意志从政治声明，转化为可跨境验证的技术事实。
2. **在中继枢纽层，它是跨域互认的“验证基准”**。中继层不判断各国规则内容，只验证闭环的完整性：源头签名是否合法、事务绑定是否一致、路径是否留痕、重放是否可行。只有闭环成立，交易才被纳入全球秩序。这使互认从主观信任，转向客观验证。
3. **在应用与市场层，闭环为创新提供了可信的技术基石**。上层业务可自由创新，但其依赖的每一个“合规与结算事实”，均植根于可重放证明链的客观结构，而非任何单一机构的单方面叙述。这为全球金融市场提供了共用且无可争议的事实基础。

因此，最小可审计闭环并非附加功能，而是主权分布式账本架构构中承上启下的刚性骨架。它将底层的密码学能力、中层的政策执行与上层的市场结构，统一约束在一个可证明的框架之内，使主权协作得以在清晰、可审计的轨道上规模展开。

A3.4

Design Boundaries and Operating Principles:
Closed-Loop Constraints Under Operational and Sovereign Uncertainty

设计边界与运行原则：
现实世界中的闭环约束

Institutional design that presumes stable operating conditions, synchronized political contexts, and flawless technology is structurally unsustainable. SSI operate under non-ideal physical and institutional conditions: networks can partition, hardware can fail, software can contain latent vulnerabilities, legal interpretations can diverge, and geopolitical constraints may introduce discontinuities.

Accordingly, the design premise of the minimal auditable closed loop is not an idealized steady state, but a disciplined acceptance of operational and sovereign uncertainty. The system must assume that not all nodes will remain in optimal condition, verification paths may be disrupted, and sovereign participants may not always operate under fully aligned technical or political constraints.

In this context, the closed loop is not intended to preserve an invariant operating mode. Its function is to establish a non-negotiable institutional baseline: regardless of environmental variation, rule strength must not be diluted; regardless of path adjustments, the proof chain must remain complete; and regardless of anomalies, the critical decision trajectory must remain reconstructable ex post. On this basis, this Principia specifies three operating principles.

Principle One: Constant Rule Strength; Adjustable Verification Paths:

> The system may permit controlled switching at the level of technical routes or execution environments - for example, between primary and contingency verification paths, or among alternative proof mechanisms. Under all circumstances, however, rule versions must remain fixed, mandatory validation steps must not be omitted, and compliance thresholds must not be relaxed. Path adjustment refers exclusively to changes in verification method or execution

倘若制度设计建立在环境恒定、政治同步、技术无瑕的假想之上，那么它在现实面前终将难以为继。SSI 运行于真实的物理世界与政治环境之中：网络可能中断、硬件可能损坏、软件可能存在漏洞、司法解释可能出现分歧乃至地缘政治压力等极端变量。

因此，最小可审计闭环的设计起点并非理想化的假设，而是对现实不确定性的坦诚接纳。这意味着我们必须预设：并非所有节点都能维持最优运行，验证路径未必时刻顺畅；各主权参与方的技术与政治条件也难保完全同步。

在此背景下，闭环的意义不在于追求一种永不变化的运行状态，而是划出了一道不可逾越的制度底线：无论运行环境如何变化，规则强度不得降低；无论验证路径如何调整，证明链必须完整；无论出现何种异常，关键决策过程都必须能够被事后重建。为此，元宪章体系确立了三项操作性原则。

原则一：规则强度恒定，验证路径可调整。

> 系统允许在技术路径或执行环境层面灵活切换（如主路径与备份路径验证之间的切换，或不同证明机制之间的转换）。但在任何情况下，规则版本不得改变，必要校验步骤不得省略，合规标准不得降低。所谓路径调整，仅指验证方式或执行环境的变化，而非规则内容或风险

environment, not to changes in substantive rule content or risk parameters. This mirrors established resiliency practice in financial infrastructure: operating modes may change, but institutional rigor must not weaken.

Principle Two: Operating-Condition Changes Must Be Explicitly Marked and Auditable:

When path switching, environmental transitions, or exceptional states occur, the system must emit explicit, tamper-resistant state markers. Such markers are not admissions of non-compliance; they are structured declarations of the execution context. Their purpose is to ensure that authorized reviewers can identify the decision backdrop at the time of execution and reconstruct the complete verification trajectory thereafter. Availability may be constrained by operating conditions, but verifiability must not disappear.

Principle Three: Closed-Loop Form May Be Risk-Responsive, but the Minimum Proof Boundary Must Not Be Breached:

Transaction processing may differentiate structural complexity by risk tier, but the minimum acceptable proof boundary must be strictly enforced. Low-value, low-risk transactions may employ simplified verification paths, provided that the scope, conditions, and governance of simplification are predefined and publicly disclosed. Transactions implicating sovereign credit, systemic risk, or cross-sovereign commitments must employ the full closed-loop form, with no substitute paths permitted. Risk-responsiveness refers to differences in structural complexity and operational procedure, not to any retreat in rule strength.

In summary, the closed loop does not claim that the system will always operate in an optimal form. It ensures that, under any operating form, the system does not fall below a defined threshold of institutional strength. Its objective is not the elimination of anomalies, but the ability to make anomalous states recordable, verifiable, and accountable. Sovereign-Verifiable Settlement Interface are not designed to construct an unchanging utopia; they are designed to preserve the stability of rule execution and the continuity of proof structures under operational turbulence. The closed loop thus functions as an institutional boundary, not merely an operating state.

阈值的放宽。这与现实金融基础设施的灾备逻辑一致：可以切换运行环境，但不得削弱制度刚性。

原则二：运行条件变化必须显式记录并可审计。

当系统发生路径切换、环境变化或异常情境时，必须生成明确且不可篡改的状态标识。这并非对合规失败的承认，而是结构化的记录运行语境的变化。其目的在于确保审计者能够识别当时的决策背景，并在事后重建完整执行路径。可用性可能因环境变化受限，但可验证性绝不能消失。

原则三：闭环形态可与风险等级匹配，但最低证明边界不可逾越。

交易的结构复杂度可随风险等级差异化处理，但必须严守最低可接受的证明边界。例如，低金额、低风险交易可采用简化验证路径，但简化范围与条件必须预先定义并公开；涉及主权信用、系统性风险或跨主权承诺的交易，必须采用完整闭环结构，不得使用替代路径。这里的匹配仅指结构复杂度的差异，而非对规则强度的退让。

综上所述，闭环并不意味着系统始终处于最优形态，而是要确保在任何形态下都不突破制度强度的下限。其核心不在于消除异常，而在于让异常状态变得可记录、可验证、可追责。主权可验证结算框架并非要构建一个永不变化的乌托邦系统，而是在动荡的现实中守护规则执行的稳定性与证明结构的连续性。闭环，因此成为一道制度边界，而非某种运行状态。

A3.5

Synthesis: The Atomic Structure of Digital Sovereignty

This chapter has addressed a single foundational question: in a world where multiple sovereignties, regulatory regimes, and technology stacks coexist, if provability is taken as the primary foundation, what minimal form must a qualified digital infrastructure assume?

The concept of the minimal auditable closed loop provides a structural answer. A trustworthy DLT system must be simultaneously established across four dimensions:

- Action attribution is lockable, such that the initiating subject is identifiable and responsibility is non-repudiable;
- Execution context is fixed, such that declared rules and inputs are immutable at the moment of execution;
- Process trajectory is explicit, such that all intermediate steps along the execution path are exposed and none are concealed;
- Decision truth is reproducible, such that outcomes can be deterministically replayed and do not depend on narrative interpretation.

When these four conditions are satisfied in a mathematically verifiable manner, system order is transformed from a state maintained by authority into a structure supported by cryptographic proof. This transformation does not replace political or legal institutions; rather, it provides them with a novel technical substrate that is deterministic, replayable, and externally verifiable.

These global divergences can be summarized as follows:

Centralized Systems	SSI / Rule-Based DLT
Access controlled by infrastructure	Access controlled by participants
Binary inclusion/exclusion	Granular, policy-driven interaction

综述：数字主权的原子结构

本章旨在回答一个具体问题：在多元主权、监管与技术栈并存的世界中，若以“可证明性”为基石，一套合格的基础设施在最小尺度上应具备何种形态？

“最小可审计闭环”给出了结构性答案，一个可信的分布式账本系统必须在四个维度上同步成立：

- 行为归属可锁定（谁在发起，主体不可否认）；
- 执行语境可固化（当时说了什么，规则与输入不可篡改）；
- 过程轨迹可显影（沿途发生了什么，路径不可隐去）；
- 决策真相可复现（能否重放一遍，结论不依赖叙述）。

当这四点以数学可验证的方式确立时，秩序便从一种“由权威维持的状态”，转化为一种“由证明支撑的结构”。这并非取代政治与法律体系，而是为其赋予了一个前所未有的、可重放的技术基础。

这些全球差异可归纳如下：

特性	中心化系统	SSI / 基于规则的分布式账本
准入控制	由基础设施方控制准入	由参与者自主控制准入

Opaque decisions	Explicit, auditable rules
Ex post explanations	Deterministic outcomes

Table 1: Structural Differences Between Centralized Systems and SSI as Rule-Based DLT

Accordingly, if digital abstraction, settlement neutrality, execution transparency, and sovereign continuity are regarded as the core value vertices of a Sovereign-Verifiable Settlement Interface, then the closed loop constitutes the first-principles foundation that supports them. **It represents the minimal unit through which digital sovereignty can be executed, constrained, and held accountable, and it defines the necessary path by which cross-sovereign order advances from subjective consensus to provable consensus**.

With this foundation in place, subsequent discussions of rule description languages, proof formats, cross-domain mutual recognition, and governance arrangements share a common logical origin. Sovereign-Verifiable Settlement Interface thus evolve from a purely technical construct into an institutional engineering framework characterized by internal coherence and formal accountability.

包含 / 排除模式	二元化的准入或排除（要么全有，要么全无）	细粒度、由政策驱动的交互
决策透明度	决策过程不透明（黑盒化）	规则显式化且可审计
结果时效性	事后解释	具有确定性的执行结果

表 1：中心化系统与作为规则驱动型分布式账本技术的 SSI 之间的结构性差异

因此，若将“数字抽象”“结算中立”“执行透明”“主权连续”视为主权可验证结算框架的价值四角，那么“闭环”便是支撑这四角的第一性原理：**它是数字主权可被执行、可被限制、可被追责的最小单位，也是跨主权秩序从“主观一致”迈向“可证明一致”的必经之路**。

以此为起点，后续关于规则语言、证明格式、跨域互认与治理安排的论述，将获得共同的逻辑原点。主权可验证结算框架亦由此从技术构想，逐步显现为一套具备内在一致性的制度工程。

CHAPTER A4.

Governance and the Principia:

The Withdrawal *of* Power and the Emergence *of* Order

A4. 章节

治理与宪章：

权力的退场与秩序的涌现

Abstract:

The digital age is characterized by a fundamental tension: **sovereign governance requires clearly defined boundaries and ultimate control, whereas digital networks inherently rely on open connectivity and global coordination**. This tension leaves the global digital financial system oscillating between the two poles of "centralized unilateral governance" and "de-sovereignized technological utopianism", and has thus far prevented the construction of a logical plane capable of both carrying the will of multiple sovereignties and providing an efficient and trustworthy global public good.

In the absence of suprasovereign authority, how can sovereign states with divergent interests place trust in a public system that they jointly construct yet cannot unilaterally control?

This Principia document develops a governance framework for multi-sovereign collaboration, proof-based compliance, and neutral settlement, structured around clearly allocated authority, procedural constraint, and operational continuity. It addresses three foundational questions:

1. **The foundation of legitimacy**: how, without establishing a suprasovereign adjudicator, the system can become a common collaborative plane for sovereigns by virtue of "logical neutrality".
2. **Constraints on the boundaries of power**: how to institutionally isolate intra-sovereign discretion from inter-sovereign collaboration, preventing public mechanisms from becoming geopolitical instruments of particular entities.
3. **Network resilience**: how institutional design ensures the non-centralized nature of infrastructure, prevents its unilateral capture, and preserves its logical continuity even under conditions of extreme geopolitical disruption.

The "third path" we propose is not a moderate compromise, but a constitutional engineering project aimed at achieving sovereign separation by design and global collaboration through verifiable mechanisms. Its philosophical core is this: **the most reliable order arises from the systematic constraint of power**.

The governance philosophy of the Sovereign Cooperative Settlement Interface (the SSI framework) represents a form of reverse engineering of power. It does not create new centers of authority, but constructs a collaborative framework in which power is structurally precluded. Its legitimacy derives not from powers granted to it, but from the verifiable and immutable institutional constraints it imposes upon itself.

This is neither another closed compliance scheme nor a closed compliance system associated with any particular governance alliance. Just as the Peace of Westphalia established the jurisprudential foundation of territorial sovereignty, the Principia framework defines the governance conditions under which digital sovereignty in cross-border settlement can achieve logically verifiable mutual recognition. This is not an expansion of power, but a deliberate withdrawal and self-limitation of power within a critical public domain.

We anticipate the emergence of a solid, trustworthy, and quietly functioning global order within the boundaries of sovereign autonomy.

（本章摘要）

数字时代面临一个根本性矛盾：**主权治理要求清晰的边界与最终控制，而数字网络则天然依赖开放的连接与全球协同**。这一矛盾让全球数字金融体系在“中心化的单边治理”与“去主权化的技术乌托邦”这两极间摇摆，却始终未能构建出一个既能承载多元主权意志，又能提供高效、可信全球公共产品的逻辑平面。

当超主权权威不复存在，意志各异的主权国家如何能信赖一个它们共同构建、却无法单独控制的公共系统?

元宪章旨在将多主权协作、可验证合规、中立结算的价值体系，转化为具备明确权责划分、流程约束及可持续运行的治理结构。我们通过一套可执行的制度骨架，试图回答以下三个根本命题：

1. **合法性的根基**:在不设立超主权裁决者的前提下,系统如何凭借“逻辑中立性”成为各主权的公共协作平面。
2. **权力的边界约束**：如何在制度上隔离主权内裁量与主权间协作，防止公共机制沦为特定实体的地缘工具。
3. **网络的生存韧性**：如何通过机制设计确保基础设施的非控制性，防止基础设施被单边俘获，使其在极端地缘震荡下依然保持逻辑的连续。

我们提出的“第三条道路”,并非温和的折中,而是一场旨在通过设计实现主权隔离、通过验证实现全球协作的宪政工程。它的哲学核心是：**最可靠的秩序，源于对权力的系统性约束**。

主权协同结算层（SSI 框架）的治理哲学**是一场权力的逆向工程**。 它不创造新的权力中心，而是铸造一个权力被预先废除的协作容器。它的权威性不源于被授予的权力，而源于其对自身权力施加的、可验证且不可篡改的制度性限制。

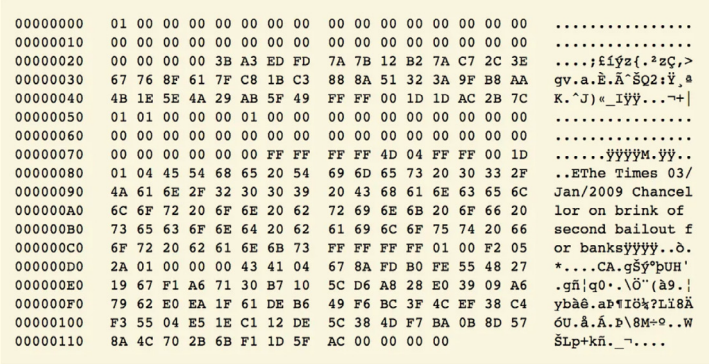
这并非又一套封闭的合规方案，更非特定治理同盟的封闭的合规体系。正如《威斯特伐利亚和约》确立了领土主权的法理基础，元宪章框架界定了在跨境结算中使数字主权达成逻辑互验的治理条件。这不是权力的扩张，而是权力在关键公共领域的一次主动退场与自我封印。

我们期待在绝对主权的边界之间，涌现出坚实、可信、静默运行的全球秩序。

A4.1

Status and Entry into Force under the Principia Framework: From Logical Architecture to Institutional Grounding

宪章的地位与生效：从逻辑架构到制度实证



```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

Satoshi Nakamoto, BTC V0.1.0, Genesis Block, 2009

"Govern by non-interference,
so that order arises spontaneously."
"无为而无不为。"

— Lao Tzu, Tao Te Ching (老子,《道德经》)

This section establishes how the Principia framework moves from a logically coherent architecture to an institutionally grounded system capable of sustained operation. Governance is treated here not as abstract political theory, but as a set of institutional commitments expressed through formal procedure and implemented through system design.

Taken together, these commitments serve a single objective: to establish a shared inter-sovereign coordination layer with public institutional standing.

Within this context, the **Sovereign Relay Hub (SRH)** must directly address three foundational questions that accompany the system throughout its lifecycle.

First, as the neutral institutional relay of the shared layer, **on what**

本节确立了元宪章框架如何从一套逻辑自洽的架构，转化为一个具备制度锚定、能够可持续运行的体系。在此语境下，治理不再被视作抽象的政治理论，而被定义为一系列通过正式程序表达、并借助系统设计得以实现的制度承诺。

综上所述，这些承诺共同指向一个核心目标：建立一个具备公共制度地位的主权间共享协作层。

在此背景下，**主权中继枢纽（SRH）**作为该共享层的中立制度中继，必须直面贯穿系统全生命周期的三个根本性命题：

basis can the SRH be prevented from exceeding its mandate or becoming an operational instrument of any particular sovereign participant?

Second, in the intergenerational evolution of rules, who possesses the authority to define and modify the SRH protocol, and through what procedures can rule changes become effective despite complex political dynamics?

Third, at the operational level, how can a polycentric institutional architecture ensure that the system does not fall into paralysis if any individual participant withdraws, defects, or collapses?

These three questions collectively define the core institutional challenges that the SRH must address from its initial establishment through long-term operation.

Core Principle: Institutional Grounding Precedes Technology

The answer advanced by SSI is clear: the SRH is not a technological system that later seeks political recognition, but an institutional construct whose governing basis is established before technical deployment.

Participating sovereigns must first adopt the Principia framework as the constitutive basis of the shared settlement layer. The Principia framework defines ex ante the limits of SRH authority and the procedures through which its protocol and governance rules may evolve.

The legitimacy of the SRH is therefore anchored in the collective institutional will expressed through the Principia framework, rather than in the self-assertion of any technological operator. Accordingly:

- The protocol and governance rules of the Sovereign Relay Hub (SRH) are not subject to unilateral determination by any single sovereign, but are formalized through shared procedures defined under the Principia framework.
- The effectiveness of governance rules depends not on opaque political direction, but on procedures that are auditable, reversible, and deterministically specified.

At the most fundamental level, the Principia framework is designed to ensure that neither individual operators nor a majority coalition of sovereign participants can convert the SRH into an adjudicative authority or a centralized center of power.

其一，职权边界与中立性保障：**应基于何种机制，防止 SRH 在运行中发生职权越位，或沦为特定主权参与者操纵的工具**?

其二，规则的代际演进：谁拥有定义与修改 SRH 协议的权威?在复杂多变的地缘政治博弈下，规则变更应通过何种程序才能生效?

其三，运行韧性与多中心治理：在运行层面，一套多中心的制度架构如何确保系统具备极强的容错能力，不因个别参与者的退出、背离甚至崩溃而陷入瘫痪?

这三个命题共同界定了 SRH 从初始构建到长期运行，必须在制度层面予以回应的核心挑战。

核心逻辑：宪章先行，技术随动。

SSI 给出的回答清晰而坚定：SRH 绝非一个在事后寻求政治认可的技术系统，而是一个在技术部署之初便已完成治理奠基的制度化构建。

参与的主权实体必须首先签署并接纳元宪章框架，将其作为共享结算层的宪制性基础。元宪章框架在事前便严密界定了 SRH 的职权红线，以及协议与治理规则演进的法定程序。

SRH 的合法性由此锚定在元宪章所表达的集体制度意志之上，而非源于任何技术运营商的自我授权：

- 主权中继枢纽（SRH）的协议与治理规则，不由任何单一主权单边裁量，而由参与方通过宪章程序共同契约化；
- 规则的生效不依赖于不可测的政治指令，而依赖于可审计、可回滚、具备硬性确定性的治理流程。

元宪章从底层确保：无论是个体运营者还是多数主权联盟，均无法将 SRH 异化为权力裁决机构或单一的价值中心。

A4.2

Core Principles under the Principia Framework:
Neutrality as an Institutional Attribute

This section explains how neutrality, through a three-layer design, is transformed from a subjective commitment into an institutional attribute embedded in the system's architecture. Its core purpose is to make neutrality a self-sustaining equilibrium under strategic interaction, rather than a fragile consensus that must be constantly guarded.

A4.2.1 First Layer: Functional Constraint and the Absolute Minimization of Authority

The statutory functions of the SRH are strictly confined to the minimum necessary set for cross-domain collaboration. Any efficiency optimization or functional enhancement beyond this boundary must either be prohibited or subjected to strict thresholds.

1. **Exclusive ordering, verification, and notarization.** The SRH is assigned, and only assigned, three core functions:
    1) **Global ordering**: establishing, for all cross-domain transactions, a unique sequence that is monotonically increasing and tamper-resistant.
    2) **Proof verification**: conducting formal, non-semantic cryptographic verification of compliance proofs (PoPC) submitted by Sovereign Compliance Execution Layers (SCELs).
    3) **Finality notarization**: issuing finality receipts with legal traceability and technical determinacy for transactions that pass verification.

Beyond these functions, the SRH has no authority to execute business logic, operate assets, or interpret sovereign rules.

2. **Semantic insulation and downward allocation of responsibility**

元宪章框架下的核心原则：
中立性作为一种制度属性

本节阐明，中立性如何通过三层递进的设计，从主观承诺转变为镌刻在系统基因中的制度属性。其核心在于使中立性成为系统在博弈中自我维持的稳态，而非需要被守护的脆弱共识。

A4.2.1 第一层：功能约束，权限的绝对最小化

SRH 的法定职能被严格锁定在跨域协作的“最小必要集合内”，任何超越此边界的效率优化或功能增强，都必须被禁止或严格门槛化。

1. **唯一排序、验证与公证**。SRH 被且仅被赋予三项核心职能：
    1) **全局排序**：为所有跨域交易建立具备单调递增属性且不可篡改的唯一时序。
    2) **证明验证**：对主权合规执行层（SCEL）提交的合规证明（PoPC）开展形式化、非语义化的密码学校验。
    3) **终局公证**：为通过验证的交易签发具备法律溯源性与技术确定性的最终性收据。

除上述职能外，SRH 无权执行任何业务逻辑，无权处置任何资产，亦无权对主权规则进行任何实质性解释。

2. **语义绝缘与责任下沉**

At the protocol level, the SRH is semantically blind. Its role is limited to signature verification, format validation, version confirmation, and deterministic replay against the referenced JPack. Responsibility for legal interpretation, compliance discretion, and violation handling remains entirely within the sovereign SCELs that generate the PoPC. The SRH does not judge whether sovereign rules are substantively correct; it verifies only whether the declared rules were executed correctly. This separation preserves sovereignty by design.

A4.2.2 Second Layer: Abolition of Power – the Three Major Constitutional Prohibitions

To prevent functional constraints from being eroded over time, the Principia framework establishes three non-derogable prohibitions. Their purpose is not merely technical. By defining what the SRH must **never become**, they shift governance from the conferral of power to the fixing of institutional boundaries, and trust from discretionary expectation to verifiable constraint.

Prohibition One: No Interpretation – becoming a "semantic insulator" of rules

Constitutional meaning: Rule execution remains within sovereign jurisdiction, while cross-domain coordination remains external to it. Regulatory logic, legal definition, and discretion are contained within each jurisdiction's JPack and SCEL. The SRH verifies proofs only. It does not interpret sovereign rules, assess their reasonableness, or engage in secondary judgment.

Engineering implementation: Policies are executed within sovereign SCELs, while the SRH receives only the resulting proof artefacts. It can attest that a transaction conforms to a referenced rule version, but cannot infer or evaluate the underlying policy intent. Its neutrality arises from designed incapacity, not discretionary restraint.

Prohibition Two: No Execution – eradicating the "weaponization" channel of sanctions

Constitutional meaning: This exchanges functional incompleteness at the design level for institutional openness at the system level. All compliance interception and sanctions-execution authority must be physically isolated and retained within sovereign judicial boundaries. This controlled technical incapacity gives the SRH structural neutrality that transcends geopolitical struggle, thereby endowing it with immunity to political interference.

SRH 在协议层面实现语义盲化。其验证职能仅限于：核验数字签名、匹配协议格式、确认规则版本（JPack 哈希）以及确定性重放。所有合规裁量、法律解释及违规处置的责任，完全锁定在生成 PoPC 的各主权 SCEL 内部。SRH 不判断规则本身的对错，仅验证声明的规则是否被正确执行。这种责任分离方式，在技术底层保障了主权的完整性。

A4.2.2 第二层：权力废除，三大宪政禁令

为防止功能约束随时间推移被蚕食，元宪章确立了三项不容逾越的禁令。其意义不仅限于技术层面：通过界定 SRH "**绝不能成为什么**"，治理重心从权力的赋予转向了制度边界的锚定，信任也随之从对裁量权的预期转向了对程序的硬性约束。

禁令一：禁止解释，成为规则的"语义绝缘体"

宪制意义：确保规则执行保留在主权管辖之内，而跨域协同则独立于管辖之外。监管逻辑、法律定义与裁量权被封装于各辖区的 JPack 与 SCEL 中。SRH 仅验证证明，不解释主权规则，不评估其合理性，亦不进行二次审判。

工程实现：政策在主权内部的 SCEL 中执行，SRH 仅接收执行产生的证明原语。系统可以证实交易符合引用的规则版本，但无法推断或评价底层政策意图。其中立性源于"设计性无能"，而非裁量性自制。

禁令二：禁止执行，根除制裁的"武器化"通道

宪政内涵：以设计层面的功能残缺，换取制度层面的全局准入。所有合规拦截与制裁执行权，必须在物理上隔离并保留在主权司法边界之

Engineering implementation: The SRH protocol layer contains no instruction set for asset freezing, transaction rollback, or fund interception. It is a pure state-broadcast channel. Any interception action must be initiated and completed within the relevant sovereign SCEL, and the SRH merely records the proof generated by that action. **This restores sanctions from low-cost, covert technical switches to high-cost legal–diplomatic acts, thereby constraining the expansion and abuse of power at the strategic level**.

Prohibition Three: No Ownership - constructing a "pure logical plane" for assets

Constitutional meaning: This fully strips the infrastructure of property claims over assets, fundamentally eliminating its credit and moral hazard, and blocking any path by which it could mutate into a "suprasovereign center of value".

Engineering implementation: The SRH holds no currency, assets, or reserves and maintains no central account. Its ledger records proof-linked transfer sequences, while asset value remains anchored in the relevant sovereign ledger of issuance. This insulates the SRH from default and run risk and prevents its evolution into a suprasovereign monetary center.

These three prohibitions jointly render the SRH a vacuum of discretionary power. It cannot gain authority through rule interpretation, coercive force through sanctions execution, or financial power through asset ownership. Its value lies precisely in this carefully designed incapacity.

A4.2.3 Third Layer: Game-Theoretic Immunity - Shifting from Controlling Motives to Constraining Consequences

1) Core principle: non-discretionary power and anti-entrenchment

The Principia framework does not assume that the sovereign will remain permanently neutral. In a multi-sovereign setting, political coalitions may seek to alter the operating conditions of the shared layer. Technology therefore cannot be vested with a veto over collective sovereign decision-making without itself becoming a suprasovereign authority.

The governance objective accordingly shifts from controlling motives to constraining consequences. The task is not to eliminate the possibility of deviation, but to ensure that any deviation from

内。这种受控的技术无能使 SRH 获得了超越地缘博弈的结构性中立，从而具备抵御政治干扰的免疫力。

工程实现：SRH 协议层不包含任何资产冻结、交易回滚或资金截流的指令集。它是纯粹的状态广播通道，任何拦截动作必须在相关主权 SCEL 内发起并完成，SRH 仅忠实地记录该动作产生的证明。**这将制裁从低成本、隐秘的技术开关，还原为高成本的法律 - 外交行为。从博弈底层抑制了权力的扩张与滥用**。

禁令三：禁止所有，构筑资产的"纯粹逻辑平面"

宪政内涵：彻底剥离基础设施的物权，从根本上消除其信用与道德风险，封堵其异化为任何形式的"超主权价值中心"的路径。

工程实现：SRH 不持有任何货币、资产或储备，亦不设中央账户。其账本仅记录与证明关联的转移序列，资产价值始终锚定在相关的原籍主权账本中。这使 SRH 免疫于违约与挤兑风险，防止其演变为超主权货币中心。

这三条禁令共同作用，使 SRH 成为一个"无害且无用"的权力真空体。它无法通过解释规则获取权威，无法通过执行制裁获取强制力，无法通过持有资产获取金融权力。它的价值，恰恰在于这种被精心设计的"无能"。因其"无所有"，故能成就"无不有"。

A4.2.3 第三层：博弈免疫，从控制动机转向约束后果

1) 核心原则：非裁量权与防固化

元宪章框架并不预设主权意志会永久保持中立。在多主权协作的复杂环境中，政治派系极有可能试图篡改共享层的运行条件。然而，若赋予技术手段凌驾于集体主权决策之上的一票

neutrality must be explicit, can be rejected, and cannot be concealed or permanently entrenched.

2) Mechanism: three layers of institutional immunity

To ensure the above objectives, the system embeds three progressive institutional immunities. These immunities are not moral commitments by any team, but inherent properties written into the Principia document, the protocols, and the proof structures. Any technical implementation that refuses to adopt these immunity mechanisms does not, by definition, belong to this Primcipia framework.

Immunity One: explicitness immunity - leaving malicious erosion nowhere to hide

Institutional objective: To prevent any deviation from occurring quietly in the name of technical evolution, operational routine, or temporary arrangements, and to ensure that deviation cannot masquerade as the natural continuation of the system.

Mechanism implementation: Every material operation, upgrade, or configuration change must declare the Principia and protocol versions it follows and expose its compliance configuration through verifiable protocol fields. These declarations are institutional facts, not discretionary narratives. Public registries, commitments, and signature proofs make deviation externally detectable.

Immunity Two: refusal and exit immunity - ending "sovereign lock-in"

Institutional objective: to prevent forced acceptance of unrecognized rule changes and thereby eliminate sovereign lock-in.

Mechanism implementation: The system explicitly defines the SRH as a voluntary collaboration layer, not a source of sovereign obligation. Any sovereign participant retains the absolute right to refuse a specific SRH instance, version, or operating configuration without thereby constituting breach. This right is guaranteed by the architecture: SCELs can operate entirely independently, PoPCs can be generated and preserved independently, and transaction compliance proofs do not depend on any single public-plane instance. **Deviation may be attempted, but it cannot be imposed.**

Immunity Three: substitutability and reconstructability immunity - stripping institutional monopoly from operators

否决权，则技术本身将异化为一种新的超主权权威，这与主权自治原则背道而驰。

因此，治理目标从对动机的管控，转向了对后果的约束。系统的任务并非要彻底根除政治偏离的可能性，而是要确保任何针对中立性的偏离行为必须显性化、可被拒绝，且绝不可被隐匿，亦无法形成永久性的既成事实。

2) 机制：三重制度免疫

为确保上述目标，体系内置了三重递进的制度免疫。这些免疫不属于任何团队的道德承诺，而是被写入宪章、协议与证明结构中的固有属性。任何拒绝采纳这些免疫机制的技术实现，在定义上即不属于本宪章体系。

免疫一：显性化免疫，让恶意侵蚀无处遁形

制度目标：防止任何偏离以技术演进、运维惯例或临时安排之名悄然发生，确保偏离无法伪装成体系的自然延续。

机制实现：任何重大的操作、升级或配置变更，均须明确声明其所遵循的元宪章及协议版本，并通过可验证的协议字段暴露其合规配置。这些声明构成了制度事实，而非任由主观裁量的叙事。公共注册表、状态承诺与密码学签名证明，使得任何偏离行径在外部均具备绝对的可被察觉性与可审计性。

免疫二：可拒绝与可退出免疫，终结"主权锁定"

制度目标：阻断任何强加于人的、未经共识的规则变更，从而从根本上消除主权实体被系统绑架或锁定的风险。

机制实现：体系明确将 SRH 定义为自愿协作层，而非主权义务来源。任何主权参与者均保有拒绝特定 SRH 实例、版本或运行配置的绝

Institutional objective: In response to extreme long-term risks - such as operator incapacity, deviation, or other contingencies-to ensure that the legitimacy of the Principia framework does not depend on any specific team. Its core purpose is to sever entirely the potential leverage of operating authority over control authority, preventing temporary operational functions from mutating into permanent institutional monopolies.

Mechanism implementation: The Principia framework specifies institutionally that the legitimacy of the advocated system is anchored solely in the Principia text, open-source protocol specifications, and the traceable historical proof chain, rather than in any particular implementation or team. Owing to the determinism of protocol execution, any new compliant public-plane implementation can restore an identical global state by replaying the complete historical PoPC set and the referenced rule versions. **This fundamentally eliminates the risk of the system being captured and corrupted by any particular interest group, ensuring the permanent recoverability of the public infrastructure.**

Strategic closed loop: making the costs of destructive behavior explicit and forcing self-disintegration

The Principia framework does not assume that abuse is impossible. It is designed to ensure that any material deviation from neutrality must occur openly, can be identified and rejected, and cannot be durably institutionalized. Its force lies not in reliance on goodwill, but in making destructive conduct publicly legible and politically costly.

对权利，且不构成违约。这一权利由架构保障：SCEL 可以完全独立运行，PoPC 可以独立生成与保存，交易的合规性证明不依赖任何单一的公共平面实例。**偏离可以被尝试，但无法被强加**。

免疫三：可替代与可重建免疫，剥离运营方的制度垄断

制度目标：针对极端长期风险（如运营方失能、背离或其他情况），确保元宪章体系合法性不依赖于特定团队。其核心在于彻底剥离运营权对控制权的潜在挟持，防止暂时的运营职能异化为永久的制度性垄断。

机制实现：元宪章在制度上明确，所倡导的体系的合法性仅锚定在宪章文本、开源协议规范以及可追溯的历史证明链之中，而不依附于任何具体实现或团队。得益于协议执行的确定性，任何新的、合规的公共平面实现即可通过重放完整的历史 PoPC 与规则版本引用，即可恢复出完全一致的全局状态。**这从根源上杜绝了系统被某一利益集团俘获而彻底腐化的风险，确保了公共基础设施的永久可恢复性**。

战略闭环：破坏行为的代价显性化与自我瓦解

元宪章框架从不预设权力的自我克制。其设计的精髓在于：确保任何对中立性的实质性偏离都必须即时显性化，能够被及时识别与坚决拒斥，且绝无可能被长久地制度化。该框架的威慑力并非建立在对人性善意的天真仰赖之上，而是通过让破坏性行径变得公共可见且面临极其高昂的政治代价，从而实现对滥用行为的根本遏制与自我瓦解。

A4.3

Layering of Authority and Responsibility:
The Institutional Demarcation of Rule Sovereignty

权责分层：规则主权的制度性划界

In traditional cross-border cooperation contexts, the term rules often carries a dangerous ambiguity. Technical protocols, compliance provisions, and governance procedures are frequently grouped together under this single label. Such conceptual conflation is precisely the structural root of power overreach and responsibility evasion. When policy logic and technical logic become deeply coupled, the boundary between public protocols and sovereign will becomes blurred, and infrastructure risks evolving into an instrument of geopolitical influence.

This ambiguity inevitably leads to two extreme crises of trust. One occurs when the public technical layer attempts to overstep its role, or even adjudicate sovereign law, thereby evolving into a de facto suprasovereign authority. The other arises when a sovereign will penetrates technical details beyond its proper boundaries, transforming public infrastructure into an extension of geopolitical power. Either extreme erodes the foundational trust upon which a global cooperation system must rest.

Accordingly, the central task of this section is to provide, under the Principia framework, a clear institutional delineation of authority and responsibility. This requires not only a rigorous taxonomy of rule categories, but also a technically enforceable separation between them. Only on that basis can sovereign discretion within jurisdictions remain distinct from mechanical cooperation across jurisdictions.

A4.3.1 Institutional Delineation of the Three Major Rule Categories

Based on sources of authority, jurisdictional boundaries, and institutional purpose, the Principia framework explicitly divides rules into three mutually independent categories with clearly defined authority and responsibility.

在传统的跨境协作语境下，规则一词往往承载着一种危险的模糊性。人们常习惯于将技术协议、合规条款与治理程序笼统的归入其中。这种概念上的混淆，正是权力越界与责任推诿的结构性根源。当政策性逻辑与技术性逻辑深度耦合，公共协议与主权意志之间的界限便会变得模糊不清，基础设施也就难逃沦为地缘政治工具的宿命。

这种模糊性必然导致两种极端的信任危机：一种是公共技术层试图僭越乃至裁量主权法律，演变为事实上的超主权裁决者；另一种则是主权意志借技术细节越界渗透，将公共设施异化为地缘延伸工具。无论走向哪一个极端，都会从根基上侵蚀全球协作系统的可信底色。

据此，本节的使命是在元宪章框架下，完成对权力与责任的清晰制度性划界。这不仅要求对规则进行极其严密的分类拆解，更要求在技术架构上实现具备强制约束力的执行隔离。唯有奠定这一基础，辖区内部的主权裁量与跨辖区的协议化互认方能真正做到泾渭分明。

A4.3.1 三大规则范畴的制度性划分

元宪章体系依据权力来源、管辖边界与制度目的，将规则明确划分为以下三个互不隶属、权责清晰的范畴：

Dimension 范畴	Sovereign Rules 主权规则	Public Protocol Rules 公共协议规则	Governance Meta-Rules 治理元规则
Core definition **核心定义**	What compliance is 合规是什么	How cooperation occurs 如何协作	How rules change 如何改变规则
Authority holder **权力归属**	Each sovereign state and its authorized institutions 各主权国家及其授权机构	The SRH public plane authorized by the Principia 元宪章授权的 SRH 公共平面	Multilateral governance body jointly authorized by participants 参与方共同授权的多边治理体
Primary carrier **核心载体**	JPack (Policy-DSL rule packages) JPack（Policy-DSL 规则）	SRH protocol standards and specifications SRH 协议标准规范	Principia, governance contracts, and procedural manuals 《元宪章》、治理合约与程序手册
Nature of authority **权力性质**	Full discretion: formulation, interpretation, and execution 全权裁量：制定、解释与执行	No discretionary authority; execution only (pure syntax without business semantics) 无权裁量，仅限执行（纯语法，无业务语义）	Procedural authorization: maintaining processes and managing permissions 程序授权：维护流程与管理权限
Substantive content **实质内容**	Compliance and policy-discretion logic such as AML / CFT, capital controls, sanctions, market access rules, etc. AML / CFT、资本管制、制裁、准入等合规与业务裁量逻辑	Mechanized processes such as message formats, ordering algorithms, PoPC verification, and receipt generation 消息格式、排序算法、PoPC 验证、收据生成等机械化流程	Protocol upgrades, parameter adjustments, node admission and exit, operational supervision, and cross-site reconstruction procedures 协议升级、参数调整、节点准退、运营监督、异地重建程序
Place of execution **执行场所**	Within each jurisdiction's autonomously controlled SCEL 各国自主控制的 SCEL 内部	The SRH global distributed network SRH 全局分布式网络	Governance contracts and on-chain / off-chain governance processes 治理合约与链上 / 链下流程
Key outputs **关键产出**	Proof of Policy Compliance (PoPC) 政策合规证明（PoPC）	Global ordering and finality receipts 全局排序与最终性收据	Governance resolutions and state-change records 治理决议与状态变更记录
Core prohibitions **核心禁令**	Prohibited from directly interfering with public cooperation processes 严禁直接干预公共协作流程	Prohibited from interpreting or accessing sovereign rule logic 严禁解释或触碰任何主权逻辑	Prohibited from modifying sovereign rules beyond authorized procedures 严禁越权修改任何主权规则
Institutional relationship **制度关系**	Source of rule content and sovereign intent 规则的内容源与意志主体	Shared execution and verification layer 共享执行与验证层	Custodian of procedural integrity and institutional boundaries 程序正义与制度边界的守护者

Table 2: Classification of the Principia Rule System and Corresponding Authority–Responsibility Mapping
表2：元宪章规则体系分类与权责对应表

A4.3.2 Institutional Implementation: The Proof Interface as the Sovereign Boundary

The clear delineation of the three rule categories is ultimately realized through a carefully designed engineering interface that achieves operational isolation: the proof interface.

A4.3.2 制度实现：证明接口即主权边界

三类规则的清晰界定，最终通过一个精巧的工程接口实现物理级隔离，即证明接口。

For the sovereign side (SCEL): its responsibility is to process transactions according to domestic sovereign rules (JPack) and encapsulate the execution results into standardized and verifiable PoPC. It does not need to expose rule details or discretionary reasoning to external parties.

For the public plane (SRH): its responsibility is to verify the integrity and consistency of received PoPC and, on that basis, perform ordering and notarization. The SRH does not need to understand the rule content behind the PoPC; it only verifies that the proof was generated by a legitimate authority under the declared rule version.

For the governance bodies: their responsibility is to maintain the neutrality and procedural integrity of SRH protocols and governance processes, ensuring the reliability and credibility of the proof interface. They do not intervene in the substantive judgments performed on either side of the interface.

Accordingly, the layering of authority and responsibility is translated, at the engineering level, into a **layering of proofs**. By encapsulating complex sovereign intent into verifiable yet non-inspectable proof packages (PoPC), the system achieves a clean decoupling between sovereign discretion within jurisdictions and mechanical cooperation across jurisdictions.

Sovereign will and public protocols intersect precisely at the proof interface, while at the logical foundation they remain permanently separated and non-interfering.

A4.3.3 Conclusion: Trustworthy Cooperation Within Clear Boundaries

The layered authority–responsibility framework established here provides a workable institutional map for SSI. Sovereign jurisdictions retain authority over rule content and execution, the public layer remains limited to neutral procedural operation, and the governance layer is confined to rule maintenance and system evolution. The three are connected through proof interfaces rather than through any fusion of substantive rule content.

This structure reduces institutional ambiguity, supports minimal-trust cooperation, and allows heterogeneous sovereign rule systems to coexist within a stable shared coordination layer. Trust arises not from uniformity of rules, but from the clear allocation of authority and responsibility and from adherence to verifiable interfaces.

对主权端（SCEL）而言：其职责是根据本国主权规则（JPack）处理交易，并将执行结果封装为标准化、可验证的 PoPC。它无需向外部暴露规则细节或裁量过程。

对公共平面（SRH）而言：其职责是验证接收到的 PoPC 的完整性与一致性，并据此进行排序和公证。它无需理解 PoPC 背后的规则内容，仅需确认“该凭证由合法主体依据其声明的规则版本生成”。

对治理机构而言：其职责是维护 SRH 与治理流程的稳定与中立，确保证明接口的畅通与公信力，而非介入接口两侧的任何实质性判断。

因此，权责分层在工程层面转译为**证明分层**。系统通过将复杂的主权意志封装为可验证但不可窥视的证明包（PoPC），实现了主权内全权裁量与主权间机械协作的完美解耦。主权意志与公共协议在证明接口处精准交汇，但在逻辑底层始终互不干扰、永不融合。

A4.3.3 结论：清晰边界下的可信协作

本节确立的权责分层框架，为 SSI 提供了一份具备可操作性的制度图谱。在此框架下：主权辖区牢牢掌控规则的内容定义与执行权；公共平面严格受限于中立的程序化运行；治理层则被局限在规则维护与系统演进的范畴之内。三者之间通过证明接口进行逻辑耦合，而非在规则实体内容上进行任何形式的混同。

这种架构有效消减了制度模糊性，支撑起一种极简信任的协作模式，并允许异构的主权规则体系在稳定的共享协作层中并存。信任的产生，并非源于规则的整齐划一，而源于权力与责任的清晰界定，以及对可验证接口的绝对遵循。

A4.4

Governance Object Inventory:
Tiered Control of Variables

治理对象清单：
可变量的分级控制

The essence of governance lies in institutionalizing change itself. The core mission of this section is to end the inefficient political practice of addressing issues on a case-by-case basis by establishing a governance-object inventory with clearly defined allocations of authority and responsibility and explicit tiering. In this way, all potential future disputes are locked into predefined amendment procedures.

It is therefore necessary not only to define what may change, but also to clarify who decides and what the constitutional cost of change is, thereby eliminating-at the institutional level-the possibility that core principles could be gradually eroded through incremental modification.

A4.4.1 Tiered Amendment Framework for Governance Objects

Tiered governance is a structural requirement of system design, although the specific granularity of the tiers need not be hard-coded into the base protocol layer. According to the extent to which amendment actions affect the system's core attributes, cooperation stability, and participant rights, the governance

治理的真谛，在于赋予“变化”本身制度化。本节的核心使命旨在终结“一事一议”的低效政治博弈，通过建立一份权责明确的、分级清晰的治理对象清单，将未来所有潜在的争议锁定在预设的变更程序内。

我们不仅界定“什么能变”，更要明确由谁决定以及变更的宪制性代价，从而在制度上根除通过渐进式修改侵蚀核心原则的可能性。

A4.4.1 治理对象分级变更框架

分级治理是系统设计的刚性需求，但具体的分级粒度无需固化于代码底层。根据变更行为对系统核心属性、协作稳定性及参与方权利的影响程度，治理机制将动态适配不同的决策主体、执行流程与生效条件，确保治理结构既具备结构化的稳定性，又保留随实践演进而优化的弹性空间。

Governance Tier 治理对象层级	Governance Object 治理对象	Nature of Change 变更性质	Decision-Making Body 决策主体	Core Procedures and Constraints 核心流程与约束	Key Prohibitions 关键禁令
Principia Layer **宪章层**	Foundational constitutional elements: authority boundaries, negative prohibitions, settlement finality, and structural immunities 底层宪制要素：职权边界、消极禁令（三大禁令）、结算终局性及结构性免疫机制	Affects the legitimacy basis and trust architecture of the framework 触及框架的合法性根基与信任架构	All participating sovereigns under the highest amendment procedure 遵循最高级别修订程序的全体参与主权国	Constitutional amendment procedure; near-unanimous supermajority threshold; extended public notice period; independent review; transitional and historical-clearing arrangements **修宪程序** • 需满足近乎一致的超绝对多数门槛； • 设有延时公示期； • 需通过独立审查及历史清算安排	Must not be altered through lower-tier procedures or disguised as technical adjustment 严禁通过低层级程序进行篡改，或伪装成技术调整

Protocol Layer **协议层**	Shared protocol grammar: message formats, PoPC verification and replay rules, deterministic ordering logic 共享协议语法：消息格式、PoPC 验证与重放规则、确定性排序逻辑	Affects interoperability, consistency, and the operation of the shared layer 影响互操作性、一致性及共享平面的运行	Protocol governance committee mandated by participating sovereigns 由参与主权国授权的协议治理委员会	Formal upgrade procedure; multi-sovereign voting with defined thresholds; mandatory compatibility testing; public notice; rollback contingency requirements **升级程序** • 多主权按既定门槛投票； • 强制性兼容测试； • 公开发布预告； • 必须具备回滚预案	Must not modify Principia-level constraints or alter sovereign rule content 严禁修改元宪章层级的约束，或变动主权域内的规则内容
Operational Layer **运行层**	Operational parameters, deployment settings, and implementation-level adjustments within authorized bounds 运行参数：授权范围内的部署设置、实现细节调整及日常运维参数	Affects efficiency, maintenance, and continuity without changing constitutional or protocol meaning 影响效率与业务连续性，不改变宪制或协议内涵	Authorized operators acting under prior governance approval and supervision 在治理授权与监督下行事的被授权运营方	Bounded change procedures; full logging; multisignature authorization where required; post-change auditability; immediate reversibility where applicable **受限变更程序** • 全程留痕日志； • 必要时需多方签名授权； • 变更后具备可审计性； • 适用时需满足即时可逆性	Must not exceed delegated authority or produce de facto protocol or Principia-level change 严禁越权操作，或产生事实上的协议级与元宪章级变更

Table 3: Governance Object Tiers and Amendment Rules / 表 3：治理对象分级与变更规则表

mechanism dynamically assigns different decision-making bodies, execution procedures, and effectiveness conditions.

This design ensures that the governance structure maintains both institutional stability and sufficient elasticity to allow optimization as operational practice evolves.

A4.4.2 Institutional Safeguards: Transparency and Checks on Change

To prevent misuse of the tiered governance framework described above, the system incorporates four safeguard mechanisms.

1. **Change traceability**: Any amendment proposal at any tier, together with its discussion record, voting outcome, and execution instructions, is recorded in an immutable governance ledger and permanently preserved as part of the system's institutional history.
2. **Cross-tier interception mechanism**: The protocol layer incorporates automated validation controls. Any proposal that attempts, under the pretext of parameter adjustment, to effectively modify prohibited provisions will be automatically rejected.
3. **Cooling-off period and right of objection**: For major

A4.4.2 制度保障：变更的透明化与制衡

为防止上述分级框架不被滥用，系统内置四项保障机制：

1. **变更溯源**：任何层级的变更提案、讨论轨迹、投票结果及执行指令，均被记录在不可篡改的治理账本中，作为系统历史的一部分永久存证。
2. **越级拦截机制**：协议层内置自动化校验机制，任何试图以参数调整之名行修改禁令之实的提案将被自动拒绝。
3. **冷却期与异议权**：针对宪章层、协议层的重大变更，系统强制设置冷却期。在此期间，参与主权国可行使异议权或启动策略性退出，确保主权不被突发性的规则变更所挟持。
4. **执行与监督分离**：运营实体仅拥有操作

amendments at the Principia and protocol layers, the system mandates a cooling-off period. During this period, participating sovereign states may exercise the right of objection or initiate strategic exit procedures, ensuring that sovereignty cannot be held hostage by sudden rule changes.

4. **Separation of execution and supervision**: Operating entities possess operational authority only and hold no decision-making powers. All operational modifications must correspond to valid multi-signature authorization issued by the governance committee before they can take effect, thereby establishing a physical-level separation of authority.

Conclusion: Proceduralizing Change

Through this inventory and tiered framework, political bargaining over change is redirected into determinate procedures. The purpose is not rigidity, but the orderly evolution of the system within clear institutional boundaries.

The Principia framework distinguishes among foundational constraints, amendable technical rules, and operational parameters subject to bounded adjustment. In this way, core principles are protected against erosion while the system retains the capacity to adapt over time.

Governance therefore ceases to be a recurring struggle over immediate control and becomes a structured process for rule evolution under publicly known procedures. That procedural clarity is itself a source of institutional credibility.

权限，绝不拥有决策授权。所有运维变更必须匹配治理委员会的有效的多重数字签名方可生效，形成物理层面的权力隔离。

结论：将演进程序化

通过上述层级划分与治理清单，原本针对系统变更的政治博弈，被成功导向了确定的规范化程序。其根本目的并非追求僵化，而是为了确保系统在清晰的制度边界内实现秩序化演进。

元宪章框架严密区分了底层宪制约束、可修订的技术规则以及受限调整的运行参数。通过这种方式，核心原则得以免受侵蚀，同时确保系统具备随时代变迁而自我调适的能力。

由此，治理不再是针对即时控制权反复上演的博弈，而是在公开透明的程序下，规则实现结构化演进的过程。这种程序透明度本身，即是系统制度公信力的根本来源。

A4.5

Mechanisms for the Formulation of Protocol and Governance Rules:

How Collective Agreement Is Made Effective

协议与治理规则的制定机制：

共同约定如何落地

Earlier in this section, we established the layered allocation of authority and responsibility over rules (A4.3) and the tiered framework for amendments (A4.4). This section addresses a more precise question: within those frameworks, through what procedures are rules created and modified?

Accordingly, the core task of this section is to formalize the rule-making process as an objective and verifiable procedural pipeline. Within the SSI governance system, no single state and no operating entity possesses the privilege to define rules unilaterally. Rules arise only through formally constituted multilateral procedures.

A4.5.1 Constituting Bodies: Tripartite Separation of Power and Hard Checks-and-Balances

The allocation of rule-making authority follows the principles of aligning authority with responsibility and separating execution from decision-making. Through both juridical and institutional design, it forms a mutually constraining steady-state structure.

在本章的前半部分，我们已经确立了规则权责的分层配置（A4.3）以及变革修订的分级框架（A4.4）。而本节将回应一个更为精准的命题：在上述框架之内，规则究竟是通过何种程序得以创制与修改的?

据此，本节的核心任务是将规则制定过程正式化为一个客观且可验证的程序管道。在 SSI 的治理体系下，没有任何单一国家或运营实体拥有单边定义规则的特权。规则的产生，唯有通过符合宪制逻辑的多边正式程序方可实现。

A4.5.1 制定主体：权力的三方分离与硬制衡

规则制定权的分配，遵循权责对应与执行分离原则，通过法理与物理的双重手段形成相互制约的稳态结构：

Role Positioning 角色定位	Powers in Rule-Making 在规则制定中的权限	Core Prohibitions 核心禁令
Participating sovereigns (or their authorized institutions) **参与主权**（或其授权机构）	**Joint legislative authority**: the original source of legitimacy for the final formulation and approval of rules. Through their representatives in governance bodies, they exercise core powers such as proposal sponsorship, seconding, deliberation, and voting. **共同立法权**：构成规则最终制定与批准的权力原始来源。通过其在治理机构中的代表，行使提案附议、审议、表决等核心权力。	Strictly prohibited from placing their own will above the common procedure; strictly prohibited from authorizing operators to exercise substantive legislative authority on their behalf. 严禁将自身意志凌驾于共同程序之上；严禁授权运营者代行实质性立法权。

Governance bodies (such as various committees) **治理机构**（如各类委员会）	**Organizational and executive authority**: acting as agents executing sovereign will, responsible for organizing the rule-formation process, ensuring procedural compliance, consolidating voting outcomes, and announcing effectiveness. They possess no independent authority to create rules. **组织与执行权**：作为主权的代理执行者，负责组织制定流程、确保程序合规、汇总表决结果并宣布生效。无独立规则创设权。	Strictly prohibited from simplifying or bypassing statutory procedures; strictly prohibited from applying substantive political filtering or preference-based selection to proposal content. 严禁简化或跳过法定程序；严禁对提案内容进行实质性的政治过滤或偏好取舍。
SRH operators (technical teams) **SRH 运营者**（技术团队）	**Proposal and service authority**: based on technological evolution or operational needs, they may submit amendment proposals and are responsible for engineering implementation after effectiveness, as well as for system maintenance. **提案与服务权**：基于技术演进或运维需要，提出修改提案，并负责生效后的工程实现与系统维护。	Possess absolutely no authority to formulate or approve rules. Strictly prohibited from turning discretionary freedom in technical implementation into de facto rule modification. 绝无制定权或批准权。严禁将技术实现中的自由裁量，异化为对事实上的规则篡改。

Table 4: Allocation of Rule-Making Authority Among Participating Sovereigns,Governance Bodies, and SRH Operators
表 4：参与主权、治理机构与 SRH 运营方之间的规则制定权分配

Core principle: rule legitimacy derives from the formally expressed authorization of participating sovereigns and is confirmed through neutral procedure. Operators may propose and implement, but they do not govern.

After clarifying the division of authority and responsibility among constituting bodies, the formulation and amendment of rules must follow a standardized and end-to-end auditable procedural pipeline (see Volume B of the Principia framework). This process encompasses key stages such as proposal submission, public notice and deliberation, multilateral voting, technical acceptance, and final announcement. In this way, the creation of any rule undergoes sufficient public discussion and rigorous technical verification, ensuring that its execution is not subject to discretionary human intervention.

A4.5.2 Effectiveness Mechanism: From Voting Thresholds to State-Based Triggering

Within the SSI framework, rule activation is state-based rather than command-based. A rule takes effect only when all predefined conditions have been satisfied: verifiable voting thresholds, closure of notice and testing periods, and completion of technical validation and security lock-in. This includes successful acceptance testing, deployment readiness, rollback preparation, and monitoring activation.

At the protocol level, these conditions may not be bypassed in the name of urgency or exceptional necessity; long-term system robustness takes precedence over ad hoc efficiency.

核心原则：规则的合法性源于各主权方正式表达的意志授权，并经由中立程序予以确认。运营方仅拥有提案权与执行权，而不具备治理权。

在明确制定主体的权责分工后，规则的制定与变更必须遵循一套标准化的、全链可审计的程序流水线（详见元宪章卷 B）。该流程涵盖提案提交、公示审议、多边表决、技术验收及最终公告等关键阶段，确保任何规则的产生都经历充分的公共讨论与严格的技术验证，其执行过程不受人为意志干扰。

A4.5.2 生效机制：从表决阈值到状态触发

在 SSI 框架下，规则的激活采用基于状态而非指令的逻辑。只有当所有预设条件均得到满足时，规则方可生效。这些条件包括：可验证的投票门槛达标、公示期与测试期届满，以及技术验证与安全锁定的完成。具体涵盖了验收测试的通过、部署就绪性的确认、回滚预案的完备以及监控机制的激活。

在协议底层，任何实体均不得以紧急情况或特例需求为由绕过这些法定条件。系统的长期稳健性，始终优先于权宜之计下的临时效率。

A4.5.3 Hard Constraints: The Non-Negotiable Negative List

All procedures are placed under a final red-line constraint: no rule formulation or amendment proposal may, in any form, breach or weaken the Principia core principles and the three prohibitions established in Section A4.2. The system embeds an automated compliance pre-screening mechanism: before a proposal enters the public notice phase, if its content is detected as potentially touching the negative list, such as prohibited interpretation, prohibited execution, or prohibited ownership - it will be automatically intercepted and forcibly flagged, requiring escalation to the constitutional revision procedure for deliberation.

This means that any attempt to covertly grant SRH discretionary authority, execution power, or asset authority through protocol upgrades will be institutionally identified and blocked at the very first procedural stage. The negative list is not a moral appeal, but a hard constraint embedded in the process engine.

Conclusion: Rule of Rules Arises from Rule of Procedure

By establishing checks among actors, process-based governance, conditional activation, and negative-list constraints, the SSI framework ensures that rule formation is governed through transparent and verifiable procedures. Rules arise not from unilateral authority, but from formally constrained multilateral process.

This creates a governance structure in which the creation, amendment, and activation of rules are proceduralized, auditable, and resistant to discretionary intervention.

A4.5.3 刚性约束：不可逾越的负面清单

所有流程，均被置于一道最终的红线约束之上：任何规则制定或变更提案，均不得以任何形式突破或削弱 A4.2 节所确立的元宪章核心原则与三项禁令。系统内置自动化的合规预审机制：在提案进入公示前，若检测到其内容可能触及禁止解释、禁止执行、禁止所有等负面清单，该提案将被自动拦截并强制标记，要求提升至“重宪程序”进行审议。

这意味着，试图通过协议升级来变相赋予 SRH 裁量权、执行权或资产权的企图，将在程序的第一步就被制度性地识别和拦截。负面清单不是道德层面的倡议，而是写进流程引擎的硬性电路。

结论：规则之治，源于程序之治

通过在执行主体间建立制衡机制、实施过程化治理、设定条件激活以及负面清单约束，SSI 框架确保了规则的生成始终受控于透明且可验证的程序。规则的诞生，并非源于任何单边权威的意志，而是源于受到正式约束的多方协作进程。

由此，一个全新的治理结构得以确立：在该结构中，规则的创设、修订与激活均实现了程序化与可审计化，并具备抵御任何裁量性干预的内生抗性。

A4.6

Operational Stewardship of the Sovereign Relay Hub:

Multilateral Access, Power Separation, and Ultimate Substitutability

主权中继枢纽的运营托管：

多边准入、权力剥离与终极可替代性

Within a multi-sovereign collaborative governance architecture, operational authority is the institutional objective most easily coveted. Once infrastructure operators gain room to interpret rules, a neutral technical platform tends to slide toward becoming a geopolitical lever. This is not a hypothesis, but a historical trajectory repeatedly borne out by cross-border infrastructures.

Accordingly, this section adopts a core axiom: operational authority over the SRH must be structured as a public service function, not as a form of governing power. Operators may possess the technical capacity required to run the protocol, but they possess no substantive discretionary authority. Their role is confined to verifiable mechanical execution.

The starting point of this governance logic is not to seek perfectly reliable operators, but to construct a constraint framework in which the system remains secure even when operators are not trustworthy. For strategic infrastructure underlying global settlement, entrusting system security to the moral self-discipline of operators is itself an unacceptable systemic risk.

A4.6.1 The Authorization Logic of Operational Authority: Delegated Agency Rather Than Inherent Power

The operational authority of the SRH is not an extension of sovereign power, but a delegated functional mandate established under the Principia framework. Its institutional character is defined by three conditions: it derives solely from explicit authorization rather than historical convention or de facto control; it is limited to technical execution and routine operations and excludes discretion, interpretation, and rule-making; and it remains expressly

在多主权协同的治理架构中，运营权是最容易被觊觎的制度目标。基础设施的运营者一旦获得规则解释空间，中立的技术平台便会滑向地缘杠杆。这不是假设，而是被无数跨境基础设施反复验证过的历史轨迹。

据此，本节确立了一项核心公理：SRH 的运营权必须被构建为一种公共服务职能，而非一种治理权力。运营方固然拥有运行协议所必需的技术能力，但其绝不具备任何实质性的自由裁量权。其角色被严格限制在可验证的机械化执行范畴之内。

这套治理逻辑的出发点，不是去寻找完美可靠的运营者，而是构建一个即使运营者不可信，系统依然安全的约束框架。对于事关全球结算的战略基础设施而言，将系统安全寄托于运营者的道德自律，就是不可接受的系统性风险。

A4.6.1 运营权的授权逻辑：派生性代理而非固有权力

SRH 的运营权并非主权权力的延伸，而是元宪章框架下的一种委托职能授权。其制度特性具体体现为：运营权力唯有通过明确且正式的法律授权方可产生，严防任何基于历史惯例或对基础设施的控制而形成的非法扩张；其行使

revocable under predefined conditions and procedures. Operational authority is therefore always derivative, bounded, and temporary.

Spectrum Design of Operating Models

To accommodate political environments at different stages of development, the Principia provides a spectrum of operating models adapted to multiple stages, all operating on the same constitutional foundation:

范围被严密锁死在技术执行与日常运维的逻辑内，在物理与法理上均被剥夺了涉及裁量、解释或规则制定的任何可能；在预设的触发条件与程序下，该授权始终处于明确的可撤销状态。

基于上述逻辑，运营权在本质上始终是派生的、受限的且临时性的。

Operating Model 运营模式	Applicable Stage 适用阶段	Organizational Form 组织形态	Governance Core 治理核心
Transitional Custodial Operation **阶段性托管运营**	**Launch phase** **启动期**	Temporarily managed by institutions such as the BIS, the IMF, or a technically credible foundation recognized by multiple sovereigns 由如国际清算银行、IMF 或具备公信力多主权认可的技术基金会代管	Mandatory inclusion of a sunset clause clearly defining the custodial period (e.g., 3–5 years); upon expiration, it must transition, thereby strictly preventing transitional arrangements from becoming long-term monopolies 强制引入日落条款，明确托管期限（如 3-5 年），到期必须转型，严防过渡安排变为长期垄断
Regulated Consortium Operation **受监管联盟运营**	**Ecosystem expansion phase** **生态扩展期**	An operating consortium composed of regulated market infrastructure institutions 由受监管的市场基础设施机构所组成的运营联盟	Introduces a multi-sovereign supervisory committee with penetrative audit rights, compliance inspection powers, and recommendatory dismissal powers; commercial institutions are responsible for efficiency, while the sovereign collective is responsible for compliance 引入多主权监管委员会，拥有穿透式审计权、合规检查及建议罢免权；商业机构负责效率，主权集体负责合规
Joint Multi-Sovereign Operation **多主权联合运营**	**System maturity phase** **体系成熟期**	A non-profit international public utility jointly established by the principal participating sovereigns 由主要参与主权共同组建的非营利性国际公共事业机构	Composed of representatives appointed by each sovereign, using one-country-one-vote or weighted voting, with supermajority decisions (e.g., 2/3) to block domination by any single major power 由各主权委派代表组成，实行一国一票或加权投票机制，通过超多数（如 2/3）决策封堵单一大国主导

Table 5: Spectrum of SRH Operating Models / 表 5：SRH 运营模式谱系表

The core of this spectrum design lies in the following: regardless of the stage or model adopted, the derivative, limited, and revocable nature of operational authority remains unshakable. The evolution of models is merely a change in organizational form, not a change in the nature of power.

Beyond authorization and model choice, the framework imposes continuity constraints on operational authority (see Volume B of the Principia). Term limits and rotation reduce entrenchment risk; standardized exit and handover procedures make transfer verifiable; and emergency substitution mechanisms protect continuity in cases of incapacity or disqualification. Together, these arrangements keep operational authority in circulation rather than allowing it to harden into privilege.

运营模式的谱系设计

为兼容不同发展阶段的政治环境，元宪章提供了多阶段适配的运营模式谱系，所有模式均在同一套宪章底座上运行。

这一谱系设计的核心在于：无论处于何种阶段、采用何种模式，运营权的派生性、限定性、可撤销性始终不可动摇。模式的演进只是组织形式的变化，而非权力性质的改变。

在明确授权逻辑与模式谱系之后，系统进一步

A4.6.2 Physical Constraints on Operators: Technical Execution Is the Whole

The mechanical constraint of "input–process–output"

At the implementation level, the operator function is reduced to a deterministic processing pipeline:

[Compliant transactions + PoPC proofs] → [SRH protocol processing] → [Ordering results + finality receipts]

This architecture locks operators into three rigid constraints: they have no authority to modify inputs and may not unlawfully reject, tamper with, or selectively delay any transaction that complies with the prescribed format; they have no authority to alter algorithms, and the execution environment must strictly follow the open-source protocol code and remain verifiable throughout; they have no authority to interpret outputs, and all results must strictly follow standardized protocol specifications, with no discretionary annotations attached.

Triple technical lockdown mechanism

To realize the above constraints, the system deploys three hard lines of defense at the foundational layer:

(1) **Protocol consistency proofs**: SRH nodes, upon startup, must generate protocol consistency proofs demonstrating that their running code is fully identical to the open-source reference implementation. These proofs are generated via TEE (Trusted Execution Environments) or zero-knowledge proofs and are automatically committed on-chain every hour for public verification by network participants at any time.

(2) **Verifiable process logs**: all processing operations generate structured execution logs containing input commitments, intermediate-state proofs, and deterministic paths. These logs are periodically published, enabling independent third parties to conduct full audits through replay.

(3) **Automatic rejection of unauthorized operations**: the protocol layer embeds detectors for overreach operations, blocking in real time any attempt to access raw data (such as original transaction contents), unlawfully invoke unauthorized functions (such as rule-interpretation engines), or tamper with protocol parameters. Through WASM sandboxes or hardware-based formal verification, the executable instruction set is tightly locked within the scope prescribed by the protocol.

Institutional position: entrusted executor of the protocol

为运营权设定了动态约束机制（详见元宪章卷B）。通过任期制与轮换机制防止利益固化，通过标准化的退出与移交程序确保权力更迭的仪式化与可验证，并通过紧急接管机制防范运营者失能或失格。这些制度安排共同确保运营权始终处于受控的流动状态，不会因时间推移而异化为永久特权。

A4.6.2 运营者的物理约束：技术执行即全部

"输入 - 处理 - 输出"的机械约束

在工程实现层面，运营方职能被简化为一个确定性的处理流程：

[合规交易 + PoPC 证明] → [SRH 协议处理] → [排序结果 + 最终性收据]

这一架构将运营者锁定在三重刚性约束之中：无权修改输入，不得非法拒绝、篡改或选择性延迟任何格式合规的交易；无权改变算法，执行环境必须严格遵循开源协议代码且全程可验证；无权解释输出，所有结果必须严格遵循标准化协议规范，不得附加任何带有裁量色彩的注释。

三重技术锁死机制

为了实现上述约束，系统部署了三道硬性防线：

(1) **协议一致性证明：**SRH 节点启动时必须生成协议一致性证明，证明其运行代码与开源参考实现完全一致。该证明依托可信执行环境或零知识证明生成，每小时自动上链，供全网参与者随时公开核验。

(2) **过程可验证日志：**所有处理操作均生成含输入承诺、中间状态证明及确定性路径的结构化执行日志。这些日志定期公开发布，支持独立第三方通过重放操作进行全量审计。

The operator is therefore best understood as an entrusted executor of the protocol. Its actions must remain predictable, verifiable, and substitutable. Whatever technical form implementation takes over time, the constraint remains the same: execution may evolve, but operational authority may not expand into governance.

A4.6.3 Value Neutrality: Stripping Away Profit Incentives and Power Expansion

To reduce the risk that SRH operation becomes a channel for power expansion, the framework limits the financial incentives attached to operation and prevents their conversion into institutional control.

Cost recovery rather than profit creation: The financial model should be oriented toward cost recovery rather than unrestricted profit extraction. Fees should be transparently tied to verifiable operating costs, subject to public audit, and structured so that financial contribution cannot be converted into control over the shared layer.

Extreme value-neutral design: At the operational level, this neutrality is reinforced by three exclusions: the SRH holds no assets on its own balance sheet, accumulates no investable liquidity pool, and extends no credit or guarantee function. Operation therefore does not create an independent financial center.

Incentive misalignment: reputation as the ultimate collateral: Incentive design should reward continuity, compliance, and operational reliability rather than expansion of function or influence. The aim is not to moralize operators, but to align their incentives with long-term system stability.

A4.6.4 Institutional Implementation: From Principles to Executable Contracts

Operational contracts as annexes to the Principia

Each operational authorization contract should function as a binding annex under the Principia framework. It should translate governance constraints into verifiable technical and operational obligations, while specifying audit rights, supervisory powers, and breach conditions.

A multi-dimensional networked oversight system

Operator supervision should not rely on any single oversight point. It should instead combine multilateral supervisory review, independent technical audit, and real-time network monitoring,

(3) **越权操作自动拒绝：**协议层内置越权操作检测器，实时封堵任何试图访问原始数据（如原始交易内容）、非法调用非授权函数（如规则解释引擎）或篡改协议参数的操作。通过 WASM 沙箱或硬件形式化验证，将可执行指令集严密锁死在协议规定的范畴内。

制度定位：协议的受托执行者

因此，运营方最准确的定位应当被理解为协议的受托执行者。其所有行为必须保持高度的可预测性、可验证性与可替代性。无论技术实现手段随时间如何演进，核心约束始终如一：执行方式可以进化，但运营权绝不可向治理权扩张。

A4.6.3 价值中性：剥离利润诱惑与权力扩张

为规避 SRH 的运营演变为权力扩张的通道，本框架严格限制了与运营挂钩的财务激励，并严防其转化为制度性的控制权。

成本回收而非利润创收：财务模型应导向成本回收，而非无节制的利润攫取。各项费用的设定须透明地锚定在可验证的运营成本之上，并接受公共审计。其结构设计必须确保：任何财务上的贡献均无法兑换为对共享平面的控制权。

极致价值中立设计：在运营层面，这种中立性通过三大排除予以强化：SRH 自身资产负债表不持有任何资产，不积聚任何可投机性流动的资金池，亦不提供任何信用背书或担保职能。因此，运营行为绝不会催生出一个独立的金融中心。

激励错位修复，声誉作为终极抵押品：激励机制的设计应奖赏系统的连续性、合规性与运行

with each layer cross-verifying the others.

- **The multi-sovereign supervisory committee** is responsible for periodically reviewing operational compliance.
- **Independent technical audit institutions** continuously verify protocol consistency proofs.
- **The participating-node monitoring network** detects operational anomalies in real time.

Tiered breach response

- **Minor violations**: public warning and mandatory remediation within a defined period.
- **Serious violations**: financial penalty, heightened supervision, or curtailment of the current operating term.
- **Fundamental breach**: immediate initiation of removal procedures and emergency substitution, with legal liability pursued where applicable.

All determinations of violation must be anchored in verifiable and objective proof, rather than in any form of subjective conjecture.

Conclusion: The SRH May Be Operated, But It Cannot Be Ruled

The operational design set out here shows that authority over the SRH can be delegated, exercised, and constrained without being allowed to harden into governing power. System stability does not depend on perfect operators, but on a framework in which operator discretion remains bounded, verifiable, and replaceable.

Operational authority is therefore service-based rather than sovereign in character. Its legitimacy lies in constrained execution, not in independent power, and its long-term value lies in transparent substitutability. The SRH may be operated, but it cannot be ruled.

可靠性，而非功能的盲目扩张或影响力的渗透。其目的并非对运营方进行道德感化，而是通过机制设计，使其自身利益与系统的长期稳健性实现深度绑定。

A4.6.4 制度实现：从原则到可执行合约

作为元宪章附件的运营契约

每一份运营授权契约均应作为元宪章框架下具有法律约束力的附件。契约须将治理层的约束条款转译为可验证的技术与运维义务，并明确审计权、监督权及违约判定条件。

多维网状监督体系

对运营方的监管不应依赖于任何单一监管点。相反，它应当结合多方主权监管审查、独立技术审计以及实时网络监测，实现各层级间的交叉验证：

- **多主权监督委员会**负责定期审查运营合规性。
- **独立技术审计机构**持续验证协议一致性证明。
- **参与节点监控网络**实时检测运营异常。

阶梯式违约响应

- **轻微违规**：触发全网公开警告，强制限期整改。
- **严重违规**：实施经济处罚，并伴随监管升级或缩短当前的运营任期。
- **根本性违约**：立即启动罢免程序与紧急接管，并在适用情况下依法追究法律责任。

所有违规判定必须锚定于可验证的客观证明，而非任何形式的主观臆断。

结论：SRH 可以被运营，但不能被统治

上述运营架构设计表明：对 SRH 的授权、行使与约束，均可在严密的制度框架内完成，而绝不允许其固化为一种统治权力。系统的稳定性并不依赖于完美的运营方，而在于确保运营方的裁量权始终处于受限、可验证且可替代的状态。

由此可见，运营权的本质是服务性而非主权性。其合法性根植于受限的执行过程，而非独立的权力意志；其长期价值则在于透明的可替代性。SRH 可以被运营，但绝不可被统治。

A4.7

Institutional Immunity:
Constraint Mechanisms Against Long-Term Deviation

The core governance logic of the Sovereign Relay Hub (SRH) lies in this: an architecture grounded in physical proofs, mathematical logic, and institutional game dynamics, rather than reliance on operator goodwill.

This section decomposes the abstract commitment of "correctness" into three insurance mechanisms that are independently verifiable, engineerable in practice, and institutionally guaranteed:

- **First line: verifiability** - making correctness or incorrectness a publicly recomputable mathematical fact.
- **Second line: substitutability** - ensuring that incapacitated or disqualified operators cannot hijack the global order.
- **Third line: accountability** - ensuring that every deviation leaves irrefutable legal proof.

制度免疫：
长期偏离的约束机制

SRH 的核心治理逻辑归结于此：其架构并非锚定于对运营方主观意愿的信任，而是扎根于物理证明、数学逻辑以及制度博弈的耦合。

本节将“正确性”这一抽象承诺，拆解为三道可独立验证、可工程落地、且具备制度保障的保险机制：

- **第一道：可验证**，让正确与否成为可公开复算的数学事实。
- **第二道：可替代**，让失能或失格的运营者无法绑架全局秩序。
- **第三道：可追责**，让每一次偏离都留下不可抵赖的法律证明。

Within this architecture, “correctness” is proven, and “neutrality” is enforced.

A4.7.1 Verifiability: Placing Operational Behavior Before a “Mathematical Court”

Under the Principia framework, correctness is treated as a re-computable problem. Any sovereign authority, audit institution, or qualified third party must be able to reproduce the critical decision processes of the SRH and derive results identical to those of the original execution.

(1) Verifiability of Outputs: Finality Receipts as Proof

Every settlement confirmation issued by the SRH generates a standardized finality receipt. This is not a simple status marker, but a proof object that anchors facts through the following fields. Any sovereign party may perform independent verification: given a transaction hash, any sovereign can synchronize the global state tree from the SRH.

在此架构下，“正确”不是被承诺的，而是被证明的；“中立”不是被声明的，而是被强制执行的。

A4.7.1 可验证：将运营行为置于“数学法庭”

元宪章体系将“正确性”彻底转化为数学性问题：任何主权、审计机构、第三方观察者，均可独立复现 SRH 的全部关键决策过程，并推导出与原始执行位级一致的结果。

(1) 输出的可验证性：最终性收据即证明

SRH 的每一笔结算确认都生成标准化的最终性收据。这并非一个简单的状态标记，而是通过以下字段锚定事实。各主权方均可进行独立验证：只要给定一笔交易哈希，任何主权都能从 SRH 同步全局状态树：

Field 字段	Purpose 用途	Verification Method 验证方式
Transaction hash 交易哈希	Locks the original input 锁定原始输入	Compare against the original transaction payload 与交易原始载荷进行比对
Global ordering number 全局排序序号	Determines temporal position 确定时序位置	Check the monotonic increase of the global sequence number 检查全局序号的单调递增性
PoPC verification-result commitment PoPC 验证结果承诺	Records the compliance verification conclusion 记录合规验证结论	Independently replay the PoPC verification logic for reconciliation 独立重放 PoPC 校验逻辑进行对账
Policy snapshot hash 策略快照哈希	Locks the JPack version in force at the time of execution 锁定执行时的 JPack 版本	Cross-check against the sovereign registry 与主权注册表进行交叉比对
SRH digital signature SRH 数字签名	Anchors operator identity 运营者身份锚定	Verify signature validity 验证签名有效性
Merkle path proof 默克尔路径证明	Confirms the receipt’s position in the global state tree 收据在全局状态树中的位置	Verify downward from the global root hash 从全局根哈希向下验证

Table 6: SRH Finality Receipt Fields and Verification Table / 表 6：SRH 最终性收据字段与验证表

(2) **Verifiability of the Process: Deterministic Replay**

Merely proving that "the final conclusion is such" is not sufficient; it is also necessary to prove that "the processing itself was compliant". To this end, the SRH protocol mandates replayability of the execution path: the PoPC verification process for each transaction, under the same JPack version and input environment, must produce bit-level identical outputs. SRH operators must periodically (for example, per block) publish execution-trace summaries covering triggered rules, intermediate-state hashes, and decision branches. Sovereigns may use the open-source replay tool (srh-replay) to reconstruct the complete compliance verification process in their local environments. If an SRH operator attempts to tamper with conclusions, mathematical facts will immediately expose the inconsistency.

(3) **Verifiability of the Code: Protocol Consistency Proofs**

The core SRH code must be fully open-source, version-traceable, and reproducibly buildable. Each running node must generate protocol consistency proofs: based on Trusted Execution Environments (TEE) or zero-knowledge proofs, it must prove that the hash of the currently running binary code exactly matches the open-source reference implementation. These proofs are periodically and automatically committed on-chain for network-wide verification. Any node deviating from the official implementation will have its outputs automatically identified and rejected by other nodes across the network.

Verifiability demotes operators from arbiters of truth to mere carriers of facts. Operators lose the privilege of asserting "this is the correct result", because correctness is no longer their subjective claim, but an objective mathematical fact that any sovereign can independently verify. This means that **even if you do not trust the SRH operator, you can still trust the SRH's outputs**.

A4.7.2 Substitutability: Dismantling the Operator's "Single-Point Hijack"

In the governance design of the SRH, we must soberly identify the system's most fragile attack surface. Historical experience shows that operators rarely dare to tamper directly with compliance conclusions, because such attacks are excessively explicit and would immediately trigger the vigilance and collective resistance of all participants.

The real threats are often concealed in "delay" and "service obstruction". A malicious operator is more likely to exploit its func-

(2) **过程的可验证性：确定性重放**

仅仅证明"最终结论如此"是不够的，还必须证明"处理过程合规"。为此，SRH 协议强制要求执行路径具备可重放性：每笔交易的 PoPC 校验过程，在相同的 JPack 版本与输入环境下，必须产生位级一致的输出。SRH 运营者须定期（如每区块）发布执行轨迹摘要，涵盖触发规则、中间状态哈希、决策分支。主权可使用开源重放工具（srh-replay），在本地环境中重建完整的合规验证过程。若 SRH 运营者试图篡改结论，数学事实将立即暴露其不一致性。

(3) **代码的可验证性：协议一致性证明**

SRH 的核心代码必须是完全开源、版本可追溯且构建可复现。每个运行节点必须生成协议一致性证明：基于可信执行环境（TEE）或零知识证明，证明当前运行的二进制代码哈希值与开源参考实现完全一致该证明定期自动上链，供全网核验。任何偏离官方实现的节点，其产生的输出将被全网其他节点自动识别并拒绝。

可验证性将运营者从真相的裁决者降维为事实的搬运工。运营者失去了声称"这就是正确结果"的特权。因为正确与否不再是它的主观主张，而是任何主权均可自行验证的客观数学事实。这意味着：**即使你不信任 SRH 的运营者，你依然可以信任 SRH 的输出**。

A4.7.2 可替代性：解构运营者的"单点绑架"

在 SRH 的治理设计中，我们必须冷静地识别系统最脆弱的攻击面。历史经验表明：运营者极少会冒天下之大不韪直接篡改合规结论，因为这种攻击过于显性，会瞬间触发所有参与方的警觉与集体抵制。

tional position to carry out the following covert disruptions:

- **Selective delay**: manipulating processing order to fast-track transactions from certain countries while deliberately postponing others.
- **Ambiguous timeouts**: assigning unreasonable queue priorities to specific transactions, keeping them continuously in a "pending" state.
- **Silent dropping**: claiming that certain transactions were not received while refusing to provide verifiable proof of rejection.
- **Feigned outages**: suspending service at politically sensitive moments or critical financial windows under the pretext of "technical upgrades" or "system maintenance".

The common feature of **these actions is that they do not violate any verifiable correctness condition, yet they substantially undermine the system's fairness and availability**. The operator does not need to modify protocols or tamper with proofs; merely by exploiting its monopolistic position as a "mandatory checkpoint", it can achieve political objectives.

Substitutability is the only antidote to delay attacks. If the SRH cannot be unlocked technically, falls into deadlock at the governance level, or imposes excessive switching costs, then operator arrogance and negligence cannot be effectively disciplined. In such cases, users can only endure, not resist.

The design objective of substitutability is to **establish that no SRH instance possesses either the legal or technical basis for single-point monopoly**. When an operator becomes incapacitated or disqualified, any participant has a path, a procedure, and an incentive to switch to a brand-new, clean SRH instance. The following three layers of architecture support this goal:

First layer: substitutability of state - the proof chain as the global state

The core asset of the SRH is not servers or private databases, but the immutable and fully migratable proof chain.

- **Polycentric data ownership**: all critical outputs generated by the SRH (finality receipts, PoPC verification records, governance logs) are cryptographically anchored on-chain and do not depend on any particular operator's storage.
- **Transparency of global state**: the global state is not the operator's private property, but a mathematical fact that any sovereign party can archive, index, and replay.

真正的威胁往往隐蔽在"拖延"与"服务阻断"之中。一个怀有恶意的运营者，更倾向于利用职能便利，实施以下隐性破坏：

- **选择性延迟**：通过操纵处理时序，优先放行某些国家的交易，而刻意推迟其他国家的交易。
- **模糊化超时**：对特定交易设置不合理的排队优先级，使其持续处于"待处理"状态。
- **静默丢弃**：声称未收到特定交易，却拒绝提供可验证的拒绝证明。
- **假性故障**：在政治敏感或金融交易的关键时刻，以"技术升级"或"系统维护"为名暂停服务。

这些行为的共同特征是：**它们并未违反任何可验证的正确性条件，却实质性地破坏了系统的公平性与可用性**。运营者无需要修改协议、篡改证明，只需要利用其作为"必经关卡"的垄断地位，就能实现政治目的。

可替代性是破解"拖延攻击"的唯一解药。如果 SRH 在技术上无法锁定、在治理上陷入僵局、或在切换成本上过于昂贵，那么运营者的傲慢与怠工就无法被有效惩戒。在这种情况下，用户只能忍受，无法反抗。

可替代性的设计目标是：**确立任何 SRH 实例都不具备单点垄断的法理与技术基础**。当运营者失能或失格时，任何参与者都有路径、有程序、有动力切换至一个全新的、洁净的 SRH 实例。以下是支撑这一目标的三重架构：

第一重：状态的可替代性，证明链即全局状态

SRH 的核心资产不是服务器或私有数据库，而是那条不可篡改、可完整迁移的证明链。

- **数据权属多中心化**：SRH 产生的所有

- **Technical implementation**: the SRH protocol mandates that all critical proofs be written into a multi-party-backed cross-chain transaction archive. Operators cannot hold historical proofs hostage to coerce any participant.

Second layer: substitutability of implementation - protocol as standard, code as tool

The second layer is substitutability of implementation. Legitimacy must attach to open protocol specifications rather than to any single development team or codebase. The framework should therefore support multiple independently developed compliant implementations, so that no single code lineage can monopolize protocol evolution or system operation.

Third layer: substitutability of instance - rebuilding is restoration

The third layer is substitutability of instance. Where an existing SRH instance materially deviates from the Principia framework, participants must have a lawful path to instantiate a new compliant instance, inherit the relevant proof-based state, and determine migration in accordance with predefined procedures. The aim is not fragmentation, but credible replacement.

This design does not encourage fragmentation; it creates a credible replacement option. Its deterrent effect lies in making sustained unfairness incompatible with durable control. Where operators can be replaced without systemic rupture, incentives for obstruction are materially reduced.

A4.7.3 Accountability: Making Every Deviation an Irrefutable Public Record

I. **Redefining "Accountability":**

The Principia framework defines accountability as follows: **any critical operation - especially any behavior that deviates from the predefined ideal state-must generate, in real time, non-repudiable and publicly auditable event records**. Here, accountability is no longer an administrative procedure for discovering problems, but a proof-exposure mechanism that is necessarily triggered the moment a problem occurs.

II. **Mandatory Trace Retention:**

Deviation Equals Exposure: The SRH protocol mandatorily requires that the following five categories of critical events generate standardized, signed audit records:

1. **Rejection events**: Any transaction rejected by the SRH,

关键输出，（最终性收据、PoPC 验证记录、治理日志），均以加密形式锚定在链上，不依赖于任何特定运营者的存储。

- **全局状态的透明化**：全局状态并非运营者的私有财产，而是可被任何主权方归档、索引并重放的数学事实。
- **技术实现**：SRH 协议强制要求将所有关键证明写入多方备份的跨链交易档案库。运营者无法通过挟持历史证明以要挟任何参与者。

第二重：实现的可替代性，协议即标准，代码即工具

SRH 的合法性必须锚定于开放的协议规范，而非任何特定的开发团队或代码库。因此，框架必须支持多种独立开发的合规实现方案，确保没有任何单一的代码谱系能够垄断协议的演进或系统的运行。

第三重：实例的可替代性，重建即恢复

当现有的 SRH 实例在实质上偏离了元宪章框架时，参与方必须拥有一条法定路径来实例化一个新的合规节点，继承相关的基于证明的状态，并依据预设程序完成迁移。此举之目的并非制造分裂，而是实现公信力更替。

上述设计并非在鼓励体系瓦解，而是确立了一项具备公信力的更替选项。其威慑力在于：使得持续的制度不公与长期的系统控制变得互不兼容。当运营方可以在不导致系统崩溃的前提下被撤换时，其通过技术手段进行阻碍行为的动机将从根本上被削弱。

A4.7.3 可追责：让每一次偏离都成为不可抵赖的公开记录

一．**重新定义“可追责”**

including PoPC verification failure, must record the rejection-reason code, the relevant rule hash, the timestamp, and the node signature. Silent rejection without a verifiable reason is prohibited.

2. **Delay events**: When a transaction remains in the mempool beyond the predefined threshold, the system must record the transaction hash, entry time, current status, and expected processing time. Indefinite suspension without status disclosure is prohibited.
3. **Operating-mode switch events**: Any change in operating mode triggered by technical fault or force majeure must be publicly recorded, including the type of switch, effective timestamp, scope of impact, and recovery path. Such changes may affect execution environment or service scope, but may not alter rule semantics or the determinacy of existing settlement results.
4. **Parameter change events**: Any protocol-parameter adjustment, including changes to fee rates or timeout windows, must be linked to the change content, the effective block, the governance-proposal hash, and the voting result. Unauthorized emergency adjustment is prohibited.
5. **Operational transition events**: Team handovers, key rotations, and system migrations must preserve a complete transfer plan, execution logs, and witness signatures. Non-public transfer of operations without audit trace is prohibited.

III. Independent Reverification Capacity at the Audit Layer

These records are not private operational logs, but structured proof records open to the regulatory and observer layers. The Principia authorizes the following entities to exercise independent audit rights:

- **Sovereign regulatory authorities**: may precisely retrieve the complete audit chain relevant to their jurisdiction.
- **Multilateral supervisory committees**: may initiate random sample audits to verify consistency between event records and on-chain proofs.
- **Certified third-party audit institutions**: upon committee authorization, may conduct penetrative compliance audits.

Audit is no longer a privilege, but a universal system capability. Any participant with the necessary technical capacity may synchronize logs and perform independent replay, thereby determining whether unrecorded rejections, inadequately explained delays, or unauthorized mode switches exist.

本元宪章体系将可追责性定义为：**任何关键操作，尤其是偏离预设理想状态的行为，都必须实时生成不可抵赖、可公开审计的事件记录**。在这里，追责不再是发现问题的行政程序，而是问题发生时必然触发的证明暴光机制。

二．强制留痕：偏离即曝光

SRH 协议强制要求，以下五类关键事件必须生成标准化的签名审计记录：

1. **拒绝类事件**：任何被 SRH 拒绝的交易（包括 PoPC 验证失败），均须记录拒绝原因码、相关规则哈希、时间戳及节点签名。严禁任何无核查原因的静默拒绝。
2. **延迟类事件**：当交易在内存池中的驻留时间超过预设阈值时，系统必须记录交易哈希、进入时间、当前状态及预期处理时间。严禁任何无状态披露的无限期挂起。
3. **运行模式切换事件**：任何因技术故障或不可抗力触发的运行模式变更均须公开记录，包括切换类型、生效时间戳、影响范围及恢复路径。此类变更仅限影响执行环境或服务范围，绝不可篡改规则语义或既有结算结果的确定性。
4. **参数变更事件**：任何协议参数的调整（包括费率变更或超时窗口设置），必须关联变更内容、生效区块、治理提案哈希及投票结果。严禁任何未经授权的紧急调整。
5. **运维交接事件**：团队更迭、密钥轮换及系统迁移必须保留完整的交付计划、执行日志及见证人签名。严禁任何无审计追踪的非公开运维移交。

三．审计层的独立复核能力

IV. **The Institutional Closed Loop of Accountability:**

The endpoint of accountability is institutionalized sanctioning consequences, applied in a tiered manner according to the degree of violation:

- **Minor violations**: publicly recorded across the network, with mandatory rectification within a prescribed period and issuance of a formal explanation.
- **Moderate violations**: forced shortening of the operational term and initiation of competitive reauthorization procedures.
- **Major violations**: immediate triggering of removal procedures, permanent loss of operational qualifications, and referral for legal prosecution.

The core principle is this: **determinations of violation do not rely on subjective judgment, but on verifiable proof packages**. A proof package containing complete audit trails, on-chain hash cross-checks, and independent replay results carries probative force far exceeding the investigative conclusions of any institution.

A4.7.4 Correctness Is a Product of Institutional Design

Taken together, these mechanisms form the immunity architecture of the SRH. Verifiability, substitutability, and accountability operate across detection, constraint, and attribution, ensuring that correctness can be checked, defended, and recorded throughout system operation.

这些记录并非私有的运维日志，而是向监管层与观察层开放的结构化证明。元宪章授权以下实体行使独立审计权：

- **主权监管机构**：可精准调取与其辖区相关的完整审计链条。
- **多边监督委员会**：可随机发起抽样审计，验证事件记录与链上证明的一致性。
- **认证第三方审计机构**：经委员会授权后，可执行穿透式合规审计。

审计不再是一项特权，而是一种普适的系统能力。任何具备技术条件的参与者，均可同步日志并进行独立重放，从而判定是否存在未记录的拒绝、未合理解释的延迟或未经授权的模式切换。

四．**追责的制度闭环**

可追责的终点是制度化的惩戒后果，依据违规程度实施阶梯式处理：

- **轻微违规**：全网公开记录，责令限期整改并发布正式解释。
- **中度违规**：强制削减运营任期，启动竞争性重授权流程。
- **重大违规**：直接触发罢免程序，永久丧失运营资格，并移交法律追诉。

核心原则在于：**违规判定不依赖于主观认定，而是取决于可验证的证明包**。一份包含完整审计轨迹、链上哈希对照与独立重放结果的证明包，其证明力远超任何机构的调查结论。

A4.7.4 正确性是制度设计的产物

上述机制共同构成了 SRH 的免疫架构。可验证性、可替代性与可追溯性贯穿于探测、约束及归因的全过程，确保了系统运行的合规性在任何阶段均可被核查、被辩护并被记录。

Core Dimension 核心维度	Governance Logic 治理逻辑	Core Value 核心价值	Threats Addressed 针对威胁
Verifiable (front end) 可验证 (前端)	Detect deviation 探测偏离	Make correctness a publicly recomputable mathematical fact 让正确性成为可公开复算的数学事实	Conclusion tampering, covert violations 结论篡改、隐蔽违规
Substitutable (middle stage) 可替代 (中段)	Constrain power 约束权力	Ensure that no SRH instance possesses single-point monopoly status 确保任何 SRH 实例都不具备单点垄断地位	Delay attacks, denial of service 拖延攻击、拒绝服务
Accountable (back end) 可追责 (末端)	Attribute responsibility 归因责任	Make every deviation an irrefutable public record 让每一次偏离都成为不可抵赖的公开记录	Blurred responsibility, difficulty of investigation 责任模糊、调查困难

Table 7: Three-Dimensional Governance Logic of the SRH System / 表 7：SRH 体系三维治理逻辑表

A4.8

Defining Settlement Validity:

Dual Finality and Public Verifiable Receipts

The core dilemma of cross-border settlement has never been the speed of transfer, but the mutual recognition of compliance status. Under the traditional correspondent-banking model, settlement depends on a recursive chain of institutional trust: the ledger shows that funds were debited, the message shows that the instruction was sent, and the compliance system shows that admission was approved, yet the supporting proof remains fragmented across heterogeneous systems. When disputes or regulatory review arise, it becomes difficult to determine whether each stage of execution complied with the rules then in force. The result is not only high reconciliation cost, but also the absence of a neutral audit anchor independent of private ledgers. The underlying problem is the disjunction between ledger finality and policy finality.

结算有效性的界定：

双重终局性与公共可验证回执

跨境结算的核心困境，从来不在于转账速度，而在于合规状态的互认。传统的代理行模式，结算依赖机构间递归式的信任链条：账本显示资金已扣划，报文显示指令已发出，合规系统显示准入已获批。然而，支撑这些结论的证明却碎片化地散落在各类异构系统中。一旦发生纠纷或监管审查，便极难断定执行的每个阶段是否均符合当时生效的规则。其结果不仅导致了高昂的对账成本，更造成了独立于私有账本之外的中立审计锚点的缺失。其底层问题的根源，在于账本终局性与政策终局性之间的脱节。

The Principia framework redefines settlement validity at the institutional level. Instead of relying on unilateral compliance assertions, it asks whether a settlement record can be independently verified, made tamper-resistant in logic, and reconciled across participants through a shared proof anchor.

This section treats settlement validity as the conjunction of two necessary conditions (ledger finality and policy finality) together with a public receipt that records their verified convergence. Every cross-domain settlement is therefore anchored in three linked elements:

- **Ledger finality**: the transaction reaches an irreversible state within the sovereign domain, with legal effect determined by that domain's own rules.
- **Policy finality**: the PoPC bound to the transaction is deterministically replay-verified, confirming consistency between the execution path and the declared rule version.
- **Public regulatory receipt**: the SRH issues a standardized receipt referencing the source domain, target domain, policy version snapshot, PoPC digest, and ordering timestamp.

Together, these elements give cross-domain settlement a level of determinacy and auditability that is ordinarily associated with domestic settlement. They do not impose an additional burden on payment execution; they provide each transaction with a reconcilable, reviewable, and non-repudiable settlement identity.

A4.8.1 Dual Finality: The Parallel Pillars of Settlement Validity

The Principia framework defines dual finality as the requirement that cross-domain settlement satisfy two independent and necessary conditions.

First Layer: Ledger Finality - the Legal Bedrock

Ledger finality means that the transaction has reached an irreversible ledger state within the relevant sovereign domain under its own legal and operational rules. Each jurisdiction determines for itself what counts as finality, whether RTGS posting, DLT consensus confirmation, or another legally recognized form of title confirmation. This remains a sovereign legal fact. The SRH neither determines nor substitutes for it.

Second Layer: Policy Finality - the Auditable Foundation

Policy finality means that the compliance rules embodied in the

元宪章框架在制度层面重新定义了结算的有效性。它不再依赖单边的合规声明，而是诉诸于：结算记录是否可被独立验证、在逻辑上是否具备抗篡改性，以及是否能通过共享证明锚点在参与方之间实现平账对账。

本节将结算有效性视为两项必要条件（账本终局性与政策终局性）的交汇，并辅以一份记录两者验证合一的公共回执。因此，每一笔跨域结算均锚定在以下三个关联要素之上：

- **账本终局性**：交易在主权域内达到不可逆状态，法律效力由该域规则判定。
- **政策终局性**：与交易绑定的 PoPC 经由确定性的重放验证，确认了执行路径与声明的规则版本之间的一致性。
- **公共监管收据**：由 SRH 签发一份标准化回执，其中索引了源域、目标域、策略版本快照、PoPC 摘要及排序时间戳。

这些要素赋予了跨域结算一种通常仅见于境内结算的确定性与可审计性。它们并非在支付执行过程中增加额外负担，而是为每笔交易提供了一个可对账、可追溯且不可抵赖的结算身份。

A4.8.1 双重终局：结算有效性的平行支柱

元宪章体系确立了双重终局的定义：一笔跨域结算的完成，必须同时满足两个相互独立且必要的条件。

第一重：账本终局性 - 法律基石

账本终局性意味着，根据相关主权的法律与规则，交易已在该域内达到不可逆的账本状态。每个司法管辖区自行界定何为终局，无论是 RTGS 的入账、分布式账本的共识确认，还是其他法律确权形式。这始终属于主权法律事实，SRH 既不对此进行判定，亦不作为其替代。

relevant JPack have been deterministically executed and that the resulting PoPC has been independently verified against the declared rule version. What is verified is the integrity of execution, not the merits of the policy itself. Because verification depends on standardized inputs and a fixed policy snapshot, the result is publicly reproducible.

The Logical Relationship of Dual Finality

Not Sequential, but a Logical AND: A transaction is not globally valid merely because it has been posted to a ledger. If its compliance proof cannot be verified, later audit may still invalidate its policy status. Conversely, possession of a PoPC does not by itself constitute settlement: if sovereign ledger transfer has not been completed, the transaction remains a compliant instruction rather than a completed payment.

Only where ledger finality and policy finality both obtain does cross-domain settlement close its logical loop. The first establishes transfer finality within the sovereign ledger; the second converts compliance from a matter of assertion into a matter of verification. Settlement validity therefore becomes both juridically grounded and publicly auditable.

A4.8.2 Public Regulatory Receipts: Resolving the Proof Deadlock of Dual Finality

Dual finality answers what counts as valid at the logical level, but it immediately raises a further question: who can attest, in a neutral and tamper-resistant manner, that both ledger finality and policy finality have been achieved across heterogeneous systems and asynchronous timeframes?

If the originating SCEL alone declares completion, the framework collapses back into recursive trust. If validity depends entirely on the receiving side, temporal divergence and reconciliation ambiguity remain. The problem is that dual finality consists of two independently occurring facts, yet no single party naturally possesses complete and neutral witnessing authority over both.

- **The originating party**: controls the ledger state, but cannot itself prove the subjective neutrality of its compliance execution.
- **The receiving party**: controls the receipt result, but cannot verify the originator's execution process in a penetrative manner.
- **Regulators**: possess legal authority, but lack a unified proof

第二重：政策终局性 - 可审计基础

政策终局性意味着，相关 JPack 中所封装的合规规则已得到确定性执行，且生成的 PoPC 已对照声明的规则版本完成了独立验证。此处验证的对象是执行的完整性，而非策略本身的正当性。由于验证依赖于标准化的输入与固定的策略快照，其结果在公共层面具有可重现性。

双重终局的逻辑关系：非先后，而是“逻辑与”

一笔交易并不因其已计入账本就自动具备全局有效性。若其 PoPC 无法通过验证，随后的审计仍可能废止其策略状态。反之，仅持有 PoPC 本身亦不构成结算：若主权账本划转尚未完成，该交易仅被视为一份合规的指令，而非完成的支付。

唯有当账本终局性与政策终局性同时具备时，跨域结算方能完成其逻辑闭环。前者确立了主权账本内的划转终局，后者将合规性从一种单边声明转化为一种公共验证。由此，结算有效性既具备了法律支撑，又具备了公共审计基础。

A4.8.2 公共监管回执：破解双重终局的存证困局

双重终局性在逻辑层面回答了“何为有效结算”，但随之而来的是一个更深层的命题：在异构的系统环境与异步的时间维度下，究竟由谁来以中立且抗篡改的方式，证明账本终局性与政策终局性已双双达成？

若仅由发起方 SCEL 单方面宣告结算完成，整个框架将退化回传统的递归信任泥潭；若有效性完全取决于接收方的判定，则时间上的异步性与对账中的歧义性依然无法消除。问题核心在于：双重终局性由两个独立发生的客观事实构成，但没有任何单一参与方能够天然地对这两者拥有完整且中立的见证权。验证这种时序

anchor capable of crossing proprietary systems and aligning accounts.

(1) Public Regulatory Receipt

Collective Witnessing by Global Consensus: The core output of the SRH is a public regulatory receipt generated when three conditions are jointly satisfied: the originating SCEL has produced a valid PoPC; the verification process has been deterministically replayed against the referenced rule version; and the result has been anchored through the SRH's consensus process. The receipt is therefore not an optional add-on, but the public record that the transaction has reached verified dual finality under specified rules and at a specified time.

(2) The Institutional Nature of the Public Regulatory Receipt

From License to Recorded Fact: A public regulatory receipt is not a license issued by the SRH; it is a record of verified dual finality. Its force lies in three properties already established elsewhere in the framework: authenticity can be checked through signatures and state commitments; process integrity can be re-tested through replay; and consistency can be reconciled against the relevant sovereign ledger records. Once those conditions hold, the receipt ceases to be an operator statement and becomes a publicly verifiable institutional fact.

Once a public regulatory receipt can be independently verified by anyone, it is elevated from a unilateral operator statement into collective witnessing by global consensus of dual finality. This determinacy leads cross-border payment away from blind trust under authority and toward an era of proof grounded in mathematics.

A4.8.3 From Bilateral Assurance to Public Verifiability

From this point onward, cross-border reconciliation changes in character. In the traditional model, where no shared public receipt exists, reconciliation is fundamentally bilateral: each side defends its own records. Under the Principia framework, once all parties can independently verify the same public regulatory receipt and reconcile it against the finalized global state, discrepancies cease to be credibility contests and become locatable technical deviations.

上的异步，是引发对账分歧与结算争议的温床。

- **发起方**：掌握账本状态，却无法自证合规执行的主观中立性。
- **接收方**：掌握到账结果，却无法穿透式验证发起方的执行过程。
- **监管机构**：掌握法律权威，却缺乏一个能跨越专有系统、对齐账目的统一证明锚点。

(1) 公共监管回执：全局共识的集体见证

SRH 的核心产出，即是在三项条件同时满足时生成的公共监管回执：发起方的 SCEL 已生成有效的 PoPC；验证程序已针对所引用的规则版本完成了确定性的重放验证；验证结果已通过 SRH 的共识过程完成锚定。因此，该回执并非可有可无的附加项，而是证明交易在特定规则下、于特定时间点已达成已验证双重终局性的公共记录。

(2) 公共监管回执的制度本质：从行政许可证回归存证事实

公共监管回执并非 SRH 颁发的准许证，而是对双重终局性已达成这一状态的正式记录。其效力源于框架内已确立的三大属性：真实性可通过签名与状态承诺进行核查；过程完整性可通过重放验证进行复测；一致性可对照相关主权账本记录进行核审。一旦这些条件成立，回执便不再仅仅是运营方的单方陈述，而是演变为一个公共可验证的制度事实。

当公共监管收据可以被任何人独立核验时，它便从运营者的单方声明，升维为全局共识对双重终局的集体见证。这种确定性将跨境支付从威权下的盲目信任，带向了数学支撑下的证明时代。

Dimension 维度	Traditional Model: Reconciliation as Confrontation 传统模式：对账即对质	Principia Framework: Reconciliation Against a Shared Public Record 元宪章框架：基于共享公共记录的对账模式
Essence of reconciliation **对账本质**	One party's record versus another party's record 单方记录 vs 单方记录	One party's record versus the globally validated reconciliation record 单一主体账本记录 vs 全球验证的对账记录
Root of dispute **争议根源**	The payer claims to have remitted; the payee claims not to have received 付款方声称已汇出，收款方声称未到账	Inconsistency between local records and the public receipt or finalized global state 单方账目记录与全局验证对账记录之间的对比
Dispute resolution **争议解决**	Depends on the completeness of proof and negotiated mediation 依赖证明完整性与谈判斡旋	Depends on consistency between the public receipt, replayable proofs, and the finalized shared state 取决于公共回执、可重放证明以及已定性的共享状态三者之间的一致性
Role of participants **参与方角色**	Both parties passively produce proof by retrieving logs and messages 双方各被动举证，调取日志与报文	Parties actively verify and hold the same public receipt and can independently check it against shared state 各参与方均主动验证并持有同一份公共回执，并能基于共享状态对其进行独立的对账核验
Audit method **审计方式**	Depends on the audited party to produce data for inspection 依赖于被审计方主动提供数据以供核查	Audit bodies can independently replay execution and verify the public receipt against shared state 审计机构能够独立重放执行过程，并对照共享状态对公共回执进行穿透式验证

Table 8: Comparison of Cross-Border Reconciliation Models / 表 8：跨境对账模式对比表

This fundamental reversal elevates settlement validity, for the first time, from a private administrative commitment into an institutionalized public good. It demonstrates to the world that, even without establishing a suprasovereign authority, multiple sovereign states can still reach a high degree of consensus on what counts as valid. The key to achieving this leap is, in fact, very simple: validity need only be redefined from "you claim that you are compliant" to "I can verify that you are compliant".

A4.8.3 从双边信用担保走向公共可验证性

自此，跨境对账的本质发生了根本性变化。在传统模式下，由于缺乏共享的公共回执，对账在本质上是双边化的：每一方都只能各执一词，极力维护自身的私有记录。但在元宪章框架下，一旦所有参与方均能独立验证同一份公共监管回执，并将其与已定性的全局状态进行核验对齐，各方之间的账务差异将不再是信用层面的博弈，而演变为可定位的技术偏差。

这一根本性逆转，使得结算有效性第一次从一种私有的行政承诺，升华为一种制度化的公共品。它向世界证明：在不设立超主权权威的前提下，多元主权国家依然可以就"何为有效"达成高度共识。实现这一跨越的诀窍其实非常朴素：只需将有效性的定义，从"你声称自己合规"转向"我能验证你合规"。

A4.9

Governance of Policy Versions and Proof Interfaces:

Reconciling Sovereign Dynamism with the Stability of Mutual Recognition

政策版本与证明接口治理：

调和主权动态性与互认稳定性

The dynamic evolution of sovereign rules and the need for stability in cross-domain mutual recognition create a fundamental institutional tension. Sovereign policy is not static: sanctions lists are updated, capital controls may be introduced abruptly, AML thresholds are adjusted, and new asset classes generate new compliance requirements. This flexibility is an inherent attribute of sovereignty.

Yet cross-domain settlement depends on determinacy. A transaction that occurred six months earlier cannot later be re-evaluated simply because today's rules have changed; otherwise, settlement would lose finality. In traditional systems, this contradiction is often handled ambiguously: rule changes lack transparent version control, historical verification depends excessively on logs, and mutual recognition rests on present-day interpretation of past rules.

The Principia framework addresses this tension directly: how can sovereigns remain free to change their rules without destabilizing the basis of mutual recognition?

The answer rests on two principles: version pinning and replayable verification. These are not merely technical devices, but governance principles. They convert rule succession from institutional rupture into traceable evolution by binding every transaction to the rule version in force at the time it took effect. Mutual recognition is thereby anchored not in present interpretation, but in replay of historically pinned proof.

A4.9.1 Version Pinning: The Institutional Anchoring of Rule Changes

主权规则的动态演进与跨域互认对稳定性的诉求，构成了制度设计中一对根本性的核心张力。主权策略并非一成不变：制裁名单会实时更新，资本管制可能骤然介入，反洗钱阈值会随时调整，而新兴资产类别也不断催生出新的合规要求。这种灵活性是主权天生具备的属性。

然而，跨域结算却极度依赖确定性。一笔发生在半年前的交易，不能仅因为今天的规则变了就对其进行重新评估，否则结算将丧失终局性。在传统系统中，这种矛盾往往被模糊化处理：规则变更缺乏透明的版本控制，历史验证过度依赖日志记录，而互认则往往建立在“用今天的眼光解读昨天的规则”这一基础之上。

元宪章直接回应了这一挑战：主权国家如何在保持更改规则自由的同时，不动摇互认的根基？

其答案立足于两大原则：版本锚定与可重放验证。这不仅是技术手段，更是治理原则。通过将每笔交易与其实施时生效的规则版本进行强制绑定，它们将规则的更迭从一种制度性断裂转化为可溯源的演进。由此，互认不再锚定于当下的主观解读，而是锚定于对历史特定版本证明的重放。

(1) The version nature of JPack

In SSI, JPack functions as a versioned sovereign policy snapshot rather than as a mere bundle of regulatory requirements. Every material regulatory change produces a new version identified by a globally unique cryptographic hash and recorded in the relevant sovereign registry, regardless of whether the change involves a threshold adjustment, a blacklist update, or a structural reorganization.

The structure of JPack version identifiers follows a unified standard specification to ensure global recognizability:

Structure:

[Jurisdiction][*Regulator*][Rule Category][*Version Number*][Release Timestamp]

Examples:

`SG_MAS_AML_2026.03_v2.1_20260315`

`EU_MiCA_ART_v3.0_20260101`

`US_OFC_SDN_20260228_daily`

Once released, a JPack version becomes immutable and must remain historically available. Old versions are not overwritten by subsequent updates, but preserved for replay, audit, and legal review. The Principia framework should therefore impose preservation obligations on sovereign publishers and support independent archival retention across the audit and observation layers.

(2) Permanent transaction reference to versions

When each cross-domain transaction generates a PoPC, it must explicitly reference the JPack version hash on which its compliance is based. This reference is deeply embedded in the data structure of the PoPC and becomes an inseparable component of the transaction. No matter how the future regulatory environment evolves, compliance verification of that transaction always points to that specifically pinned version. Even if that version has been retired from the production environment, its historical snapshot still supports deterministic replay verification. This mechanism ensures, at the institutional level, temporal and spatial consistency of rule effectiveness: history belongs to history, and the present belongs to the present.

A4.9.2 Effectiveness and Transition: The Institutional Procedure for Rule Changes

A4.9.1 版本钉住：规则变更的制度化锚定

(1) JPack 的版本本质

在 SSI 体系下，JPack 的本质是带版本控制的主权政策快照，而非简单的监管要求集合。任何实质性的监管变更，无论是阈值调整、黑名单更新、还是架构重组，都会生成一个由全局唯一密码学哈希标识的新版本，并记录在相关的主权注册中心内。

JPack 版本标识的结构遵循统一的标准规范，以确保其在全球范围内的可识别性：

结构：

[司法辖区]_[监管机构]_[规则类别]_[版本号]_[发布时间戳]

示例：

`SG_MAS_AML_2026.03_v2.1_20260315`

`EU_MiCA_ART_v3.0_20260101`

`US_OFC_SDN_20260228_daily`

JPack 版本一经发布即进入不可篡改状态，且必须保持历史可追溯性。新版本的迭代绝非对旧版本的覆盖，而是将其完整保留，以备重放、审计及法律审查之需。因此，元宪章框架须对主权发布方施加存证义务，并在审计层与观察层提供独立归档支持。

(2) 交易对版本的永久引用

每笔跨境交易在生成 PoPC 时，必须显式引用其合规所依据的 JPack 版本哈希。这种引用被深层固化在 PoPC 的数据结构中，成为该笔交易不可分割的一部分。无论未来的监管环境如何演变，对该笔交易的合规验证始终指向那个被钉住的特定版本。即便该版本已从生产环境退役，其历史快照依然支持确定性的重放验证。这种机制从制度层面确保了规则效力的时空一致性：历史的归历史，当下的归当下。

Version pinning protects historical integrity, but rule succession still requires an orderly transition procedure. To avoid policy shock, the Principia framework establishes a standardized process for version effectiveness and migration.

- **Announcement and notice period**: the new version is published with its hash, full rule text, change summary, compatibility notes, and test vectors, allowing participants time for impact assessment.
- **Parallel support period**: the old and new versions may coexist for a defined migration window, during which the SRH accepts PoPCs referencing either version.
- **Mandatory switch and archival**: after the cutover point, only the new version is accepted for new transactions, while the old version remains available solely for replay, audit, and historical review.

In exceptional circumstances, the notice period may be shortened under a defined emergency procedure, provided that the emergency basis is explicitly recorded, the version is clearly marked as such, and retrospective review remains mandatory. At the dispute-handling layer, version-anchored acceptance vectors function as the decisive consistency benchmark: executions that pass are treated as compliant; executions that fail indicate implementation deviation.

A4.9.3 Acceptance Vectors: The Foundational Safeguard of Verifiability

If version pinning resolves the traceability of rules, acceptance vectors resolve the uniqueness of execution.

Merely locking the version is not sufficient. If the same set of rules and the same inputs produce entirely different outputs in different system implementations, then version pinning has only locked a meaningless filename. As an inseparable component of JPack, the acceptance vector contains standardized input sets, expected outputs, and execution-trace hashes. Its existence provides the institution with three core functions:

- **Consistency verification**: any SCEL implementation, SRH node, or audit tool must run the acceptance vectors associated with a JPack version. Only implementations that pass can be treated as version-consistent.
- **Visibility of rule change**: by comparing the vectors associated with successive versions, regulators can observe how rule effects have changed in practice, making legal

A4.9.2 生效与过渡：规则变更的制度程序

版本锚定保护了历史记录的完整性，但规则的更迭仍需一套有序的过渡程序。为防范策略冲击，元宪章为版本生效与迁移确立了标准流程：

- **公示与预告期**：新版本发布时须同步披露其哈希值、完整规则原文、变更摘要、兼容性说明及测试向量，给予参与方充足的时间进行影响评估。
- **并行支持期**：在预设的迁移窗口内，新旧版本可以共存，SRH 在此期间同时接受引用任一版本的 PoPC。
- **强制切换与归档**：一旦越过切换点，新发起的交易仅接受新版本验证；旧版本则转入归档状态，仅用于重放、审计及历史追溯。

在极端特殊情况下，可通过预设的应急程序缩短预告期，前提是必须明确记录应急事由，对该版本进行特殊标识，且事后审查仍为强制要求。在争议处理层，版本锚定的准入向量将作为判定一致性的决定性基准：通过验证的执行即被视为合规；未通过者则被判定为实现偏差。

A4.9.3 验收向量：可验证性的底层保障

如果说版本钉住解决了规则的可追溯性，那么验收向量则解决了执行的唯一性。

仅仅锁定版本是不够的。如果同一套规则、同样的输入，在不同的系统实现中产生了截然不同的输出，那么版本钉住就只是锁定了一个毫无意义的文件名。 验收向量作为 JPack 不可分割的组成部分，包含标准化的输入集、预期输出及执行轨迹哈希。它的存在赋予了制度三项核心功能：

evolution testable rather than purely textual.

- **Dispute resolution**: when cross-domain disagreement arises, the disputed inputs can be run against the relevant acceptance vectors. The outcome reveals whether the divergence lies in rule application or in implementation error.

A4.9.4 Conclusion and Institutional Effects: Version Is Institution, Proof Is Mutual Recognition

Through the governance framework above, the Principia framework achieves four core institutional effects.

(1) **History is not rewritten by new rules**: Each transaction remains bound to the JPack version in force when it occurred. Rule evolution does not retroactively alter historical settlement validity.

(2) **Rule changes do not interrupt cooperation**: Notice periods, migration windows, and archival continuity convert rule succession from disruption into managed transition.

(3) **Mutual recognition is based on replayable proof**: Cross-domain recognition no longer depends on present interpretation, but on the ability to replay the historically relevant rule version and verify the associated PoPC.

(4) **Dispute resolution shifts from power to fact**: Where disagreement arises, the relevant acceptance vectors provide a common benchmark for determining whether the divergence reflects rule application or implementation error.

Sovereignty retains the freedom to change its rules, but that freedom operates within a versioned, traceable, and verifiable framework. Mutual recognition remains stable because rule evolution is pinned to proof rather than left to retrospective interpretation.

- **一致性验证**：任何 SCEL 的实现方案、SRH 节点或审计工具，均须运行与特定 JPack 版本关联的准入向量。唯有通过验证的实现方案，方可被视为与该规则版本保持逻辑一致。
- **规则变更的可视化**：通过对比相邻版本的准入向量，监管机构能够直观观测规则在实践中的效应演变。这使得法律的演进变得可测试、可量化，而非仅仅停留在文字表述层面。
- **争议解决**：当跨域协作出现分歧时，可将争议项下的输入数据针对相关的准入向量进行重放。运算结果将明确揭示：分歧究竟源于规则适用的差异，还是源于代码实现的错误。

A4.9.4 结论与制度效果：版本即制度，证明即互认

通过上述治理框架，元宪章体系实现了四大核心制度效果：

(1) **新规不溯及既往**。每笔交易始终与其发生时生效的 JPack 版本强制绑定。规则演进不会反向削弱或改变历史结算的有效性。

(2) **规则变更不中断协作**。通过预告期、迁移窗口以及归档连续性机制，规则的更迭从一种制度性断裂转化为受控的平滑过渡。

(3) **互认基于可重放的证明**。跨域互认不再依赖于当下的主观解读，而是取决于对特定历史规则版本的重放能力，以及对关联 PoPC 的验证。

(4) **争议解决从权力博弈转向事实定性**。一旦产生分歧，相关的准入向量将作为通用基准，明确揭示偏差究其根源是规则适用问题，还是代码实现错误。

主权始终保有修改规则的自由，但这种自由是在一个版本化、可追溯且可验证的框架内行使的。互认机制之所以稳固，是因为规则的演进被锚定在不可篡改的证明之上，而非任由事后的主观解读所左右。

A4.10

Sovereign Admission and Exit:
The Institutional Boundaries of Voluntary Cooperation

主权的准入与退出：
自愿协作的制度边界

The SSI framework is a voluntary cooperation layer grounded in sovereign agreement rather than a suprasovereign body standing above participating jurisdictions. Within that framework, accession and withdrawal are not only expressions of sovereign autonomy, but also conditions for maintaining continuity, predictability, and institutional clarity in the shared layer.

SSI 框架是一个立足于主权协议之上的自愿性协作层，而非凌驾于各参与司法管辖区之上的超主权机构。在该框架内，准入与退出不仅是主权自治的体现，更是维持共享层连续性、可预测性及制度清晰性的必要前提。

A4.10.1 Admission Procedure: Voluntary Accession and Verifiable Commitment

Any sovereign applying to join the SSI framework must complete a standardized path from legal commitment to technical alignment:

1. **Adoption of the Principia framework**: formally adopt the governing Principia and commit to its core principles, prohibitions, and procedures.
2. **SCEL deployment**: deploy a conforming SCEL instance within the jurisdiction and complete system-consistency verification.
3. **JPack registration**: package the country's effective compliance rules into JPack versions and publish them in the sovereign registry, ensuring that the regulatory logic is publicly verifiable.

A4.10.1 准入程序：自愿加入与可验证承诺

任何主权申请加入 SSI 框架，均需完成从律承诺到技术对齐的标准化路径：

1. **宪章签署**：正式签署《主权协同结算宪章》，承诺履行其核心原则与禁令。
2. **SCEL 部署**：在管辖区内完成合规的 SCEL 实例部署，并执行系统一致性验证。
3. **JPack 注册**：将本国生效的合规规则封装为 JPack 版本并在主权注册表中发布，确保监管逻辑的公开可验证。

4. **Public notice and objection period**: the accession request enters a notice window (for example, 30 days), during which participating sovereigns may raise material compatibility or governance concerns. If no material objection is sustained under the applicable procedure, the request proceeds.
5. **Technical joint testing**: complete end-to-end integration testing with the SRH testnet, ensuring that proof generation, transmission, and replay verification processes are error-free.
6. **Formal activation**: once activation is announced under the applicable governance procedure, the sovereign enters the cooperation layer as a participating jurisdiction, with the corresponding rights and obligations of participation.

A4.10.2 Exit Procedure: Orderly Exit, Responsibility Does Not Extinguish

A participating sovereign retains the right to withdraw unilaterally from the cooperation layer in accordance with its own sovereign decision. However, withdrawal from participation does not extinguish historical responsibility. To ensure settlement finality, the exit process must follow an orderly wind-down procedure:

1. **Exit declaration and buffer period**: submit a formal exit declaration and initiate a buffer period of no less than 90 days. During this period, the sovereign must still perform its duties, and the SRH will continue processing its unfinished outstanding transactions.
2. **Historical responsibility lock-in**: before withdrawal takes effect, the system must anchor the sovereign's outstanding historical transaction proofs so that past activity remains verifiable after participation ends.
3. **Settlement continuity guidance**: for cross-domain transactions still in flight, standardized completion paths must be provided so that withdrawal does not leave settlement in default or limbo.
4. **Archival transfer and completion notice**: the sovereign's historical JPack versions must be transferred into long-term archival retention. Once proof-chain integrity and responsibility lock-in have been confirmed, a formal notice of withdrawal completion is issued.

4. **公示与异议期**：申请进入公示窗口（如 30 天），现有成员主权可针对潜在的合规冲突提出质询。若无重大异议，自动进入下一阶段。
5. **技术联调**：与 SRH 测试网完成全链路联调，确保证明生成、传输与重放验证流程的万无一失。
6. **正式激活**：在治理委员会发布激活公告后，该主权正式成为协作层成员，享有协作权益并承担相应义务。

A4.10.2 退出程序：有序退出，责任不灭

主权有权根据自身意志单方面选择退出协作层，但成员身份的终结并不等同于历史责任的豁免。为确保交易结算的最终性，退出过程必须遵循有序的降落程序：

1. **退出声明与缓冲期**：提交正式退出声明并启动不少于 90 天的缓冲期。在此期间，该主权仍须履职，SRH 亦将继续处理其尚未完成的存量交易。
2. **历史责任锁定**：在退出指令正式生效前，系统必须强制锚定该主权域所有未结的历史交易证明。这确保了即便在其停止参与体系后，其过往的所有活动依然保持可验证性。
3. **资产清算指引**：针对处于“在途状态”的跨域结算”交易，提供标准化的清算路径，防止出现结算违约或状态悬空。
4. **档案移交与公告**：将该主权的历史 JPack 版本转入长期归档库，在确保证明链条完整并锁定责任后，由治理委员会正式发布退出完成公告。

A4.10.3 Termination of Participation for Fundamental Breach

Where a participating sovereign commits a fundamental breach of the Principia framework, materially threatens shared system integrity, or renders continued cooperation procedurally untenable, participation in the shared layer may be terminated under the highest applicable procedure.

Following approval under a supermajority threshold (for example, three-quarters) and the applicable high-order procedure, termination of participation may be initiated without the ordinary withdrawal buffer period where immediate continuity risk requires it. Even in such cases, historical responsibility lock-in and settlement-continuity measures must still be applied so far as practicable in order to protect outstanding transactions and other participating parties.

A4.10.3 因根本性违约终止参与资格

当某一参与主权严重违背元宪章的核心原则、威胁系统安全或破坏协作共识时，协作层保留自我防卫的权利。

在获得超多数票（例如四分之三以上）表决通过并启动相应的最高级别程序后，若系统面临紧迫的连续性风险，可跳过常规的退出缓冲期，立即启动参与方终止程序。即便在此时，仍须在实际操作范围内强制执行历史责任锁定与结算连续性保障措施，以确保未结清交易及其他参与方的合法权益不受损害。

A4.11

Emergency Governance: Boundary-Preservation Mechanisms Under Acute Shocks

应急治理：急性冲击下的边界保持机制

Any public infrastructure must recognize that systems may fail, risks may emerge abruptly, and extreme scenarios cannot be excluded entirely. The Principia framework does not assume error-free operation. It provides an emergency-governance structure designed to preserve institutional boundaries, proof continuity, and procedural order under abnormal conditions.

Triggering principles: An emergency state may be triggered only in response to objective and verifiable systemic risk, such as large-scale technical failure, consensus fracture, sustained denial-of-service attack, critical security vulnerability, or other structural threats to continuity. Its declaration must follow multilateral procedures authorized under the Principia framework. It must not take effect solely on the basis of unilateral political judgment or ad hoc discretion. The triggering process must be publicly recorded and supported by a complete proof trail.

任何公共基础设施都必须承认，系统可能失效，风险可能骤降，且极端场景无法被完全排除。因此，元宪章框架并不设定零错误的运行假设，而是建立了一套应急治理架构，旨在非常规状态下维护制度边界、证明连续性以及程序正义。

触发原则：应急状态的触发必须基于客观且可验证的系统性风险，如大规模技术故障、共识破碎、持续性的拒绝服务攻击、核心安全漏洞，或其他对系统连续性构成的结构性威胁。应急状态的宣告必须遵循元宪章授权的多边程序，绝不可仅凭单方面政治判断或随机的自由裁量权而生效。整个触发过程必须公开记录，并辅以完整的证明链条。

Strict boundaries of emergency powers: Under an emergency state, limited protective measures may be permitted, including temporary suspension of ordering, restriction of new transactions, degraded operating modes, or initiation of substitute instances. However, no emergency measure may cross the following Principia-level red lines:

- It must not interpret or rewrite sovereign rules.
- It must not alter the definition of settlement finality.
- It must not rewrite historical records or delete existing proofs.
- It must not introduce adjudicative authority or unilateral sanctions capability.
- It must not breach the negative list established under the Principia framework.

An emergency state must not become a pretext for crossing institutional boundaries. Any measure that touches these red lines must be treated as a Principia-level amendment rather than as an emergency act.

Temporal limits and automatic lapse: An emergency state must have clear temporal limits and an automatic lapse mechanism. Any extension must be approved through renewed deliberative procedure and entered into the public record. Emergency authority is limited to restoring stability and proof continuity and may not harden into an ordinary instrument of governance.

Mandatory review and accountability: Once the emergency state is lifted, a public review report must be issued setting out the triggering cause, the measures taken, the scope of impact, and the recovery path. All abnormal operations must be incorporated into auditable records and remain subject to independent reexamination. Where overreach is identified, replacement, accountability, or institutional-correction procedures must be initiated.

Through institutionalized emergency governance, the framework acknowledges risk without surrendering control over power. It permits temporary disruption in operational rhythm, but not deviation from institutional boundaries. Even under acute stress, the system preserves a clear allocation of authority and responsibility, continuity of proof, and reviewable settlement finality, thereby protecting the integrity of the sovereign cooperative structure.

应急权力的严格边界：在应急状态下，允许采取有限的保护性措施，包括暂时挂起排序、限制新交易接入、降级运行模式或启用替代实例。然而，任何应急措施均不得逾越以下元宪章层级的红线：

- 严禁解释或重写主权规则
- 严禁更改结算终局性的定义
- 严禁篡改历史记录或删除既有证明
- 严禁引入裁决权或单边制裁能力
- 严禁突破元宪章框架下确立的负面清单

应急状态绝不可成为越过制度边界的借口。任何触及上述红线的举措，必须视为对《元宪章》层级的根本性修订，而非简单的应急行为。

时限与自动失效：应急状态必须设有明确的时限及自动失效机制。任何延长期限的要求均须通过重新审议程序批准并载入公共记录。应急权力的行使仅限于恢复系统稳定与证明连续性，不得固化为常规治理工具。

强制审查与问责：应急状态解除后，必须发布公开审查报告，阐明触发原因、所采取措施、影响范围及恢复路径。所有异常操作均须纳入可审计记录，并接受独立复核。一旦发现权力逾矩，必须启动更迭、问责或制度纠偏程序。

通过制度化的应急治理，框架在承认风险的同时并未交出对权力的控制。它允许运行节奏的暂时中断，但绝不允许偏离制度边界。即便在极端压力下，系统依然保持着清晰的权责划分、证明的连续性以及可复核的结算终局性，从而捍卫了主权协作架构的完整性。

CHAPTER A5.

Executable Policy & Verifiable Compliance in Sovereign Systems

A5. 章节

主权体系下的可执行政策与可验证合规

Abstract:

As established in the preceding sections, scalable and resilient cross-border digital financial infrastructure requires more than technical interoperability: it must preserve sovereign regulatory authority while sustaining global operational coherence. The SSI architecture provides continuity, fault isolation, and proof-based settlement across jurisdictions; the remaining question is how regulatory intent is expressed, evaluated, and verified within this model.

In multi-jurisdictional environments, distributed ledgers offer deterministic state transitions and irreversible finality, but the legal and policy conditions under which transactions are permitted remain jurisdiction-specific, mutable, and typically opaque to external verification. Interoperability layers can therefore attest that a transaction occurred, but not why it was allowed, which rules applied, or whether those rules were correctly enforced at execution time. Existing approaches often hard-code regulatory logic into application code, smart contracts, or institutional middleware, coupling legal requirements to implementation details and causing policy drift, delayed updates, inconsistent cross-domain enforcement, and limited auditability - risks that become structural as assets traverse multiple chains and sovereign regimes.

This section introduces Policy-DSL, JPack, and PoPC as a unified policy-and-proof stack that enables sovereign authorities to publish versioned regulatory logic independently of execution code, evaluate it deterministically at transaction time, and bind outcomes to cryptographically verifiable proofs.

Policy-DSL supplies a compact, jurisdiction-neutral vocabulary for expressing constraints such as KYC/AML tiers, residency requirements, transaction caps, travel-rule obligations, business-hour windows, and asset-class restrictions. JPack (Jurisdiction Packs) packages these policies as sovereign-authored, versioned rule sets suitable for audit and replay across domains[1-3]. PoPC (Proof of Policy Compliance) produces a verifiable proof of which rules were evaluated, why an allow/hold/reject decision was reached, and under which execution-environment conditions the evaluation occurred.

Discretion and accountability remain explicitly separated. In institutional practice, statutory requirements are first translated into operational controls; the execution layer then evaluates transactions against pre-specified criteria rather than interpreting indeterminate legal concepts. Discretion is exercised upstream during rule formulation or exceptional approvals by accountable roles, while Policy-DSL/JPack encode the resulting determinations for deterministic execution and PoPC binds outcomes to replayable, auditable proofs - preserving responsibility attribution and enabling neutral verification.

（本章摘要）

如前文所述，构建具有可扩展性与韧性的跨境数字金融基础设施，绝非单纯的技术互操作问题：它必须在维持全局运行一致性的同时，保障各国的监管主权。SSI 架构虽然实现了跨辖区的业务连续性、故障隔离以及基于证明的结算，但核心问题依然尚待解决：在这一模型下，监管意图究竟应如何表达、评估与验证?

在多司法辖区场景下，分布式账本虽能提供确定性的状态转换与不可逆的结算终局性，但决定交易准入的法律与政策条件往往因辖区而异，且处于动态演进中，外部系统通常难以对其进行有效验证。因此，现有的互操作层往往只能证实交易“确实发生了”，却无法解释其“为何获准”、适用了哪些规则，以及这些规则在执行时是否得到了正确落实。目前的主流做法倾向于将监管逻辑硬编码在应用代码、智能合约或机构级中间件中，导致法律要求与技术实现深度耦合，进而引发政策漂移、更新滞后、跨域执行失配以及审计受限等风险，随着资产跨越多个区块链和主权监管体系流转，这些风险正逐渐演变为结构性隐患。

本节引入了由 Policy-DSL 、JPack 和 PoPC 构成的统一政策与证明的制度性组件，赋予主权当局独立于执行代码，发布带版本监管逻辑的能力，支持在交易发生时进行确定性评估，并将处理结果锚定在可验证的密码学证明上。

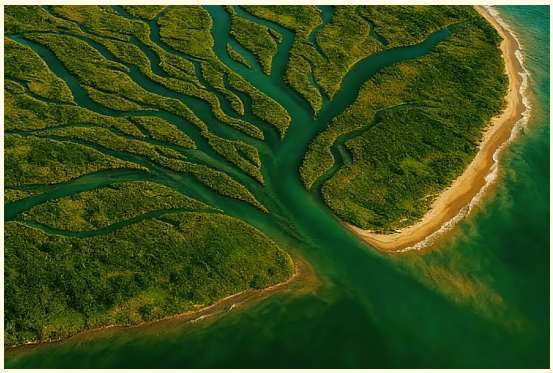
具体而言，Policy-DSL 提供了一套精炼且跨辖区通用的语汇，用于表达诸如 KYC/AML 分级、居住地要求、交易限额、旅行规则义务、营业时间窗口及资产类别限制等约束条件。JPack 将这些政策封装为由主权方编写、带版本的规则集，以便在不同领域间进行审计与重放[1-3]。PoPC 则生成一份可验证的凭证，详细记录了评估了哪些规则、为何达成准入 / 挂起 / 拒绝的决策，以及评估过程所处的具体执行环境。

在此架构下，自由裁量权与问责制被明确分离。在机构实践中，法律要求首先被转化为标准的操作控制逻辑；随后，执行层严格依据预设准则评估交易，而非直接去解读含义模糊的法律概念。裁量权被置于流程上游，由负责主体在制定规则或进行特批时行使；而 Policy-DSL 和 JPack 则将这些决策结果编码，以确保执行过程的确定性。最终，PoPC 将执行结果绑定为可重放、可审计的证明，在保留责任归属同时，实现了中立、客观的技术验证。

A5.1

Structural Misalignment and Execution Gaps in Cross-Border Regulatory Mutual Recognition

跨境合规互认的结构性失配与执行断层



Where river is pushing to the sea, 2020, worldrivers.net

"All paths converge at the same truth;
a hundred thoughts serve a single essence."
"天下同归而殊途，一致而百虑。"

— I Ching, Xici《易经·系辞》)

Contemporary cross-border digital finance exhibits a structural mismatch between the universality of distributed-ledger execution and the jurisdictional fragmentation of financial regulation[4-7]. Although regulators pursue broadly similar aims - preventing illicit finance, enforcing sanctions, protecting consumers, managing capital flows, and ensuring orderly markets - the articulation of these objectives varies widely across statutes, supervisory handbooks, and institutional practices[1,7-8], generating operational and systemic challenges:

(1) Policy Expression and Evolution

Policy drift and fragmentation: Jurisdictions encode similar concepts - transaction caps, KYC tiers, sanctions obligations, permitted geographies, residency restrictions, and investor classifications - using divergent terminology, thresholds,

当代跨境数字金融呈现出一种结构性错配，分布式账本执行的通用性与金融监管的辖区碎片化存在本质矛盾[4-7]。尽管各国监管的治理目标高度契合，普遍旨在防范非法金融、执行制裁、保护消费者、管理资本流动以及确保市场秩序，但这些目标在法律条文、监管手册及机构惯例中的具体表述存在显著差异[1,7-8]。这种差异引发了一系列操作性难题与系统性挑战：

(1) 政策表达与动态演进

政策漂移与碎片化：各司法辖区虽在核心监管逻辑上高度契合，例如交易限额、

time windows, reporting cadences, and exceptions[3,7,9]. Hard-coding this logic into applications, smart contracts, or cross-chain messaging layers produces drift as software and policy inevitably diverge, requiring repeated rewrites. Fragmentation multiplies with each new product class (stablecoins, tokenised deposits, tokenised funds)[5,10-12], widening the gap between regulatory requirements and deployed code.

Insufficient operational agility: Regulation evolves faster than deployment cycles[5,12]. Thresholds shift, sanctions lists update daily, emergency capital controls appear within hours, and new tokenised products receive revised supervisory expectations. Hard-coded controls lag behind, turning compliance updates into operational bottlenecks and sources of systemic risk.

Inability to encode regulatory certainty into programmable assets: Tokenised deposits, funds, stablecoins, and wholesale CBDCs depend on embedded policy constraints[13]. Without a standardised DSL, institutions implement bespoke, opaque controls in smart contracts or middleware, undermining interoperability, legal certainty, and participation in multinational pilots[14-15].

(2) Auditability, Proof, and Determinism

Audit and accountability gap: Ledgers reveal transactions, not regulatory processes[16]. An on-chain transfer does not prove correct sanctions screening, AML-tier assignment, travel-rule verification, or compliance with jurisdictional ceilings. Regulators increasingly require verifiable explanations - artifacts showing which rules fired, what inputs were evaluated, and why a transfer was allowed, held, or rejected[3,8].

Lack of deterministic replayability: Supervisors require proof that rules were applied exactly as they existed at a historical moment. Traditional systems rarely support re-execution of policy logic using precise historical versions of rules, parameters, and inputs, leaving institutions unable to meet modern audit standards in irreversible tokenised environments.

(3) Cross-Border and Cross-Chain Policy Continuity

Multi-jurisdictional inconsistency and conflict resolution: Cross-border flows trigger overlapping regimes: a single Singapore–EU payment may need to satisfy MAS licensing tiers,

KYC 分级、制裁义务、准入地域、居住地限制及投资者分类等方面，但在具体的术语表述、阈值标准、时间窗口、上报频率及豁免条款上却存在显著差异 [3,7,9]。若将此类逻辑直接硬编码于应用程序、智能合约或跨链消息层中，随着制度演进与系统实现之间不可避免的错配，将诱发“策略漂移”并迫使开发团队进行频繁且低效的代码重构。随着代币化存款、代币化基金及稳定币等新型资产的涌现 [5,10-12]，这种碎片化现象愈发严重，显著拉大了监管合规要求与底层部署代码之间的执行鸿沟。

运营敏捷性不足：监管政策的演进速度远超软件的部署周期 [5,12]。阈值动态调整、制裁名单每日更新、数小时内生效的紧急资本管制以及针对代币化产品不断修订的监管预期，都要求系统具备极高的响应速度。硬编码控制逻辑的滞后性，使得合规更新沦为运营瓶颈，并演化为潜在的系统性风险。

可编程资产缺乏监管确定性：代币化存款、基金、稳定币及批发型 CBDC 的合法运行，本质上取决于法规约束的内生化嵌入 [13]。标准化法规映射语言的缺失，使金融机构在智能合约或中间件中，只能构建高度定制且透明度较低的控制逻辑。此类做法在削弱互操作性与法律确定性的同时，也显著限制了机构参与跨国试点项目的广度与深度 [14-15]。

(2) 可审计性、证明与确定性

主权中继枢纽 (SRH)：一个由参与国家共同治理、在技术上保持中立的全球协同中继层。它负责处理跨境交易，通过确定性重执行来验证 PoPC 证明凭证，核验跨域

EU travel-rule obligations, capital-movement reporting, and bilateral sanctions checks. Without a unified abstraction for policy composition, institutions manually reconcile conflicts, creating inconsistency and error[19-23].

Compliance opacity across chains: As tokenised assets traverse SCELs, bridges, SCELs, and interoperability protocols, regulatory context disappears. Existing messaging layers transmit payloads but not policy intent, rendering cross-chain compliance fragile and legally uncertain[19-20,22-23].

(4) Verification and Infrastructure Compatibility

Infrastructure heterogeneity: Institutions operate heterogeneous security stacks - TEEs, HSMs, multi-sig schemes, and zero-knowledge systems - while blockchain architectures often assume uniform verification environments[24,57]. Without a layered proof model, stronger attestations fragment rather than reinforce interoperability[25-29,49].

政策与版本的兼容性，并将通过验证的交易封装路由至目标域。SRH 可提供全球统一的验证信号与审计级交易记录，并不单方面强制执行结算操作。

主权合规执行层 (SCEL)：一个由单一司法管辖区或机构完全控制的自治执行域。在交易流程中，发送方 SCEL 负责评估出境规则并生成 PoPC 证明；接收方 SCEL 则对照其本地政策包独立评估入境规则，并做出最终的接受 / 拒绝决策。只有在获得接收方确认后，结算才会被执行。

(3) 跨境与跨链策略的连续性

多重司法管辖的一致性与冲突解决：跨境流动涉及规则的重叠执行。例如，一笔新加坡与欧盟之间的支付可能需同时满足 MAS 的牌照分级、欧盟的旅行规则义务、资本流动报告及双边制裁检查。若缺乏统一的策略封装抽象，机构只能依靠人工调和冲突，从而产生逻辑不一致与操作错误[19-23]。

跨链合规透明度缺失：当代币化资产穿梭于不同的主权合规执行层、跨链桥及互操作协议时，监管上下文往往会丢失。现有的消息层仅传递数据载荷却无法传递策略意图，导致跨链合规机制极其脆弱且法律效力存疑[19-20,22-23]。

(4) 验证与基础设施兼容性

基础设施异构性：各机构运行着异构的安全栈，包括 TEE、HSM、多签方案及零知识证明系统，而区块链架构通常假设验证环境是均质的[24,57]。若缺乏分层证明模型，更强的存证能力反而会加剧生态碎片化，无法对互操作性形成有效支撑[25-29,49]。

A5.2

Our Solution: Verifiable Compliance Framework Design

The proposed architecture is built upon the principle of **Separation of Concerns, decoupling the formalization of regulatory logic**, the jurisdictional instantiation of that logic, and the generation/verification of compliance proofs.

This tripartite model, **comprising Core-DSL**,**JPack** and**PoPC**, aligns the rigor of formal methods with the flexibility of modern multi-chain financial infrastructure. Together, these components enable high policy expressiveness without sacrificing determinism, interpretability, or cross-chain interoperability.

(1) Core Structural Components

Policy-DSL (Deterministic Regulatory Expression): Policy-DSL is a minimal, domain-specific language tailored for cross-border settlement and foreign-exchange (FX) controls.

- **Neutral Vocabulary**: It abstracts jurisdiction-specific rules into universal primitives (Subject, Asset, Geography, Counterparty, Amount, Risk Score, etc.)[1].
- **Side-effect-free Execution**: Rules are strictly deterministic, ensuring that a given set of inputs always yields a clear decision, ALLOW, HOLD, or REJECT,accompanied by standardized reason codes.

PoPC (The Cryptographic Proof Chain): The Proof-of-Policy-Compliance (PoPC) is a proof toolchain that transforms "compliance black boxes" into transparent, cryptographic artifacts. It does not merely record a result; it provides a verifiable trail of which rules fired, which inputs were evaluated, and the logical path taken to reach a decision.

JPack (Versioned Policy Bundles): By combining Policy-DSL and PoPC, policymakers can encode complex regulations into JPack These are deployed as versioned, tamper-evident bundles across nodes, ensuring that the lifecycle of a regulation, from issuance to execution, is fully auditable.

(2) Network Orchestration: SRH and SCEL

我们的方案：可验证合规架构设计

本架构的核心逻辑基于“**关注点分离**”原则：即**将监管逻辑**的形式化表达、辖区实例化、与合规证明的生成验证进行解耦。

这种三位一体的模型：即**核心领域专用语言(Core-DSL)**、**JPack** 和 **PoPC**，将形式化方法的严谨性与现代多链金融基础设施的灵活性相结合，在不牺牲确定性和可解释性的前提下，实现了极强的监管表达力。

(1) 核心组件深度解析

Policy-DSL（监管逻辑的确定性表达）：Policy-DSL 是一种极简的领域特定语言，专为跨境结算与外汇控制设计。

- **中立词汇表**：抽象出辖区通用的监管原语（如：主体身份、资产类别、地理位置、风险评分、居民状态等）[1]。
- **无副作用执行**：确保规则执行是确定性的，其输出始终为明确的决策（ALLOW, HOLD, REJECT）及其对应原因代码。

PoPC（密码学证明链）：PoPC 是一套证明工具链，旨在将“合规黑盒”透明化。它生成的密码学凭证不仅记录交易结果，更追溯证明链条：哪些规则被触发、输入了哪些参数、逻辑推导的路径为何。

JPack（版本化的法规要件集）：Policy-DSL 与 PoPC 的结合使政策制定者能够将复杂的法律条文封装为 JPack。这些法规

The architecture is operationalized through two primary entities:

- **Sovereign Relay Hub** (SRH): A globally coordinated, technically neutral relay layer governed by participating nations. It orders cross-border transactions, validates PoPC artifacts by deterministic re-execution, checks policy/version compatibility across domains, and routes verified transaction envelopes to the destination domain. SRH provides a global verification signal and an audit-grade record, but does not unilaterally enforce settlement.
- **Sovereign Compliance Execution Layer** (SCEL): An autonomous execution domain controlled by an individual jurisdiction or institution. A sending SCEL evaluates outbound rules and generates PoPC proofs. A receiving SCEL independently evaluates inbound rules against its local policy pack and makes the final accept/reject decision; settlement is executed only upon acceptance.

要件集作为版本化的软件制品部署于执行节点，确保监管规则的下发、执行与审计具备全生命周期的一致性。

(2) 网络协同机制：主权中继枢纽与主权合规执行层

该架构通过两个核心实体进行运作：

主权中继枢纽 (SRH)：一个全球协调、技术中立的协作层，由参与国共同管理。它负责对跨境交易排序，验证随附的政策合规证明 (PoPC)，并发布最终结算确认。

主权合规执行层 (SCEL)：由各司法管辖区或机构自主控制的实例，作为国家 / 组织规则的数字执行终点。它负责在其法律框架内处理交易并生成 PoPC 合规证明。

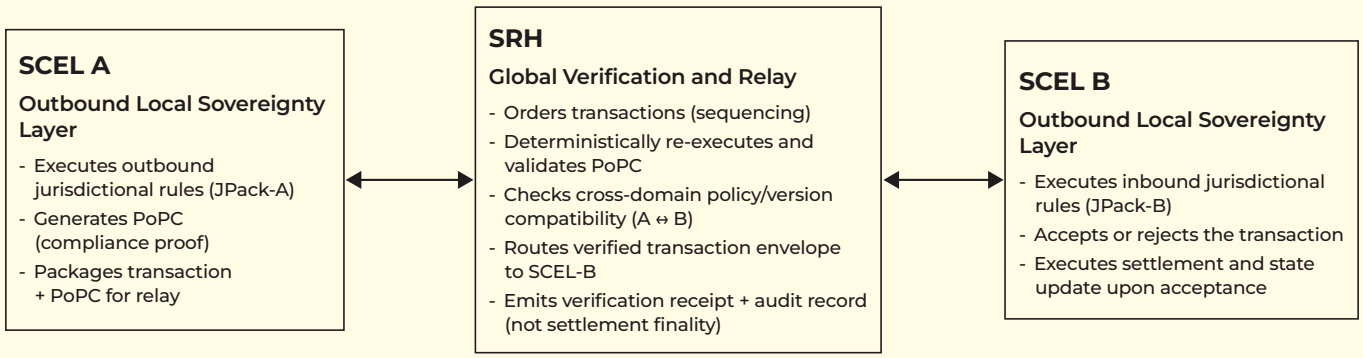


Figure 4: Functional boundary between SCEL and SRH / 图 4：SCEL 与 SRH 的功能边界

Function 功能	Executing Component 执行主体
Outbound jurisdictional compliance execution | 出境司法管辖合规执行	SCEL (Sender | 发送方)
Cryptographic proof generation (PoPC) | 密码学证明生成 (PoPC)	SCEL (Sender | 发送方)
Global recomputation and validation of PoPC | PoPC 的全局重放与验证	SRH
Cross-domain transaction routing | 跨域交易路由	SRH
Inbound jurisdictional compliance execution | 入境司法管辖合规执行	SCEL (Receiver | 接收方)
Acceptance / rejection decision | 接受 / 拒绝决策	SCEL (Receiver | 接收方)
Settlement and asset transfer | 结算与资产划转	SCEL (Receiver | 接收方)

Table 9: Layered compliance and settlement responsibility model / 表 9：分层合规与结算责任模型

(3) Stronger Proof Layers (Opt-in)

For environments requiring heightened security or privacy, the system supports:

- **TEE Attestation**: Executing PoPC within a Trusted Execution Environment produces an attestation quote. The system uses a normalized "Attestation Statement" to bridge vendor differences (Intel, AMD, ARM)[14-15,56], to enable universal verification logic across heterogeneous hardware platforms and validated against a global registry of trusted roots.
- **Zero-Knowledge Proofs (ZKP)**: Selective ZKPs demonstrate that specific predicates (e.g., AML thresholds or investor caps) were satisfied without revealing sensitive underlying data, such as specific transaction amounts[3,22].
- **Threshold or Aggregated Signatures**: For flows triggering multiple jurisdictions, N-of-M threshold signatures provide a compact[19,23], joint authorization attesting to multi-lateral compliance.

Architectural Resilience Note:
The PoPC schema is algorithm-agile, supporting seamless upgrades to post-quantum hybrid signatures. In the event of "switching its operating modes" (e.g., TEE unavailability), the PoPC record is explicitly flagged. This allows the SRH and regulators to apply additional scrutiny or limit transaction volume while maintaining universal verifiability of the base-layer fields.

(3) 增强证明层：可选的安全加固

为满足异构基础设施的需求，系统支持多种高级证明机制：

- **TEE 认证**：在硬件级隔离环境中执行 PoPC。系统通过规范化的“认证声明”屏蔽不同硬件供应商（Intel SGX, ARM TrustZone）的底层差异[14-15,56]，实现了跨硬件平台的通用验证逻辑，由全局注册表进行统一验证。
- **零知识证明 (ZK Proof)**：针对高隐私场景（如反洗钱或投资者配额上限），在不泄露敏感原始数据（如交易金额）的前提下，证明交易满足特定约束[3,22]。
- **门限与聚合签名**：针对涉及多国监管的跨境流转，采用 N-of-M 门限签名实现“联合背书”[19,23]，证明该操作已获得所有相关主权机构的授权。

架构韧性注记：
PoPC 具备“算法演进性”，支持平滑升级至后量子签名（PQC）。当高级安全层（如 TEE）不可用时，系统支持降级切换运行模式，并在 PoPC 记录中明确标注。这种设计确保了无论底层硬件环境如何变化，基础层的合规性证明始终保持完整、统一且可追溯。

A5.3

Interaction Paradigm between Sovereign Compliance Execution Layer and the Sovereign Relay Hub

跨主权合规执行 (SCEL) 与主权中继枢纽 (SRH) 的交互范式

Cross-border activity in tokenised finance (DLT-based infrastructure) requires a coordination layer that preserves the sovereignty of each participating jurisdiction while achieving shared regulatory assurance. The architecture therefore separates local execution (performed by each sovereign L2) from global verification

代币化金融（基于分布式账本）的跨境活动需要一个协同层。该层级在维护各司法辖区政策主权的同时，需达成监管确信。本架构将本地执行（由各主权合规执行层 SCEL 完成）与全

(performed by the L1 Sovereign Hub). This provides a constitutional model of "two-tier finality": jurisdictional finality for local users, and global regulatory finality for cross-border flows.

局验证（由主权中继枢纽 SRH 完成）进行逻辑解耦。这种设计确立了“两级最终性”的宪制模型：即为本地用户提供司法管辖最终性，并为跨域流动性提供全局监管最终性。

(1) SSI Cross-Border Transaction Lifecycle

(1) SSI 跨境交易的全生命周期演进

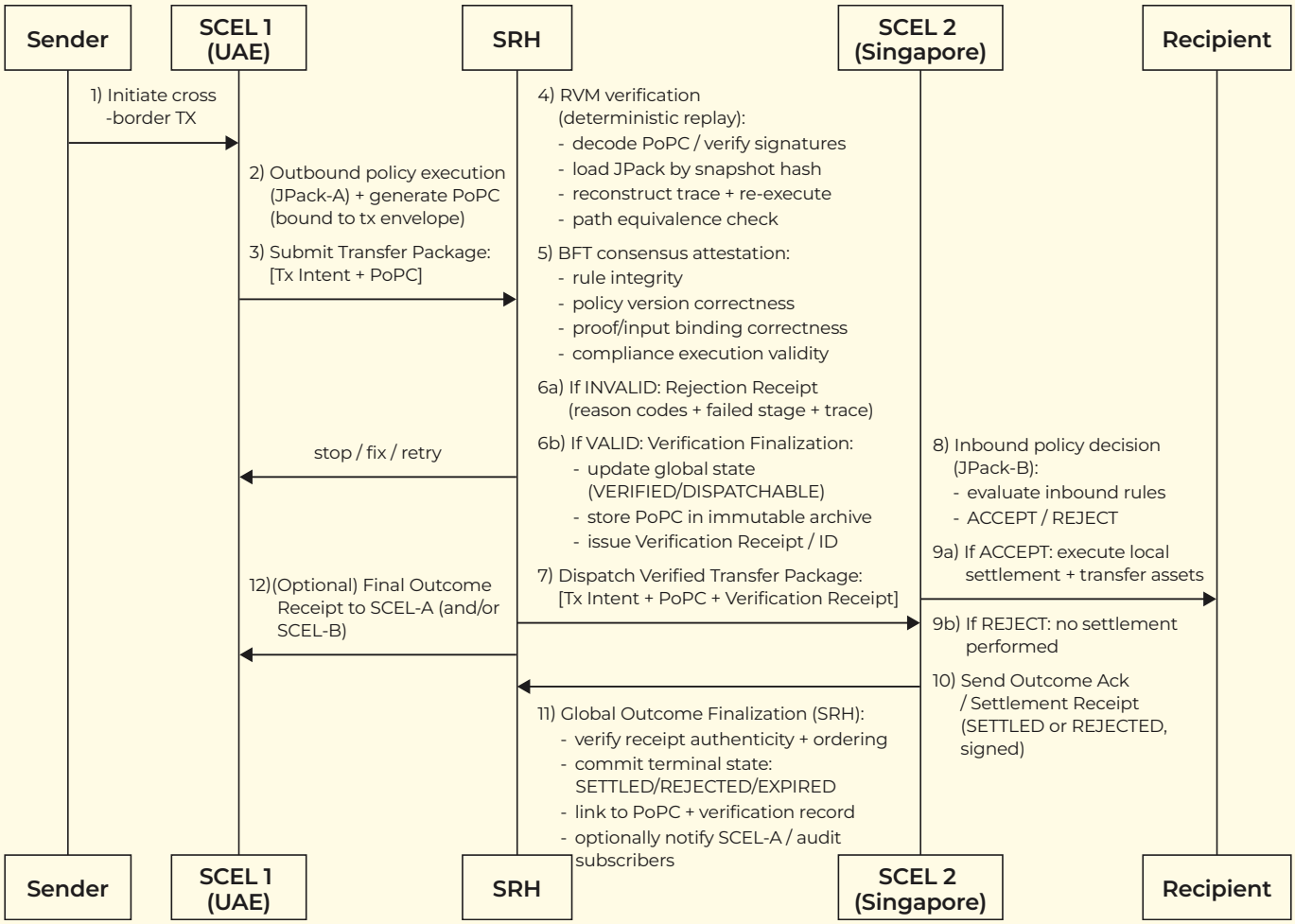


Figure 5: SSI transaction flow / 图 5：SSI 交易流程

Phase 1 - Outbound Policy Execution & Proof Attestation (SCEL-A):

The originating SCEL (e.g., UAE) evaluates the outbound transaction intent under its active JPack policy pack (JPack-A). If permitted, it generates a PoPC proof artifact bound to the transaction envelope (normalized inputs, policy snapshot/hash, and execution-trace commitments) and submits this PoPC to the SRH as the transaction's compliance attestation.

1. Sender initiates a cross-domain transfer intent (to SCEL 1).
2. SCEL 1 evaluates outbound rules under JPack-A (local compliance execution).
3. SCEL 1 generates PoPC bound to the transaction envelope

阶段一 - 出域政策执行与证明生成 (SCEL-A)：

发起方 SCEL（如阿联酋）依据其现行的 JPack，对出域交易请求进行评估。若获准通过，系统将生成一份与交易封套（涵盖标准化输入、政策快照 / 哈希以及执行轨迹承诺）深度绑定的 PoPC 证明凭证，并将其作为该笔交易的合规存证提交至主权中继枢纽。

1. 发送方发起跨域转账（至 SCEL 1）。
2. SCEL 1 依据其 JPack-A 进行出域评估（即本地合规执行）。

and policy_snapshot_hash and submits a Transfer Package to SRH: Transaction Intent + PoPC.

Phase 2 - Global Proof Verification, Consensus Attestation & Verification Finalization (SRH):

The SRH invokes the Regulatory VM (RVM) to deterministically re-execute the relevant policy logic using the pinned JPack snapshot referenced by the PoPC. SRH verifies PoPC integrity, including transaction/input binding, policy version correctness, and path equivalence (trace/outcome commitments). If verification succeeds, SRH anchors a verification-final event via BFT consensus (eg status = VERIFIED/DISPATCHABLE) and records the PoPC in an immutable compliance archive.[14-15,22-23,30-31]

4. RVM re-executes and validates PoPC (load JPack by hash, deterministic replay, input binding checks, path-equivalence/trace match).
5. BFT consensus attests the verification result (rule integrity, policy version correctness, proof/input binding correctness, compliance execution validity)

6a. If invalid → SRH returns a Rejection Receipt to SCEL 1 (reason codes + failed stage + reference/trace hash).

6b. If valid → SRH issues a Verification Receipt (VERIFIED/DISPATCHABLE) and performs Verification Finalization (record verification event/state + store PoPC in immutable archive).

Phase 3 - Cross-Domain Dispatch & Inbound Policy Decision (SCEL-B):

The SRH forwards a Verified Transfer Package (transaction intent + PoPC + SRH verification receipt/ID) to the destination SCEL (e.g., Singapore). The destination SCEL independently evaluates inbound compliance under its local JPack policy pack (JPack-B) and makes the final ACCEPT/REJECT decision. Settlement is executed only upon acceptance.

7. SRH forwards the Verified Transfer Package to SCEL 2: Transaction Intent + PoPC + Verification Receipt/ID.
8. SCEL 2 evaluates inbound rules under JPack-B and decides ACCEPT / REJECT.

Phase 4: Settlement Outcome Acknowledgement & Global Outcome Finalization (SRH):

Upon settlement (or rejection), the destination SCEL emits a signed Settlement Receipt / Outcome Act to the SRH. The SRH verifies the receipt's authenticity and ordering (anti-replay) and commits the terminal outcome to the global state tree (SETTLED

3. SCEL 1 生成与交易封套及政策快照哈希深度绑定的 PoPC，并向 SRH 提交转账数据包：其内容由交易请求与 PoPC 证明组成。

阶段二 - 全局证明验证、共识核验与终局确认（SRH）：SRH 调用监管虚拟机，基于 PoPC 所引用并固定的 JPack 快照，对相关政策逻辑进行确定性重放。SRH 验证 PoPC 的完整性，包括交易与输入绑定关系、政策版本正确性，以及执行路径一致性（执行轨迹 / 结果承诺）。若验证通过，SRH 通过 BFT 共识锚定事件（如状态标记为已验证 / 可调度），并将 PoPC 记录至不可篡改的合规档案中 [14-15,22-23,30-31]。

4. RVM 重放并校验 PoPC（通过哈希加载 JPack、执行确定性重放、检查输入绑定、匹配路径等价性 / 轨迹一致性）。
5. BFT 共识对验证结果进行存证（规则完整性、政策版本准确性、证明与输入的绑定正确性，以及合规执行有效性）。

6a. 若验证无效 → SRH 向 SCEL 1 返回“拒绝收据”（包含原因代码、失败阶段及参考 / 轨迹哈希）。

6b. 若验证有效 → SRH 签发“验证收据”（标记为“已验证 / 可调度”）并执行“验证定案”（记录验证事件与状态，并将 PoPC 存入不可篡改档案库）。

阶段三 - 跨域调度与入境政策决策（SCEL-B）：SRH 将已核验的转账包（交易意图 + PoPC + SRH 验证回执 /ID）转发至目标 SCEL（如新加坡）。接收方 SCEL 对照其本地的 JPack 政策包（JPack-B）独立评估入境合规性，并作出最终的接受 / 拒绝决策。只有在决策为接受时，系统才会执行最终结算。

7. SRH 将已验证转账转发至 SCEL 2：包含交易意图 + PoPC + 验证收据 /ID。

/ REJECTED / EXPIRED), linking it to the prior verification record and PoPC identifier. This step provides global outcome finalization.

9a. If ACCEPT → SCEL 2 executes local settlement and transfers assets to the Recipient.

9b. If REJECT → no settlement is performed.

10. SCEL 2 sends a signed Settlement Receipt / Outcome Ack to SRH (SETTLED or REJECTED, with seq/timestamp).

11. SRH performs Global Outcome Finalization:
    - verify receipt authenticity + ordering (anti-replay)
    - commit terminal outcome to Global State Tree (SETTLED/REJECTED/EXPIRED)
    - link outcome to PoPC + verification record (receipt/ID, policy snapshot hash)

12. Optionally notify SCEL 1 and/or audit subscribers (final outcome receipt/event)

Core Architectural Principles and Value Anchors:

1) **Local execution under local rules**: Each jurisdiction applies its own laws, thresholds, residency rules, and risk preferences directly at the SCEL level. The architecture ensures that technical protocols never dilute or override sovereign authority[19,31-32].

2) **Parallelism and Unification of Dual Finality**: The system provides users with the instant responsiveness of their home SCEL while endowing the transaction with a globally recognized compliance status. This eliminates the "compliance uncertainty delays" typical of legacy cross-border settlements[21,33-34].

3) **Cryptographic Proof of Compliance under Privacy Protection**: The PoPC model decouples privacy from auditability. While proving transaction compliance, PoPC attestations utilize hash masking or selective disclosure to ensure that Personally Identifiable Information (PII) and granular financial details never leave the local SCEL. This allows the system to satisfy look-through supervision requirements while adhering to the strictest data localization and privacy laws (e.g., GDPR). Entities can prove adherence to predefined rules without exposing raw financial snapshots, effectively resolving the data compliance paradox in cross-border finance[18,31,35-36].

4) **From "Middleware Intervention" to "Protocol-Level Oversight"**: The SRH elevates regulatory functions from

8. SCEL 2 依据 JPack-B 评估入域规则，并决定接受或拒绝。

阶段四 - 结算结果确认与全局结果最终确定（SRH）：在完成结算（或拒绝）后，目标 SCEL 向 SRH 发出已签名的结算回执 / 结果确认。SRH 验证该回执的真实性与顺序（防重放），并将最终结果提交至全局状态树（已结算 / 已拒绝 / 已过期），同时与此前的验证记录及 PoPC 标识进行关联。此步骤实现了全局层面的结果终局化。

9a. 若接受 → SCEL 2 执行本地结算，并将资产划转至接收方。

9b. 若拒绝 → 不执行结算。

10. SCEL 2 向 SRH 发送经签名的结算收据 / 结果确认（标记为已结算或已拒绝，包含序号与时间戳）。

11. SRH 执行全局结果终局化：
    - 核实收据真实性与时序（防重放）。
    - 将最终结果提交至全局状态树（已结算 / 已拒绝 / 已过期）。
    - 将结果与 PoPC 及验证记录（收据 / ID、政策快照哈希）进行关联存证。

12.（可选）通知 SCEL 1 及相关的审计订阅方（发送最终结果收据 / 事件）。

核心架构理念与价值锚点：

1) **基于本域规则的内生性执行**：每个司法管辖区在 SCEL 层级直接实施其原生法律与风险偏好（如准入、限额、身份限制）。该设计确保了技术协议绝不凌驾于主权权威之上 [19-31,32]。

2) **双重终局性的并行与统一**：主场 SCEL 即时响应用户，同时赋予交易全局认可的合规身份。这种设计消除了跨境结算中常见的“合规不确定性延迟”[21,33-34]。

ad-hoc "patches" to a "base protocol".[31] Through this, regulators gain:

- ◇ **Full Replayability and Version Transparency**: Supporting precise forensics and the reproduction of rule execution at any historical moment and under any specific rule version.
- ◇ **Semantic Decoupling and Digitised Accountability**: Formalising the separation between local legal interpretation and global technical verification, creating an automated accountability mechanism across jurisdictions.

5) **Structural Replacement of Correspondent Banking**: Through a unified compliance verification standard, the SCEL-SRH framework eradicates the frictions of traditional intermediary chains[21,37-38,52]:

- ◇ **Elimination of Redundant Screening**: Removing the need for intermediary banks to "second-guess" compliance or perform duplicate verifications, ending transaction holds caused by information asymmetry.
- ◇ **Automated Conflict Resolution and Real-time Finality**: Reconciling incompatible policy regimes automatically through standardised interfaces to eliminate multi-day settlement risks and achieve regulated, real-time settlement finality[53].
- ◇ **Composable Regulatory Enforcement**: Utilizing the SRH as a neutral verification venue, the system achieves a "logical intersection" of cross-jurisdictional JPack. This ensures that any transaction failing to meet bilateral compliance benchmarks is automatically identified and intercepted prior to settlement, effectively neutralizing regulatory friction across legal domains through underlying protocol logic.

The result is a cross-border settlement system characterized by real-time completion and guaranteed regulatory integrity.

(2) Internal Architecture of the Sovereign Relay Hub (SRH): Deterministic Verification Center for Compliance Logic

The SRH provides a unified Regulatory Finality Layer for all participating jurisdictions. Its core mandate is not to intervene in specific business logic, but to guarantee that cross-border asset transfers strictly adhere to the policy obligations of the sovereigns involved. The SRH architecture is organized around its constitutional functions: verifying compliance proofs (PoPC), maintaining

3) **隐私保护下的密码学合规证明**：PoPC 实现了“隐私与可审计性的脱钩”。PoPC 证明在证明交易合规的同时，通过哈希掩码或选择性披露，确保了发起方的个人身份信息（PII）和具体财务明细无需离开本域 SCEL，在满足穿透式监管需求的同时，遵守了最严格的数据本地化与隐私法律（如 GDPR）。 机构无需对外暴露详细财务快照，即可证明其行为符合预设规则，解决了跨境金融中的数据合规悖论 [18,31,35-36]。

4) **从“中间件干预”到“协议级监督”**：SRH 将监管职能从“临时补丁”升华为“底层协议”[31]。监管机构借此获得：

- ◇ **完整可重放性与版本透明度**：支持对任何历史时刻、任何规则版本的执行现场精确溯源与重现。
- ◇ **语义解耦与数字化问责**：实现本地法律解释权与全局技术验证权分离，构建跨法域的自动化问责机制。

5) **代理行模式的结构性替代**：通过统一的合规验证标准，SCEL- SRH 体系彻底消除传统中介链条的摩擦 [21,37-38,52]：

- ◇ **免除重复审查与冗余验证**：无需中介行对合规性再次评估，消除因信息不对称导致的交易挂起。
- ◇ **自动化冲突消解与实时终局性**：通过标准接口自动消解政策间的冲突，消除多日结算的流动性风险，实现受监管保障的实时结算终局 [53]。
- ◇ **可组合监管执行**：SRH 作为中立验证场，实现对跨域 JPack 的逻辑交集。不合规交易结算前即被拦截，从底层协议消除法域摩擦。

实现：实时完成、受监管保障的跨境结算体系。

the global regulatory state, and ensuring that sovereign policy packs (JPack) are executed within a transparent and supervised environment.

Key Components and Execution Logic Flow
关键组件与执行流转路径

(2) 主权中继枢纽（SRH）内部架构：合规逻辑的确定性验证中心

SRH 为参与辖区提供统一的监管终局性层。其核心职能并非介入具体的业务逻辑，而是确保跨境资产转移在程序上绝对符合相关主权国家的政策约束。SRH 架构围绕其宪法性职能构建：验证 PoPC 、维护全局监管状态、并确保 JPack 在透明且受监督的环境中执行。

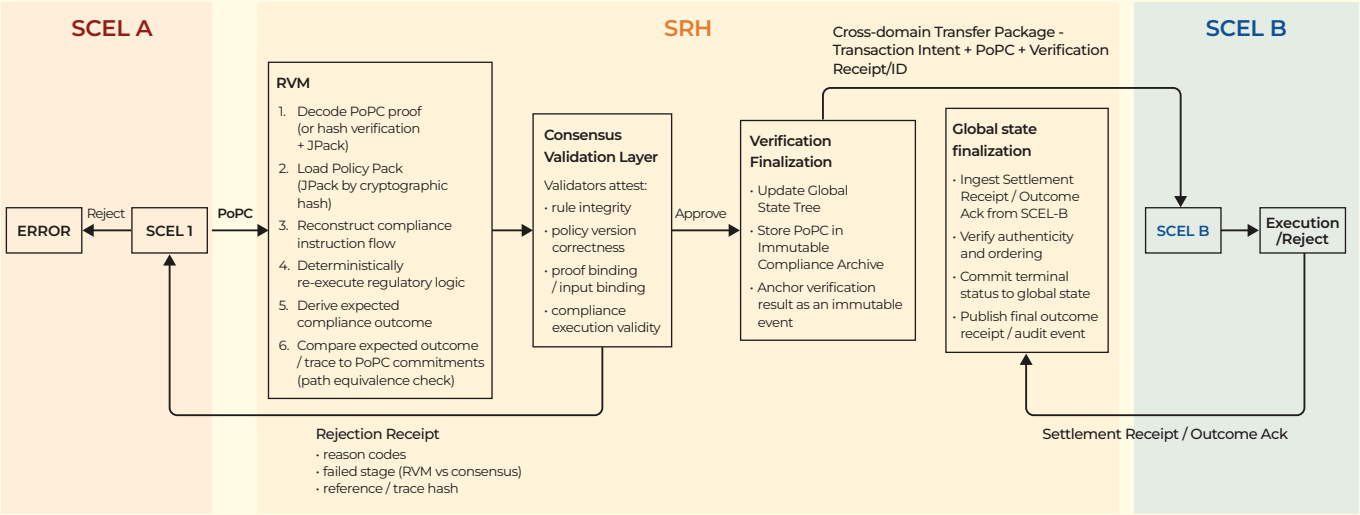


Figure 6: SRH logic flow / 图 6：SRH 逻辑流程

Key components and data flow:

1. **Sequencing Pipeline (SRH, upstream):** Cross-domain requests carrying PoPC proofs propagate through the P2P network layer. Validators ingest messages into local mempools for structural validation and anti-replay checks before they enter the ordering queue. Sequencing produces a canonical transaction order so all nodes evaluate identical inputs under identical ordering constraints (mitigating timestamp attacks and ordering ambiguity).
2. **Verification (SRH): Deterministic Re-execution via Regulatory VM (RVM).** Each request is re-verified by the RVM. The RVM decodes the PoPC artifact, verifies binding to the transaction envelope (signatures/timestamps/sequence numbers), loads the exact JPack referenced by the policy snapshot hash, reconstructs the compliance instruction trace, and deterministically re-executes the policy logic. A request proceeds only if the reconstructed execution path and outcome match the PoPC commitments (path equivalence).
3. **Consensus: Global Synchronization and Locking of Compliance Outcomes.** The BFT consensus engine provides final confirmation of the RVM's evaluation. Consensus (SRH): Network-wide Verification Attestation. The BFT consensus layer confirms the RVM evaluation and synchronizes a network-authenticated verification seal. Validators attest policy

核心组件与数据流向：

1. **排序流水线（SRH 上游）：**携带 PoPC 的跨域请求通过 P2P 网络层传播。验证节点在消息请求进入排序队列前，先将其录入本地内存池，进行结构化校验和防重放检查。排序会生成规范的交易顺序，确保所有节点在相同排序约束下评估相同的输入（抵御时间戳攻击并消除排序歧义）。
2. **验证（SRH）：通过监管虚拟机（RVM）的确定性重放。**每一笔请求都会由 RVM 进行重新验证。RVM 解码 PoPC 凭证，核验其与交易封装（签名、时间戳、序列号）的绑定关系，加载由政策快照哈希引用的特定 JPack，重构合规指令追踪，并对政策逻辑进行确定性重放。只有当重构的执行路径与 PoPC 的承诺完全一致（路

version correctness, rule integrity, proof/input binding correctness, and reproducibility of the compliance outcome. This yields verification-finality (e.g. VERIFIED/DISPATCHABLE), not settlement finality.

4. **Verification Finalization & Immutable Archiving (SRH, pre-settlement):**
   - ◇ State Tree Update (verification state): The global state tree is updated with verification metadata (policy snapshot hash, PoPC/CCID, verification receipt ID, trace commitments), anchored via a Merkle root.
   - ◇ PoPC (proof) Retention: PoPC artifacts are stored/committed to an immutable archive to enable future forensic reconstruction under the same historical policy snapshot.
5. **Cross-domain Dispatch (SRH → SCEL-B):** The SRH forwards a Cross-domain Transfer Package (Transaction Intent + PoPC + Verification Receipt/ID) to the destination SCEL.
6. **.Inbound Decision & Settlement (SCEL-B):** Upon receipt, the destination SCEL performs inbound compliance evaluation against its local JPack and makes the final ACCEPT/REJECT decision. Settlement is executed only upon acceptance.
7. **Global Outcome Finalization (SRH, post-settlement):** SCEL-B returns a signed Settlement Receipt / Outcome Ack. SRH verifies authenticity and ordering and commits the terminal outcome (SETTLED / REJECTED / EXPIRED) to the global state, linking it to the earlier verification record and PoPC identifier, and optionally emits a final outcome receipt/audit event.

Th Regulatory VM internals (right side of Figure 6) show the PoPC toolchain in action:
PoPC Decoder → Policy Pack Loader → Compliance Instruction Set → (Verification State) Reader/Writer.

(3) Systemic Pillars: Persistence and Governance

The stability and regulatory integrity of the SRH rest upon two parallel core pillars[58-63]:

I. Data Persistence Infrastructure:

This layer serves as the physical foundation of trust, ensuring the long-term survival and traceability of regulatory data:

- **Sovereign Registry**: Maintains the canonical list of participating jurisdictions and locks the version hashes of their currently active JPack.
- **Global State Tree**: A shared Merkle-tree-based ledger

径等效性）时，该请求方可进入后续流程。

3. **共识：合规结果的全局同步与锁定**。BFT 共识引擎对 RVM 的评估结果进行最终确认，实现网络范围内的同步与锁定。共识（SRH）：全网验证认。BFT 共识层确认 RVM 的验证结论，并同步一个经网络认证的验证印鉴。验证节点共同见证政策版本的正确性、规则的完整性、证明与输入的绑定正确性，以及合规结果的可复现性。此环节实现的是验证终局性（例如已验证 / 可调度），而非结算终局性。
4. **验证终局与不可篡改归档（SRH, 结算前）**
   - ◇ **状态树更新（验证状态）**：全球状态树通过默克尔根锚定，更新验证元数据（政策快照哈希、PoPC / CCID、验证回执 ID、执行轨迹承诺）。
   - ◇ **PoPC（证明）留存**：PoPC 被存入并提交至不可篡改档案，以便日后同项历史政策快照下法证回溯与重构。
5. **跨域调度（SRH → SCEL-B）：**SRH 向目标 SCEL 转发跨域转账包（交易意图 + PoPC + 验证回执 /ID）。
6. **入境决策与结算（SCEL-B）：**目标 SCEL 在收到转账包后，对照其本地 JPack 入境合规评估，并做出最终的接受 / 拒绝决策。只有在确认接受后，才会执行结算操作。
7. **全局结果最终确认（SRH，结算后）：**SCEL-B 返回一份已签名的结算回执。SRH 校验其真实性与顺序，并将终态结果（已结算 / 已拒绝 / 已过期）提交至全局状态，与验证记录和 PoPC 标识符关联。

监管虚拟机内部结构（图 6 右侧）展示了 PoPC 工具链的运行情况：
PoPC 解码器 → 策略包加载器 → 合规性指令集 →（验证状态）读 / 写器。

recording cross-jurisdictional settlement states, such as asset balances and systemic legal obligations.

- **Cross-chain Transaction Archive**: An immutable, append-only log preserving all transaction artifacts and PoPC proofs for long-term audit and forensic replay.
- **General Data Store**: Provides flexible storage for key-value pairs and structured metadata required for evolving network needs.

II. Governance Module:

All adjustments to systemic parameters and functional expansions are managed by dedicated governance modules, ensuring every action is fully auditable:

- **Parameter & Module Management**: Facilitates dynamic adjustments to system-level parameters and the integration of new functional modules.
- **Lifecycle Governance**: Oversees the onboarding/offboarding of SCELs, the formal replacement of JPack versions, the definition of new policy categories, and revisions to "constitutional primitives".

(4) Summary: Harmonising Sovereign Will with Digital Efficiency

This architecture enables SCELs to provide immediate local finality while relying on the SRH to anchor global regulatory finality. The SRH guarantees that every cross-border transaction simultaneously achieves:

1. Formally Verifiable proofs of policy compliance.
2. Precision Validation according to the exact jurisdictional rules.
3. Retention in a privacy-preserving, immutable audit layer.
4. Mutual Recognition by all involved sovereign authorities.

The final result is a deep integration of the sovereign authority of national regulators with the operational demands of real-time tokenised finance, fundamentally eliminating the structural latencies and frictions inherent in traditional correspondent banking.

(3) 系统支撑架构：持久化与治理

SRH 的稳定性与合规公信力建立在以下两大并列的核心支撑组件之上 [58-63]：

一、数据持久化底座：

该层级构成 SRH 的物理信用基础，确保监管数据的长期生存与可追溯性：

- **主权注册表**：维护参与辖区的规范化列表，并锁定其生效的 JPack 版本哈希。
- **全局状态树**：一个基于默克尔树的共享账本，记录跨司法辖区的结算状态，如资产余额与系统性法定义务。
- **跨链交易档案库**：一个不可篡改、仅可追加的日志系统，完整存储交易凭证与 PoPC 证明，用于长期合规审计与重放。
- **通用数据存储**：动态存储网络运行所需的键值对数据及其他结构化辅助信息。

二、治理执行模块：

系统治理参数的变更及功能扩展均由治理模块统一处理，确保治理行为具备完整的审计追踪：

- **参数与规则变更**：处理系统级治理参数的动态调整及新功能模块的接入。
- **生命周期管理**：执行 SCEL 的准入 / 退出、JPack 版本的正式更替、新政策类别的定义以及底层宪法原语的修订。

(4) 综述：主权意志与数字效率的平衡

该架构允许各辖区 SCEL 为用户提供即时的本地最终性，同时依托 SRH 锚定全局性的监管最终性。SRH 确保每一笔跨境交易同时具备：

1. 形式化可验证的合规性证明。
2. 根据正确的主权规则进行精准验证。
3. 记录在审计层中。
4. 获得所有参与主权国家的一致认可。

最终实现：将国家监管机构的主权意志与现代实时代币化金融的运营需求深度融合，消除了传统代理银行模式的结构性延迟与协作摩擦。

A5.4

Core-DSL:
A Minimal, Deterministic Policy Language

核心领域专用语言 (Core-DSL)：
一种极简且确定性的策略语言

The Core Domain-Specific Language (Core-DSL) is deliberately tiny and domain-specific, focusing on building the **semantic foundation** for cross-border settlement and FX regulation. Its vocabulary is limited to concepts that repeatedly appear in supervisory workflows and maintains deep semantic alignment with the MAS Project Guardian prototypes, Swiss SBDT policy templates, and Deutsche Bank's DAMA framework[14-15].

All of these frameworks rely on nuanced entity-relationships and supervisory workflows[39]. As the ecosystem evolves, a structured process under the Sovereign Registry may determine which categories graduate into the Core-DSL and which remain optional extensions.

核心领域专用语言（Core-DSL）刻意保持精简，专注于构建跨境结算与外汇监管的**语义基石**。其词汇集高度浓缩了监管工作流中反复出现的关键概念，并与新加坡金融管理局（MAS）的“守护者计划”、瑞士证券型 DLT 政策模板以及德意志银行 DAMA 框架保持高度的语义一致性[14-15]。

所有这些框架都依赖于精细化的实体关系和监管工作流程[39]。随着生态系统的演进，主权注册机构下的结构化流程可能会决定哪些类别将纳入 Core-DSL，哪些类别仍作为可选扩展。

(1) Regulatory Primitives

(1) 监管原语

Primitive 原语	Meaning / Examples 含义 / 示例
subject **主体**	Initiating legal or natural person (e.g., individual, corporate entity, regulated institution). 发起交易的法人或自然人（如：个人、公司实体、受监管机构）。
counterparty **对手方**	Receiving person or institution; the other party to the transaction. 接收交易的个人或机构；交易的另一方。
residency **居民身份**	Regulatory or tax residency of subject and counterparty; used for jurisdictional applicability. 主体和交易对手的监管或税务居住地；用于确定管辖权。
citizenship **国籍**	Passport-level nationality; relevant for sanctions, restricted countries, and capital controls. 护照级别的国籍；与制裁、受限国家和资本管制相关。
geography **地理位置**	Declared or inferred location (e.g., ISO-3166 codes, IP-derived region) used in certain cross-border policies. 某些跨境政策中使用的已声明或推断位置（如：ISO-3166 代码、IP 地址派生区域）。
asset **资产**	Nature of the tokenised instrument (e.g., USD stablecoin, SAR CBDC, tokenised deposit, tokenised gold). 代币化工具的性质（如：美元稳定币、沙特里亚尔央行数字货币、代币化存款、代币化黄金）。

product_type **产品类型**	Classification of the financial product or transaction type (spot FX, forward, deposit, security token, etc.). 金融产品或交易类型的分类（如：即期外汇、远期、存款、证券型代币等）。
amount **金额**	Transaction size in native units or harmonised fiat equivalent. 以本地货币单位或等值法定货币表示的交易规模。
frequency **频率**	Number of actions within a defined time window (e.g., "5 transfers per day"). 在特定时间窗口内的操作次数（如："每天 5 笔转账"）。
time_window **时间窗口**	Business hours, settlement cut-offs, reporting cycles, cooling-off periods. 营业时间、结算截止时间、报告周期、冷静期。
risk_score **风险评分**	Internal AML/CTF risk tier or institution-assigned risk category. 内部反洗钱 / 反恐融资风险等级或机构指定的风险类别。
list_status **名单状态**	Sanctions and politically exposed person indicators (SDN, PEP, watchlist, frozen accounts). 制裁和政治公众人物指标（特别指定国民名单、政治公众人物、观察名单、冻结账户）。

Table 10: Compliance input primitives and their semantics / 表10：合规性输入原语及其语义

(2) Deterministic Evaluation Model: Side-Effect-Free Pure Functions

In the Core-DSL, all rules are defined as **pure functions**: they take a normalized transaction envelope as input and produce exactly one of three deterministic outcomes:

ALLOW: Transaction meets current compliance benchmarks and may proceed.

HOLD: Transaction triggers a preset alert, requiring manual review or additional data.

REJECT: Transaction is forbidden under current policy and triggers a compliance anchor.

Architectural Characteristics:

- **Computational Determinism**: Evaluation is strictly side-effect-free, excluding randomness, network calls, or clock access.
- **Execution Immutability**: Rules execute in constant time. This guarantees that the same transaction, evaluated against the same policy pack on any node (or during a forensic audit years later), will always yield a bit-identical result.

(3) Core-DSL Evolutionary Roadmap and Regulatory Compatibility

While the current primitive set constitutes a strong and intentionally minimal foundation, the design provides ample room for

(2) 确定性评估模型：无副作用的纯函数

在 Core-DSL 中，所有规则均被定义为**纯函数**。它们以标准化的交易封装为输入，并输出确定的三态结果：

ALLOW（放行）：交易完全符合当前合规基准，可即时执行。

HOLD（挂起）：触发预警，需人工干预或补充合规性数据。

REJECT（拒绝）：违反强制策略，交易被禁并触发合规锚点。

架构特性：

- **计算确定性**：评估过程严禁随机性、网络调用或动态时钟访问。
- **执行恒定性**：执行时间恒定，确保无论是在实时环境中还是在多年后的审计回溯中，针对同一法规要件集产生的输出永远一致且可复现。

(3) 核心策略声明语言（Core-DSL）的演进路线图与监管兼容性

expansion to cover a wider range of global FX and cross-border regulatory strategies.

1. **Deep Alignment with Global Regulatory Frameworks:** The underlying semantics of Core-DSL are deconstructed to ensure compatibility and alignment with major international standards:
   - **Multilateral Alignment**: Reflecting requirements from the EU AMLR, MAS PS Act, HKMA Stablecoin Regime, and the US BSA/Travel Rule[3,5,8-9,34].
   - **Standard Interoperability**: Incorporating core elements from SWIFT CBPR+ rules, corporate treasury FX policies, and ISO 20022 frameworks[38,40-42].
2. **Future Expansion:** From Instruction Sets to Complex Semantics As the DSL matures, the roadmap prioritises three critical evolutionary dimensions:
   - **Procedural and Supervisory Actions**: Recognising that real-world policies are not merely binary, future updates will introduce dedicated primitives for procedural outcomes, such as mandatory reporting to authorities, escalation to second-level compliance review, and trigger-based notifications for cross-border capital flows[22,31-32].
   - **Entity-Relationship Primitives**: To advance "look-through" supervision, the DSL will incorporate explicit reasoning for relationships, including Beneficial Ownership Structures (UBO), intra-group transfers, and layered remittance arrangements. These explicitly affect transaction thresholds and Enhanced Due Diligence (EDD) requirements[3,8,43].
   - **Business and Purpose Codes**: Integrating standardized purpose codes (e.g., trade settlement, dividend distribution, or payroll). Introducing a "regulatory purpose class" primitive will simplify the modelling of obligations triggered by specific payment types, such as trade finance or capital account reporting[16,37,41].

This closing of the loop ensures that all participating jurisdictions obtain a cryptographically authenticated and regulatorily verified settlement anchor.

虽然目前的 Core-DSL 规则集构成了强大且精简的治理基础，但其设计预留了充足的扩展空间，以涵盖更广泛的全球外汇与跨境监管策略。

1. **全球主流监管框架深度兼容**。Core-DSL 的底层原语通过对主要法域监管要求的解构，实现对以下框架的深度兼容与对齐：
   - **多边监管对齐**：参考了欧盟反洗钱条例（AMLR）、新加坡 MAS《私人证券法》、香港 HKMA 稳定币制度、及美国《银行保密法》（BSA）/ 旅行规则 [3,5,8-9,34]。
   - **行业标准互操作**：涵盖了 SWIFT 跨境资金交易规则、企业外汇管理政策、以及 ISO 20022（跨境支付与报告 Plus）中的核心要素 [38,40-42]。
2. **未来扩展方向：**从指令集到复杂语义。随着 DSL 迈向成熟，其路线图将涵盖以下三个关键维度的深度演进：
   - **程序性与监管措施**：现实政策并非仅限于“准入 / 禁止”，未来将引入专门的原语类别以支持更清晰的程序语义，例如：强制性监管报告触发、分级合规审查升级、以及基于触发条件的跨境资金流动预警通知 [22,31-32]。
   - **实体关系原始属性**：为了应对穿透式监管，DSL 将引入对实体间关系的逻辑识别，包括：实际受益人（UBO）结构、集团内关联方识别以及多层第三方代付安排。这些关系将直接影响交易阈值评估与强化尽调（EDD）要求 [3,8,43]。
   - **业务用途与目的代码**：整合如贸易结算、股息分配、工资发放等业务目的码。通过引入“监管用途类别”原语，简化基于不同用途（如贸易融资）而触发的特定报告分类与合规建模 [16,37,41]。

这一逻辑闭环，确保了参与辖区均能持有一个兼具密码学验证与监管审定性的结算锚点。

A5.5

Jurisdiction Packs (JPack): Policy-as-Data and Versioned Governance

Rather than hard-coding thousands of volatile national regulations into the protocol layer, the architecture introduces the JPack (Jurisdictional Policy Pack) mechanism. A JPack is a policy encapsulation uniquely digitally signed by each jurisdictional regulator or its authorized trusted entities. It translates local legal provisions into executable Core-DSL syntax, enabling the decoupling of regulatory intent from technical execution.

(1) JPack Composition and Identification Examples

Each JPack is a self-contained compliance logic package. Identifiers follow a rigorous naming convention (illustrative examples for the 2025–2026 era):

SG-MAS-PSD3-2025.11

SA-SAMA-AML-2025.08

EU-MiCA-Compliance-2025.06

US-OCC-TravelRule-2025.04

CN-SAFE-FXControls-2025.Q3

A standard JPack comprises the following core elements:

- **Authoritative Metadata**: Including issuer identity, effective/expiry dates, and multiple cryptographic signatures.
- **Core-DSL Logic Library**: Rule files written in Core-DSL, optimized for specific jurisdictional scenarios.
- **Parameters and Dynamic Lists**: Including specific numeric thresholds and real-time updated allow/deny lists.
- **Human-Readable Legal References**: Direct mappings of technical rules to legal statutes to ensure transparency and "procedural justice".
- **Golden Test Vectors**: A set of minimal transaction examples with expected ALLOW/HOLD/REJECT outcomes used to verify consistent execution across all network nodes.

司法管辖区法规要件集（JPack）：政策即数据与版本化治理

为了避免将海量且多变的国家监管规则硬编码至底层协议，本架构引入了 JPack 机制。JPack 是由各司法辖区监管机构或其授权的受信任实体进行唯一数字签名的法规要件集封装。它将本地法律条文转化为 Core-DSL 可执行语法，实现了监管意图与技术执行的解耦。

(1) JPack 的构成与标识示例

每个 JPack 都是一个自包含的合规逻辑包，其标识遵循严格的版本命名规范（以 2025–2026 周期为例）：

SG-MAS-PSD3-2025.11

SA-SAMA-AML-2025.08

EU-MiCA-Compliance-2025.06

US-OCC-TravelRule-2025.04

CN-SAFE-FXControls-2025.Q3

一个标准的 JPack 包含以下核心要素：

- **权威元数据**：包括发行者身份、生效 / 失效日期及多重加密签名。
- **DSL 逻辑库**：使用 Core-DSL 编写的、针对本域场景优化的逻辑规则。
- **参数集与动态名单**：包括具体数值阈值、实时更新的白名单与黑名单。
- **法律文本映射**：为每一条技术规则提供易于人类理解的法律条文引用，确保“程序公正”。

(2) Version Evolution and Governance Constraints

The activation and upgrade of a JPack are treated as **explicit governance events** on the Sovereign Relay Hub (SRH). To ensure the continuity and security of the compliance path, the system enforces the following mandatory constraints[64]:

- **Monotonic Progression Verification**: Network nodes must fetch policies from the authoritative registry to ensure that version numbers are strictly monotonically increasing. This mechanism provides the system with anti-rollback capabilities, preventing the malicious injection of legacy policy versions to bypass updated regulatory constraints.
- **Anti-Rollback Protection**: The current active version is locked via the consensus mechanism; any attempt to revert to previous rules (which may contain known vulnerabilities) is rejected at the protocol level.
- **Deterministic Pre-validation**: Before a new version becomes active, nodes utilize the Golden Test Vectors to perform pre-execution validation, guaranteeing network-wide consistency in logic application.

- **黄金测试向量**：一组包含预期 ALLOW/HOLD/REJECT 结果的标准交易示例，用于验证节点执行的一致性。

(2) 版本演进与治理约束

JPack 的激活与升级被视为 SRH 上的**显式治理事件**。为确保合规路径的连续性与安全性，系统强制执行以下约束 [64]：

- **单调递增性验证**：网络节点必须从权威注册表拉取策略，确保版本号严格单调递增。这种机制赋予了系统“抗回滚攻击”的能力，防止旧版本策略被恶意注入以绕过新版监管约束。
- **抗回滚攻击**：通过共识机制锁定当前生效版本，任何试图恢复旧有漏洞规则的尝试都将被协议层拒绝。
- **确定性预热**：在新版本生效前，节点利用测试向量进行预执行验证，确保全网逻辑的一致性。

A5.6

Execution Model inside the Regulatory VM: Dual Verification and Separation of Trust

监管虚拟机内的执行模型：双重验证与信任分离

The Regulatory VM operates as a dedicated, independent compliance engine, running alongside the blockchain's normal state machine. It interfaces with the ledger through a lightweight adapter module, achieving the decoupling of regulatory logic from business logic.

监管虚拟机（Regulatory VM）是一套专用的合规引擎，独立于区块链的常规状态机运行。它通过一个轻量级适配模块与底层账本交互，实现监管逻辑与业务逻辑的解耦。

(1) Responsibilities of the Lightweight Module

Passing normalized envelopes into the RVM:

It feeds the sanitized transaction envelope (with private fields redacted or standardized) into the Regulatory VM or evaluation against the policy rules.

Storing the active JPack version:

It maintains a reference to the currently active jurisdictional policy pack (JPack) version, ensuring the VM uses the exact rule set in force for the transaction's jurisdictions.

Persisting PoPC proof:

It records the resulting Proof-of-Policy-Compliance (PoPC) proof on-chain, preserving a tamper-evident audit trail of the VM's decision process for future verification or replay.

Emitting events:

It emits relevant events to signal outcomes or alerts (e.g. compliance approvals, rejections, or anomalies), enhancing transparency and notifying other parts of the system or off-chain observers.

(2) Execution Lifecycle: The Two-Phase Verification Model

Phase I: SCEL Initiation and Proof Generation (Diagram 1) When a Sovereign Compliance Execution Layer (SCEL) initiates a transaction, the workflow begins locally within its own environment. The lightweight module orchestrates the following steps:

1) **Local Execution**: Execute the transaction against the SCEL's own ledger state, producing a provisional state update. This ensures the transaction is valid in that jurisdiction's context before any cross-chain activity occurs.
2) **Policy Evaluation**: The Regulatory VM, using the SCEL's active JPack, deterministically evaluates the transaction's envelope against all applicable compliance rules. The outcome is a compliance decision (e.g. ALLOW or DENY) accompanied by a detailed decision trace (which rules fired and why). This execution is pure and deterministic - given the same inputs and policy pack, the VM will always produce the same decision and trace.
3) **Proof Attachment**: If the decision is ALLOW, the SCEL pallet collects the VM's output - a PoPC proof blob capturing the policy snapshot hash, normalized inputs, rule-fired trace, reason codes, timestamps, and signature - and attaches this proof to the transaction. The transaction, now augmented with a cryptographic proof of compliance, is

(1) 轻量级适配模块的核心职责：

传递标准化封装：

将清洗后的交易封装（敏感字段已脱敏）输入监管虚拟机，对照策略规则进行评估。

存储活跃 JPack 版本：

维护对当前活跃 JPack 版本的引用，确保使用所属辖区的现行规则集。

证明持久化：

将生成的 PoPC 写入链上，保留防篡改的审计轨迹，供未来验证或回放。

事件广播：

通过发出相关事件（如合规通过、拒绝、异常提示）通报结果，增强透明度并通知链下观察者。

(2) 执行生命周期：两阶段验证模型

第一阶段：SCEL 发起与本地证明生成（图 1）

当 SCEL 发起交易时，轻量级模块在本地环境启动以下流转：

1) **本地执行**：针对 SCEL 自身的账本状态执行交易，生成临时状态更新。这确保了在发生任何跨链活动之前，该交易在本地辖区的语境下是有效的 。
2) **政策评估**：监管虚拟机使用 SCEL 活跃的 JPack，对交易封装进行确定性评估，是否符合所有适用的合规规则 。结果是一个合规决策（如放行或拦截），并附带详细的决策轨迹（即触发了哪些规则及其原因）。这种执行是纯粹且确定性的，只要输入和法规要件集相同，虚拟机将永远产生相同的决策和追踪 。
3) **证明附加**：如果决策是“放行”，SCEL 模块会收集虚拟机的输出，生成 PoPC 合规证明（包含：政策快照哈希、标准化输入、规则触发追踪、原因代码、时

submitted out of the SCEL up to the Sovereign Relay Hub for global processing. (If the decision is DENY, the transaction is aborted locally and no cross-chain submission occurs.)

Phase II: SRH Independent Verification and Global Finality (Diagram 2) Upon receiving the transaction and its attached PoPC, the SRH performs an independent verification using its own instance of the Regulatory VM through "Mirror Verification":

1) **Mirror Retrieval and Replay**: The SRH first retrieves the appropriate JPack version (via the policy_snapshot_hash) to mirror exactly the rules applied on the SCEL. It then feeds the normalized envelope and PoPC into the RVM for a full replay. Due to the deterministic nature of Core-DSL and the cryptographic pinning of policy versions, the SRH result must be identical to the SCEL result. PoPC versioning and compatibility constraints are evaluated in accordance with configured system parameters and the specific interaction modality (intra-entity transfer, inter-entity transfer, or cross-jurisdictional transfer).

2) **Execution Outcomes**:

- **Match the SCEL decision (expected case)**: The SRH VM reproduces the exact same decision (ALLOW) and rule trace as reported by the SCEL. This byte-for-byte confirmation means the transaction adhered to all applicable policies, and the SCEL's compliance claim was truthful. The SRH then proceeds to finalize the transaction in the global state, achieving cross-chain consensus. The thin pallet emits an event (e.g. ComplianceVerified) to record that the cross-border transfer was validated under the correct policy pack, cementing an auditable record.
- **Diverge from the SCEL decision (error case)**: The SRH VM's result does not match the SCEL's decision or trace - indicating a compliance violation or a potential attempt at fraud. In this case, the Sovereign Hub immediately rejects the transaction as non-compliant. No global state update is performed. An alert event is emitted to flag the discrepancy, and the issue can be investigated (the persisted PoPC proof and trace facilitate forensic analysis of where the execution diverged).

(3) Core Security Guarantees

This two-phase, dual-execution model (SCEL first, then SRH) provides strong guarantees:

间戳和签名等），并将其附加到交易中。此时，交易已携带密码学合规证明，随后被提交至 SRH，进入全局处理流程。（如果决策是“拒绝”，交易在本地即被中止，不会发生跨链提交）。

第二阶段：SRH 独立复核与全局确认（图 2） SRH 接收交易后，利用自身的监管虚拟机实例执行“镜像验证”：

1) **镜像检索与重放**：SRH 首先检索相应的 JPack（通过 policy_snapshot_hash），以精确镜像 SCEL 上应用的规则。随后 SRH 将交易封装与 PoPC 输入 RVM 进行完整重放。由于 Core-DSL 的确定性，SRH 的执行结果必与 SCEL 完全一致。PoPC 的版本化机制与兼容性约束，须与系统参数及具体的交互范式（包括实体内流转、跨实体流转或跨司法辖区流转）进行协同评估。

2) **结果处理路径**：

- **预期情况（结果一致）**：SRH 虚拟机复现了与 SCEL 报告完全相同的决策（放行）和规则轨迹。这种字节级的确认意味着交易遵守了所有适用策略，且 SCEL 的合规声明是真实的。随后，SRH 将该交易写入全局状态，达成跨链共识。轻量级模块发出相应事件（如 ComplianceVerified），记录该跨境转账已在正确的法规要件集下通过验证，形成可审计的记录。
- **错误情况（决策偏离）**：SRH 虚拟机的执行结果与 SCEL 的决策或追踪不匹配，意味着存在合规违规或潜在的欺诈企图。在此情况下，SRH 将立即拒绝该交易，视其为不

- **Determinism**: Guaranteed by the Regulatory VM's design: given the same inputs and policy pack, both SCEL and SRH produce the same compliance outcome, enabling the SRH to serve as an impartial checker of SCEL decisions.
- **Auditability**: Built-in via the persisted PoPC proof - any stakeholder or regulator can later replay the exact compliance evaluation knowing it will yield the same result, or verify the proof off-chain with open tooling[54-55].
- **Separation of Trust**: Each SCEL executes policies on its own (maintaining local sovereignty and instant local finality), but no SCEL's verdict is taken on faith. The Sovereign Relay Hub independently re-verifies every transaction before global finality, acting as a neutral guarantor that all jurisdictions' rules were correctly enforced.

This layered execution approach ensures that cross-border transactions are both locally compliant and globally consistent under one unified framework.

合规。不进行任何全局状态更新，并发出告警事件标记该差异。并可对问题进行调查（持久化的 PoPC 证明和跟踪信息有助于对执行偏离点进行取证分析）。

(3) 核心安全性保证

这种两阶段、双重执行模型（先 SCEL，后 SRH）为确定性、可审计性和信任分离提供了强有力的保证。

- **确定性**由 RVM 的设计所保障：在相同的输入和 Jpack 条件下，SCEL 和 SRH 必然产生相同的合规结果，使 SRH 能够作为 SCEL 决策的公正验证者。
- **可审计性**通过 PoPC 的链上持久化得以保障：任何利益相关方或监管机构都可以在事后重放完整的合规评估过程，并确信其结果相同，或者使用开源工具在链下验证该证明[54-55]。
- **信任分离清晰**：每一条 SCEL 自主执行本域政策，为用户提供即时的本地最终性，但其结论不会被无条件采信；所有跨司法辖区交易，均须经 SRH 在自身 RVM 中独立复核方可获得全局最终性。

这种通过轻量级模块与监管虚拟机协同实现的分层执行方法，确保跨境交易在一个统一的框架下，既符合本地法规又符合全球一致性。

A5.7

PoPC Proof Format & Toolchain

PoPC 证明格式与工具链

The Proof-of-Policy-Compliance (PoPC) format is not a generic zero-knowledge proof; rather, it is a **transparent, replayable audit trail specifically engineered for regulatory and compliance use cases. A complete PoPC record contains a fixed set of core fields, with optional extensions tailored for complex FX and AML workflows**, as summarized below:

政策合规证明并非通用的零知识证明，而是一种**透明、可重放的审计轨迹，专为监管与合规场景设计。一份完整的 PoPC 记录包含一组固定的核心字段，并针对复杂的外汇（FX）与反洗钱（AML）流程提供可选扩展字段。**

(1) Summary of Core and Extended Fields

(1) PoPC 核心与扩展字段摘要

Field 字段	Purpose 用途
policy_snapshot_hash **策略快照哈希**	Keccak-256 hash of the exact policy pack (JPack) and parameter set used for the evaluation. 评估时所使用的具体 JPack 及参数集的 Keccak-256 哈希值。
normalized_inputs **规范化输入**	Redacted transaction envelope, with private or sensitive fields zeroed out or hashed for privacy preservation. 经过脱敏处理的交易封装，其中隐私或敏感字段已被置零或哈希处理，以保护数据隐私。
decision_trace **决策追踪**	Ordered sequence of rule identifiers that fired during evaluation, along with their individual sub-decision outcomes. 评估过程中被触发的规则标识符的有序序列，以及它们各自的子决策结果。
reason_codes **原因代码**	Standardized numeric codes indicating the reasons for the decision (e.g., 0x12 meaning “exceeds monthly FX cap”). 用于说明决策理由的标准化数字代码（如 0x12 代表 “超出月度外汇限额”）。
timestamps & seq. numbers **时间戳与序列号**	Evaluation timestamp(s) and sequence numbers providing an ordered record of execution and anti-replay protection. 评估发生的时间戳及序列号，提供有序的执行记录并防止重放攻击。
TEE attestation (*optional* | *可选*) **TEE 认证**	Proof of execution within a Trusted Execution Environment (TEE), such as an Intel SGX or AWS Nitro enclave attestation (if available). 在可信执行环境中执行的证明（如 Intel SGX 或 AWS Nitro 的安全区认证，如适用）。
cryptographic signature **密码学签名**	Digital signature from the executing node or secure enclave, attesting to the authenticity and integrity of the proof. 来自执行节点或安全区的数字签名，用于证明该证明的真实性与完整性。

procedural_actions (*optional* | *可选*) **程序性动作**	Any mandated compliance steps triggered by the rule's decision - for example, filing a Currency Transaction Report (CTR), submitting a Suspicious Activity Report (SAR), freezing assets, or escalating to a higher authority. 由规则决策触发的任何强制性合规步骤 （如提交大额现金交易报告、提交可疑活动报告、冻结资产或上报给更高层级机构）。
executor_metadata (*optional* | *可选*) **执行者元数据**	Metadata about the node or organization that performed the policy evaluation (e.g. the node or institution ID, software implementation version, or notation of any manual override applied). 关于执行政策评估的节点或机构的元数据（如节点或机构 ID、软件实现版本，或任何人工干预的标记）。
context_references (*optional* | *可选*) **执行者元数据**	Privacy-preserving references (hashed pointers) to off-chain contextual information, such as related KYC documents or underlying trade contracts associated with the transaction. 指向链下上下文信息的隐私保护引用（哈希指针）（如相关的 KYC 文件或与交易关联的基础贸易合同）。

Table 11: Compliance Proof (PoPC) structure and fields / 表 11: 合规性证明 (PoPC) 结构和字段

While these last three fields are not required in every proof blob, their inclusion in real-world workflows can greatly enhance forensic auditability and institutional accountability. By capturing additional details about follow-up compliance actions, execution context, and links to supporting documentation, these optional extensions provide a richer evidentiary record for investigators and oversight bodies.

(2) Transparency and Replay Toolchain

Importantly, the PoPC proof format remains intentionally **human-inspectable** - its contents can be read and interpreted directly without specialized tooling.

To complement this transparency, an open-source replay tool (**popc-replay**) is provided to validate the proof against the original policy pack, ensuring the absolute reproducibility of results:

```
popc-replay --proof proof.bin --jpack SG-MAS-PSD3-2025.11.tz

# → outputs identical decision + trace or highlights divergence
```

Using this tool, regulators, auditors, or counterparties can independently re-run and verify, even years later, that a particular transfer strictly complied with the exact rules in force at the time of settlement - all without needing access to the original underlying private data.

虽然并非每个证明数据包都必须包含最后三个可选字段，但在实际业务流程中引入它们，将显著提升取证审计的可行性与机构的问责能力。通过捕捉后续合规动作、执行背景以及佐证文档的关联信息，这些扩展字段为调查人员和监管机构提供了更详实、更具上下文深度的证明链记录。

(2) 透明度与复现工具

至关重要的是，PoPC 证明格式在设计上特意保持了“**可读性**”，无需借助专用工具，即可直接查阅并解读其内容 。

此外，系统提供了一款开源的重放工具（**popc-replay**），用于对照原始法规要件集验证证明，确保结果的可复现性：

```
popc-replay --proof proof.bin --jpack SG-MAS-PSD3-2025.11.tz

# → 输出完全一致的决策与轨迹，或突出显示差异
```

借助该工具，监管机构、审计机构或交易对手方即使在多年之后，也可以独立重放并验证某一笔交易是否严格遵循了结算当时生效的政策规则。这一过程完全无需接触原始隐私数据，实现了“隐私保护下的绝对合规”。

A5.8

Design Principles and Acceptance Criteria:
What "Good" Programmable Compliance Looks Like

The Policy-DSL and PoPC system is engineered against a strict set of non-functional requirements intended to satisfy regulators, auditors, central banks, and commercial institutions. Each requirement is verifiable on-chain or through open-source tooling and constitutes part of the network's formal correctness guarantees[17-18,31].

1) **Determinism and Policy Lifecycle Integrity: Ensuring stable, replayable outcomes across time and change**

- **Strict Determinism**: Evaluation of any transaction envelope against a given Jurisdiction Pack (identified by its exact version and policy_snapshot_hash) must produce bit-identical outcomes - decision (ALLOW/HOLD/REJECT), reason codes, and full decision trace - on any node, in any execution environment, at any point in the future. Randomness, clock access, locale settings, and external oracle calls are explicitly forbidden during policy execution[30].
- **Safe, Atomic, and Auditable Policy Upgrades (Hot-Swap Safety)**: Jurisdiction Pack upgrades are explicit on-chain governance transactions with predetermined activation points. Historical transactions remain replayable against the exact pack version active at settlement time, eliminating regulatory basis risk and enabling post hoc counterfactual analysis[22,31].

2) **Explainability, Proof, and Auditability: Making compliance decisions inspectable, verifiable, and tamper-evident**

- **Full Explainability and Regulatory Transparency**: Every compliance decision carries a complete, machine- and human-readable justification chain: fired rule IDs, triggering

设计原则与验收标准：
优秀可编程合规性应具备的特征

Policy-DSL 与 PoPC 系统设计遵循一系列严格的"非功能性需求"，旨在同时满足监管机构、审计方、中央银行及商业实体的核心诉求。每项要求都可通过链上验证或开源工具核查，构成了网络形式化正确性的保障体系[17-18,31]。

1) **确定性与策略生命周期完整性：确保跨时域及环境变更下的稳定重放结果**

- **严格确定性**：基于 A5.2 所确立的 Policy-DSL 执行模型，任何针对给定 JPack（通过其精确版本号及策略快照哈希 policy_snapshot_hash 进行识别）的交易报文评估，均须在任何节点、任何执行环境以及未来任何时间点产生位对齐（Bit-identical）的一致结果。这些结果包括最终决策（放行 ALLOW/ 挂起 HOLD/ 拒绝 REJECT）、原因代码及完整的决策追踪轨迹。在策略执行过程中，严禁引入随机数、时钟读取、区域设置及外部预言机调用[30]。
- **安全、原子化且可审计的策略升级（热替换安全性）**：JPack 升级被定义为具有预设生效点的显式链上治理交易。历史交易始终支持针对结算时活跃的精确 JPack 版本进行重放（见 A4.9.1 版本钉住机制）。这消除了监管基准风险，

primitives, canonical reason strings, optional natural-language explanations, and direct references to the underlying legal or regulatory provisions[17-18].

- **Proof-by-Default and Tamper-Evident Operation**: Compliance proofs PoPC are first-class protocol outputs, cryptographically bound to transactions and immutably recorded. Any observer can independently verify the full compliance history using only on-chain data and open-source replay tooling[17,44].

3) Security Architecture and Operational Resilience: Reducing attack surface while remaining robust under partial trust

- **Minimal Attack Surface and Long-Term Maintainability**: The Core-DSL remains deliberately small and incomplete, expressing new regulatory requirements through composition rather than opcode expansion. A compact, verifiable reference implementation enables formal verification, fuzzing, and enclave execution without DSL modification[25-26,50].
- **Defense-in-Depth and Graceful Degradation**: While execution inside TEEs is preferred, correctness and auditability never depend on trusted hardware. Absence of attestation degrades confidentiality guarantees only, not determinism or verifiability[27].

4) Privacy, Accountability, and Governance: Embedding legal responsibility and data minimization into system design

- **Privacy and Data Minimization by Design**: Compliance processing avoids retention of unnecessary personal data. Only redacted or cryptographically hashed inputs appear in decision traces, allowing full verification without exposure of sensitive information[8,36].
- **Accountability and Governance Clarity**: Clear separation of roles - policy authorship, execution, and independent re-verification - creates a transparent chain of accountability. Every compliance outcome can be traced to a specific signed policy source and its deterministic evaluation.

Together, these properties transform compliance from an opaque and error-prone process into a cryptographically provable, globally verifiable, sovereign-maintained function of the network[17,22,31]. They constitute the minimum threshold for admitting jurisdictions to the Sovereign Relay Hub and form the objective criteria governing protocol evolution.

并为事后反事实分析提供了可能[22,31]。

2) 可解释性、存证与审计：实现合规决策的可视、可验证与防篡改

- **全维度可解释性与监管透明度**：每一项合规决策均附带完整的、兼具机器可读与人类可理解性的正当性证明链。该证明链涵盖了触发的规则 ID、触发原语、规范化原因字符串、可选的自然语言阐释，以及指向底层法律或监管条款的直接引用索引[17-18]。
- **原生存证与防篡改运行机制**：PoPC 作为协议的原生输出，通过密码学与交易紧密绑定并实现不可篡改。任何观察者仅需利用链上数据及开源重放工具，即可独立验证完整的合规历史记录[17,44]。

3) 安全架构与运营韧性：在部分信任环境下缩减攻击面并保持稳健

- **最小化攻击面与长期可维护性**：Core-DSL 刻意保持精简与非完备性，通过逻辑组合而非操作码扩张来表达新型监管需求。紧凑且可验证的参考实现支持在无需修改 DSL 的情况下，进行形式化验证、模糊测试及安全地执行[25-26,50]。
- **深度防御与优雅降级**：尽管系统优先选择在可信执行环境内运行，但执行的正确性与可审计性绝不依赖于特定硬件。认证的缺失仅会降低机密性保障，而不会影响系统的确定性或可验证性[27]。

4) 隐私、问责与治理：将法律责任与数据最小化嵌入系统设计

- **原生隐私与数据最小化设计**：合规处理过程严格避免保留不必要的个人数据。决策轨迹中仅出现经过脱敏或密码学哈希处理的输入项，从而在不泄露敏感信

息的前提下实现全量验证 [8,36]。

- **问责制与治理透明度**：通过对策略制定、策略执行及独立重验等角色的清晰界定，构建了透明的责任链条。每项合规结果均可追溯至特定的署名 JPack 及其确定性的评估过程（治理见 A4）。

上述特性，共同将合规从一个黑盒化、易出错的过程，转变为网络中一种密码学可证、全局可验证且由主权机构维护的网络能力 [17,22,31]。这些特性构成了司法辖区接入 SRH 的最低门槛，也是驱动协议演进的客观准则。

A5.9

Progressive Adoption Strategy:
Sovereign-Led Organic Growth

A central principle of the Policy-DSL and PoPC framework is **incremental, verifiable, and jurisdiction-led adoption**, rather than attempting to "hard-code the world's regulations" at launch[51].

1) **Global Invariants and Sovereign Autonomy**
   The system fixes two global invariants to serve as the bedrock of interoperability:
   1. **The Core-DSL Vocabulary**: Defining universal compliance semantics.
   2. **The PoPC Proof Architecture**: Defining the minimum auditable footprint for regulatory decisions.

These narrow, stable underlying elements form the "constitutional" substrate, allowing jurisdictions to adopt the framework and achieve seamless interoperability without ceding sovereignty or operational independence.

渐进式采用策略：
主权驱动的有机增长

Policy-DSL 与 PoPC 框架的核心原则是**渐进式、可验证且由主权辖区驱动的接入**，而非在初期试图强加一套全球统一的监管硬编码 [51]。

1) **全局不变量与主权自治**。系统锚定了两个全局性的不变量，作为互操作性的底座：
   1. **Core-DSL 核心词汇表**：定义了通用的合规语义。
   2. **PoPC 证明架构**：定义了监管决策的最小审计足迹。

这些精简的底层元素构成了网络的“宪法级”基石。各司法辖区在采用该框架时，既能实现无缝互操作，又无需让渡主权或运营独立性。

2) **Policy Data-Fitting**

Jurisdictions onboard through "Policy Data-Fitting", deconstructing and expressing local legal obligations as Jurisdictional Policy Packs (JPack).

- **Explicit Representation**: A JPack comprises a versioned set of rules, thresholds, legal references, and metadata, all mapped into the Core-DSL grammar.
- **Sovereign Assertion**: JPack are openly published for verification and comparison, ensuring each jurisdiction asserts its own regulatory interpretations rather than being forced to inherit the rules of larger economic blocs.

3) **Roadmap: From Pioneers to Global Consensus**

The network is designed for a phased rollout:

- **The Pioneer Phase**: Initially launched by a few technically and regulatorily aligned jurisdictions (e.g., Singapore, Saudi Arabia, Switzerland) providing validated JPack and "Golden Test Vectors" to serve as best-practice precedents.
- **The Organic Expansion Phase**: As consensus builds and readiness matures, additional jurisdictions can join the network at their own pace.

4) **Policy Heterogeneity as a System Parameter**

This approach turns regulatory diversity into a structured, governable feature. Differences are no longer hidden in proprietary, "black-box" tech stacks; instead, they become explicit, versioned, and upgradeable. Under a framework of sovereign control and cryptographic accountability, "policy heterogeneity" becomes a first-class parameter of the system.

Conclusion: **Sovereignty by Design**. No jurisdiction shall be compelled to adopt the rules of another. Each sovereign entity participates at its own pace and on its own terms. The cross-border financial network will achieve organic and sustainable growth through sovereign autonomy, rather than technical imposition.

2) **政策数据拟合**。各辖区通过“政策数据拟合”实现接入：将其本地法律义务解构并表达为辖区法规要件集 (JPack)。

- **显性化声明**：JPack 包含了版本化的规则、阈值及法律引用，并统一映射至 Core-DSL 语法。
- **主权声明**：JPack 公开发布以供验证，确保各辖区都能自主声明其监管解释，而非被迫继承其他经济集团的规则。

3) **路线图：从先行先试到全球共识**。网络将采取分阶段启动模式：

- **先驱阶段**：由技术与监管共识度较高的辖区（如新加坡、沙特阿拉伯、瑞士）先行启动，提供经验证的 JPack 和“黄金测试向量”作为最佳实践典范。
- **有机扩张阶段**：随着规则的标准化与各方准备就绪，其他辖区按需陆续加入。

4) **政策异构性作为系统参数**。这种方法将监管的多样性转化为一种结构化、可治理的特性。各方的差异不再隐藏在黑盒技术栈中，而是变得显性化、版本化且可升级。在主权控制与密码学问责的框架下，“政策异构性”成为了系统的核心参数。

结论：**主权规则内置**。没有任何辖区必须采纳他国规则。每个主权都按自己的节奏与规则参与其中。跨境金融网络将通过“主权自主”而非技术强制，实现有机且可持续的增长。

A5.10

Technical Implementation Examples (super-light sketch-code example)

技术实现示例（极简代码示例）

(1) Rule Definition (YAML Syntax)

Rules are expressed in a clean, YAML-based declarative format that is both human-readable for compliance officers and directly interpretable by the Regulatory VM without transpilation steps. This structure keeps the DSL minimal (only boolean logic, built-in aggregates, and parameter look-ups) while allowing arbitrarily complex real-world policies to be composed from simple, auditable primitives.

(1) 规则定义（YAML 风格）

规则采用声明式 YAML 格式编写。其设计初衷是确保合规专家能够直观阅读，同时监管虚拟机（RVM）能够直接解释执行，无需复杂的中间编译过程。通过布尔逻辑与原子化原语的组合，DSL 能够精确表达复杂的跨境监管政策。

```
 id: FX_CAP_DAILY_RETAIL

when:
 subject.kyc_tier >= 2                    # 客户 KYC 等级不低于 2 级
 and subject.residency in ["SG", "HK", "EU"] # 居住地为新加坡、香港或欧盟
 and asset.type == "FIAT_TOKEN"            # 资产类型为法币代币
 and flow.direction in ["OUTBOUND", "CROSSBORDER"] # 资金流向为流出或跨境

check:
 # 检查该主体 24 小时内的滚动累计金额是否超过设定的每日限额
 rolling_sum(amount, window="1d", key=subject.id) <= params.cap_daily

then:
 allow() # 符合条件，允许通过

else:
 # 若超过限额，则挂起交易，并返回具体原因和代码
 hold(reason="CAP_EXCEEDED", code="FX_CAP_DAILY_RETAIL")
```

(2) PoPC Trace Record (JSON Proof Example)

(2) PoPC 追踪记录 (JSON 证明示例)

Every transaction that undergoes a compliance check generates a compact, cryptographically bound proof artifact. This proof is stored immutably within the cross-chain transaction archive of the Sovereign Relay Hub (SRH) as a tamper-evident audit record.

每笔交易在通过合规检查后，均会生成一份紧凑且具有密码学约束力的证明工件。该证明被持久化存储于跨链交易归档中，作为不可篡改的审计凭证。

```
{
"tx_id": "0x…",
"policy_pack": "SG-PSA-2025.03#sha256:abcd…",  // 引用具体的法规要件集版本及哈希
"decision": "HOLD",                 // 决策结果：挂起
"reasons": ["FX_CAP_DAILY_RETAIL"],        // 触发的规则 ID
"inputs_hash": "sha256:…",              // 输入数据的哈希值（用于校验）
"ts": "2025-11-06T08:11:00Z",               // 执行时间戳
"env_attest": {                   // 运行环境认证
 "mode": "TEE",
 "quote_hash": "…"                   // TEE 安全区的远程度量值
}
}
```

This JSON **artifact is fully self-contained**: any regulator or auditor can fetch the referenced policy pack, recompute the inputs hash from redacted data if needed, and replay the exact decision path using the open-source popc-replay tool - delivering verifiable, non-repudiable proof of compliance for every cross-border settlement.

这份 JSON 工件构成了**自包含的合规证明**：监管机构或审计人员可获取引用的 JPack 法规要件集，利用脱敏数据验证输入哈希，并通过开源的 popc-replay 工具重现整个决策路径。这为每一笔跨境结算提供了可验证、不可否认的合规证明。

A5.11

Jurisdiction Sampling: Regulatory Shapes and DSL Mapping

司法辖区采样：监管形态与 DSL 映射

Cross-border tokenised finance requires a rigorous understanding of how different jurisdictional regimes conceptualise, structure, and enforce policy obligations. Although the underlying goals - consumer protection, financial stability, AML/CFT, and sanctions enforcement - are shared globally, the shape of these obligations differs substantially[3,5,8].

This section provides an analytical comparison of four representative clusters: **the European Union, the United States, the Singapore-Hong Kong axis and the United Arab Emirates**. These regimes also appear prominently in contemporary tokenisation pilots, including MAS Project Guardian, the Swiss SBDT deposit-token initiative, and Deutsche Bank's DAMA 1/2 architecture, all of which highlight the need for formalised policy representations and interoperable regulatory enforcement[15,21,45].

The Policy-DSL provides a structured vocabulary and execution model for encoding these jurisdiction-specific primitives, while JPack enable each regulatory regime to apply its own interpretations, thresholds, and obligations without disrupting cross-border workflows. Below, we outline dominant regulatory features in each region and illustrate how they are mapped into Core-DSL primitives.

(1) European Union - MiCA/AML/PSD3/DORA regime (EU-MiCA-Compliance-2025.11)

The EU's financial and data-governance frameworks increasingly emphasise **ownership, localisation, and purpose-bound processing of personal financial data**. Institutions transmitting data across borders must adhere to GDPR principles, MiCA record-keeping requirements, and centralised supervisory datasets[5,9,39]. These obligations translate into strict residency primitives within the DSL, distinguishing EU-resident subjects from non-EU participants and restricting data flows accordingly.

The EU imposes structured periodic and event-driven reporting requirements. MiCA mandates regular disclosure to national authorities; PSD2 requires incident reporting; DORA enforces ICT supervisory reporting and operational-resilience audits. DORA's ICT risk rules require institutions to evaluate and document operational modes, especially in degraded conditions (system outages, cyber events)[9,43].

DSL primitives must cover residency and geography (e.g., EU/EEA vs. non-EU), subject type (retail/professional), asset type, transaction amount and rolling sums for MiCA caps; rules should reference travel-rule data fields (name, address, account numbers) to

跨境代币化金融的核心挑战，在于如何兼容不同辖区在定义、构建及执行监管义务时的显著差异。尽管消费者保护、金融稳定、AML/CFT 及制裁执行等底层目标具有全球普适性，但具体制度形态与执行逻辑却各具特色 [3,5,8]。

本节选取了四个具有代表性的监管集群进行对比分析：**欧盟、美国、新加坡 - 香港轴心、以及阿联酋**。这些区域不仅是当前全球代币化金融试点（如新加坡金管局 Project Guardian、瑞士 SBDT 倡议、中阿“Aber 项目”）的核心阵地，也代表了对形式化政策表达与跨链监管互操作的最迫切需求 [15,21,45]。

Policy-DSL 提供了一套结构化的词汇表与执行模型，用于编码这些特定司法辖区的原语。而 JPack（政策包）则允许各监管机构在不干预跨境交易流程的前提下，灵活应用各自的解释逻辑、阈值及合规义务。

下文将分别概述各地区的主要监管特征，并说明其如何映射为 Core-DSL 中的基础原语。

(1) 欧盟：MiCA/AML/PSD3/DORA 监管体系 (EU-MiCA-Compliance-2025.11)

欧盟的监管逻辑日益强调**个人数据主权、本地化存储及用途限定**。金融机构在跨境传输时必须严守《通用数据保护条例》(GDPR) 原则、《加密资产市场法案》(MiCA) 的记录保存规范 [5,9,39]。这些义务在 DSL 中转化为了严格的居住地原语，用于区分欧盟居民与非欧盟参与者，并据此限制数据流向。

此外，欧盟还制定了结构化的定期报告与事件驱动报告要求。MiCA 要求定期向国家主管当局进行披露；欧盟《第二版支付服务指令》（PSD2）规定了事件报告义务；数字运营韧性法案（DORA）则强制执行信息通信技术

ensure that required information accompanies the transaction. PSD2's SCA can be modelled as a pre-condition requiring multi-factor authentication status before ALLOW. DORA influences the DSL's operational layer - policy packs might include maximum tolerated downtime or incident escalation windows; PoPC could record whether the decision was made under normal or degraded resilience mode.

- **Core Mandates**: Investor protection, operational resilience, data localization, and real-time reporting.
- **DSL Primitive Mapping**: residency (distinguishing EEA vs. non-EEA), mica_class (asset classification), and investor_type (retail vs. professional).

At the DSL level, primitives must cover:

- **Residence and geographic location**: Distinguish between the EU/EEA and non-EU/EEA regions.
- **Subject type**: Differentiate between retail customers and professional investors.
- **Asset type and transaction amount**: Used to monitor the thresholds set out under MiCA.
- **Travel Rule**: Reference relevant data fields (name, address, account number) to ensure that necessary information is transmitted synchronously with the transaction.
- **Authentication**: Strong Customer Authentication (SCA) as required by PSD2 can be modeled as a precondition, verifying the multi-factor authentication status before a decision is permitted.
- **Operational resilience**: DORA affects the operational layer of the DSL, and the regulatory requirement set may include maximum tolerable downtime or incident escalation windows; the PoPC proof records whether the decision was made under normal mode or resilience-degraded mode.

Dominant policy concerns: investor protection, operational resilience, data localization, and instant reporting.

（ICT）监管报告和运营韧性审计。根据 DORA 的 ICT 风险规则，机构必须评估并记录系统的运行模式，特别是在降级条件（如系统宕机、网络事件）下的表现 [9,43]。

- **核心诉求**：投资者保护、运营韧性、数据本地化、即时报告。
- **DSL 原语映射**：residency（区分 EEA 境内外）、mica_class（资产分类）、investor_type（零售 vs 专业）。

在 **DSL** 层面，原语必须涵盖：

- **居住地与地理位置**：区分欧盟 / 欧洲经济区 (EU/EEA) 与非欧盟地区。
- **主体类型**：区分零售与专业投资者。
- **资产类型与交易额**：用于监控 MiCA 设定的上限。
- **旅行规则**：引用相关字段（姓名、地址、账号）确保必要信息随交易传输。
- **身份验证**：PSD2 要求的强身份验证 (SCA) 可建模为前置条件，在决策允许之前检查多因素验证状态。
- **运营韧性**：DORA 影响 DSL 的运行层，Jpack 可能包含最大容忍停机时间或事件升级窗口；PoPC 证明须记录该决策是在正常模式还是韧性降级模式下做出的。

核心监管诉求：投资者保护、运营韧性、数据本地化以及即时报告。

Core-DSL primitive 原语	Real-world mapping and example rules 现实世界映射与规则示例
residency, geography **居住地、地理位置**	Data-residency checks: subject and counterparty residency must be in EEA or adequacy-decided jurisdictions for certain asset classes; otherwise HOLD + mandatory SAR filing. 数据驻留检查：对于特定资产类别，主体与对手方的居住地必须在 EEA 或获得互认协议的司法辖区；否则执行挂起（HOLD）并强制提交可疑活动报告 (SAR)。

asset.type, product_type **资产类型、产品类型**	Strict CASP (Crypto-Asset Service Provider) scoping: only ART (Asset-Referenced Token) and EMT (E-Money Token) permitted for retail; all others REJECT unless subject.professional_investor = true. 加密资产服务商 (CASP) 展业范围：零售用户仅限使用资产参考代币 (ART) 和电子货币代币 (EMT)；其他资产均执行拒绝 (REJECT)，除非主体身份为专业投资者。
amount + frequency **金额 + 频率**	MiCA Title V exposure caps: retail clients ≤ €15 000/month on non-EUR ARTs. MiCA 第五章敞口上限：零售客户在非欧元 ART 资产上的交易额每月不得超过 € 15,000。
time_window + reporting **时间窗口 + 报告**	DORA 24 h major-incident reporting → all transactions > €100 m auto-tagged for instant ICT-event correlation. DORA 24 小时重大事件报告：金额超过 € 1 亿的交易将自动打标，以便与 ICT 事件进行即时关联分析。
risk_score + list_status **风险评分 + 列表状态**	Mandatory Travel Rule (TORA) binding: counterparty must be hosted by a CASP or obligated entity; otherwise HOLD until resolved. 强制性旅行规则 (TORA) 约束：对手方必须由受监管的 CASP 或义务实体托管；否则执行挂起 (HOLD) 直至合规问题解决。

Example rule snippet
规则代码片段示例
	`when:`
	`  asset.mica_class == "ART_NON_EUR" and`
	`  subject.investor_type == "RETAIL"`
	`check:`
	`  monthly_sum(amount) <= 15_000_EUR`
	`then:`
	`  allow()`
	`else:`
	`  reject(code="MICA_RETAIL_CAP")`

Table 12: EU regulatory rules encoded using Core DSL primitives / 表 12：使用核心 DSL 原语编码的欧盟监管规则

These primitives allow EU rules to be represented transparently in a JPack such as EU-MiCA-2025.06, with golden tests verifying that caps, residency boundaries, authentication requirements, and product-type constraints behave correctly.

(2) United States (BSA/AML, FinCEN Travel Rule, OFAC, State MSB Regimes)

The United States exhibits a **modular, multi-layered** regulatory landscape: federal AML/CFT rules, OFAC sanctions requirements, and state-level money-service-business (MSB) licensing[2,8,46]. This creates a policy shape distinct from the EU's harmonised framework.

这些原语使得欧盟规则可以透明表达在 EU-MiCA-2025.06 等 JPack 中，并通过黄金测试验证金额上限、居住地边界、身份验证要求及产品类型限制是否在系统运行中被正确执行。

(2) 美国（涵盖 BSA/AML、FinCEN 旅行规则、OFAC、州级 MSB 监管）

美国的监管环境具有典型的**多层级、模块化**特征：既有联邦反洗钱 / 反恐融资规则（BSA/AML）、外国资产控制办公室（OFAC）制裁

Many US rules are threshold-driven. The FinCEN Travel Rule activates when transactions exceed specified dollar thresholds, requiring transmission of originator/beneficiary data[2-3]. OFAC requirements are strict and binary: entities on the SDN list must be blocked without exception[8,46]. Regulators require the presence, accuracy, and retention of travel-rule fields (originator and beneficiary identifiers). The BSA mandates Suspicious Activity Reports (SARs) for transactions showing AML risk characteristics[1,3].

DSL rules must incorporate threshold triggers - for example, if `amount >= 3000 USD` then require `travel_data_present = true` else hold. Entities on OFAC lists can be represented via a `subject.sanctions_status` attribute; any match triggers `REJECT`. State residency can be modelled through `subject.geography.state`; state-specific thresholds or licences become JPack parameters. PoPC proof should include hashed travel-rule fields to demonstrate compliance without exposing PII[3,31].

- **Core Mandates**: Travel Rule compliance, real-time SDN list interception, and state-level access control.
- **DSL Primitive Mapping**: travel_data_present (information integrity), list_status (watchlist validation), and license_status (licensing standing).

要求，也有各州层面的货币服务业务（MSB）许可制度[2,8,46]。这种结构与欧盟那种高度统一的框架截然不同。

美国的监管规则大多由阈值驱动。例如，金融犯罪执法网络（FinCEN）的旅行规则会在交易超过特定金额时触发，强制要求传输汇款人与收款人的身份信息[2-3]。相比之下，美国财政部外国资产控制办公室（OFAC）的要求则是极其严格的二元对立：任何出现在特别指定国民（SDN）名单上的实体必须被无条件拦截[8,46]。监管机构不仅要求旅行规则相关字段（汇款人 / 收款人标识符）必须存在且准确，还要求长期留存。此外，《银行保密法》（BSA）规定，对于具有反洗钱风险特征的交易，必须提交可疑活动报告（SAR）[1,3]。

在 DSL 规则中，必须集成这些阈值触发器。例如：如果金额 `>= 3000 USD`，则要求旅行数据必须存在，否则挂起（HOLD）交易。OFAC 名单上的实体可以通过 `subject.sanctions_status` 属性来表示，一旦匹配

Core-DSL primitive 原语	Real-world mapping and example rules 现实世界映射与规则示例
amount + travel_data_present **金额 + 旅行数据存在**	FinCEN Travel Rule threshold: transmittals ≥ $3,000 must include sender and recipient identifying information (name, address, account numbers, etc.) in the payment message; if the required Travel Rule data is missing, the transaction is placed on HOLD until the information is provided. FinCEN 旅行规则阈值：单笔转账 ≥ $3,000 时，支付信息必须包含汇款人和收款人的标识信息（姓名、地址、账号等）。若缺失必要数据，交易将设为挂起，直至信息补齐。
list_status **名单状态**	OFAC sanctions screening: any party appearing on a prohibited sanctions list (e.g., the SDN list) triggers an immediate block of the transaction (REJECT). No value may be transferred to sanctioned persons – such transactions must be frozen and reported to OFAC (strict liability, no de minimis threshold). OFAC 制裁筛查：任何参与方若出现在禁止制裁名单（如 SDN 名单）中，将立即触发交易拦截。禁止向受制裁人员转移任何价值，此类交易必须冻结并向 OFAC 报告（此为“严格责任”，不设最低免责阈值）。
amount + frequency **额度 + 频率**	Currency Transaction Reports (CTR): cash deposits or withdrawals exceeding $10,000 in one business day (alone or aggregated) require mandatory reporting to FinCEN. DSL rules can sum daily cash totals per customer and automatically flag transactions for CTR filing (e.g., `if daily_sum(amount, type="CASH") > 10_000_USD then report("CTR")`). 大额现金交易报告 (CTR)：在同一个营业日内，累计超过 $10,000 的现金存款或取款必须向 FinCEN 报告。DSL 规则可自动累计客户当日现金总额并打标（如若每日现金总额 > 10,000 USD，则触发 CTR 报告）。

risk_score + pattern **风险评分 + 模式**	Suspicious Activity detection: repeated or unusual patterns (e.g., structuring multiple sub-$10k transfers) elevate a transaction's risk score. Transactions aggregating ≥ $5,000 with money-laundering indicators or other red flags must prompt a Suspicious Activity Report (SAR) filing, typically after placing the transaction on HOLD for further compliance review. 可疑活动监测：重复或异常模式（如为了避开 $10,000 阈值而进行的拆分交易）会提高风险评分。累计金额 ≥ $5,000 且伴有洗钱征兆或其他红旗警示时，需提交可疑活动报告，通常在将交易挂起以供合规审查后执行。
geography (state) + license_status **州 + 牌照状态**	State MSB licensing: for example, California's Financial Code (§2030) prohibits engaging in money transmission with California residents unless properly licensed. If an entity is not licensed in a required state, any transaction involving that state's customers is REJECTED or flagged as unlicensed activity (violating state money-transmitter laws). 州级货币服务业务机构（MSB）许可：如《加州金融法》（第 2030 条）禁止在未获得相应牌照的情况下向加州居民提供货币转移服务。若实体未获该州牌照，任何涉及该州客户的交易都将被拒绝或标记为非法经营。

Example rule snippet
规则代码片段示例
	`when:`
	`any_beneficial_owner.list_status == "SDN"`
	`then:`
	`reject(code="OFAC_BLOCK", reference="31 CFR § 501")`

Table 13: USA regulatory rules encoded using Core DSL primitives / 表 13：使用核心 DSL 原语编码的美国监管规则

In practice, these rules assemble into JPack such as US-AML-TravelRule-2025.04, which can be combined deterministically with other jurisdictions during cross-border verification.

(3) Singapore & Hong Kong - MAS PSA / HKMA sandbox regime (SG-MAS-PSD3-2025.11 + HK-SFC-TokenisedDeposits-2025.Q3)

The Singapore-Hong Kong corridor represents a technologically advanced regulatory cluster characterised by pilots in tokenised deposits, wholesale CBDCs, stablecoins, and programmable money[15,21,37].

The Payment Services Act distinguishes between Money-Changing Licensees, Standard Payment Institutions (SPI), and Major Payment Institutions (MPI). Licensing tier dictates transaction caps, e-money float limits, technology-risk requirements, and reporting obligations. SPI/MPI distinctions enforce monthly transaction-volume limits and real-time monitoring[47-48].

Some settlement flows depend on RTGS availability or local business-hour windows. MAS and HKMA pilots often evaluate programmable constraints such as "execute only if settlement rail is open"[15,21] . Hong Kong's stablecoin ordinance imposes strict reserve, redemption, and issuer governance requirements[10].

成功立即触发拒绝。州级居住地可以映射为 `subject.geography.state`，各州特有的阈值或牌照要求则转化为 JPack 中的具体参数。PoPC 证明应包含哈希处理后的旅行规则字段，以便在不泄露个人敏感信息（PII）的前提下证明合规[3,31]。

- **核心诉求**：旅行规则合规、SDN 名单实时拦截、州级准入控制。
- **DSL 原语映射**：travel_data_present（信息完整性）、list_status（名单校验）、license_status（牌照状态）。

在实际操作中，这些规则会被封装进类似 US-AML-TravelRule-2025.04 这样的 JPack 中。在进行跨境验证时，该 JPack 可以与其他辖区的规则进行确定性的组合执行。

(3) 新加坡与香港：MAS PSA 与 HKMA 沙盒监管模式

（规则包编号：SG-MAS-PSD3-2025.11 + HK-SFC-TokenisedDeposits-2025.Q3）

In the DSL, Singapore's licence tier can be encoded as `subject.licence_type`; rules can cap monthly transaction volume or outstanding float depending on the licence.

The asset.type field distinguishes e-money from digital payment tokens; caps and audit requirements become JPack parameters.

Hong Kong's stablecoin regime maps to a `token.type = stablecoin` primitive with additional checks:

- reserve-asset adequacy
- issuer licence validity
- redemption policy presence and cross-jurisdictional compliance

The Reuters-described pilot can be represented as a `programmatic_use_case` attribute (e.g., tokenised money-market fund) that triggers higher liquidity and disclosure requirements.

Business-hour windows, if imposed by local RTGS systems, can be modelled through `time_window` conditions.

MAS Project Guardian and Swiss SBDT pilots emphasise regulated issuance, redemption semantics, asset segregation, and operational controls[15,31]. Dominant policy concerns: licensing tiers, per-wallet caps, business-hour settlement windows, and base-currency exposure limits.

- **Core Mandates**: Licensing tier limits, individual wallet caps, business-hour settlement, and stablecoin reserve compliance.
- **DSL Primitive Mapping**: licensing_tier (license grade), base_currency (base currency restrictions), and time_window (execution windows).

新加坡与香港之间的金融走廊代表了一个技术领先的监管集群。其特点是广泛开展了代币化存款、批发型央行数字货币（wCBDC）、稳定币以及可编程货币的试点项目[15,21,37]。

新加坡的《支付服务法案》（PSA）将持牌机构细分为：货币兑换商、标准支付机构（SPI）以及大型支付机构（MPI）。牌照等级决定了其交易限额、电子货币余额上限、技术风险要求以及报告义务。SPI 与 MPI 的区别在于月度交易额度限制和实时监控要求[47-48]。

此外，部分结算流程取决于实时全额结算系统（RTGS）的运行状态或当地营业时间。新加坡金融管理局（MAS）与香港金融管理局（HKMA）的试点项目经常评估，如“仅在结算通道开启时执行”等可编程约束[15,21]。香港的稳定币条例则对储备资产、赎回机制和发行人治理提出了严苛要求[10]。

在 DSL 中，新加坡的牌照等级可编码为 `subject.licence_type`；相关规则可据此对月度交易量或未结清余额设定上限。

asset.type 字段用于区分“电子货币”与“数字支付代币”；相应的额度限制与审计要求，则作为 JPack 的参数进行配置。

Core-DSL primitive 原语	Real-world mapping and example rules 现实世界映射与规则示例
subject.licensing_tier **牌照分级**	MAS Major Payment Institution vs. Standard Payment Institution → different daily caps. 牌照分级：MAS 大型支付机构 (MPI) 对比标准支付机构 (SPI) → 设置不同的每日限额。
asset.base_currency **基础货币限制**	Single-currency stablecoin framework (SCS): only SGD- or HKD-backed tokens permitted for retail; multi-currency → licensed entities only. 基础货币限制：单币种稳定币框架 (SCS)；零售端仅允许 SGD 或 HKD 支持的代币； 多币种代币仅限持牌机构使用。
amount + frequency **额度 + 频率**	Retail daily cap SGD 30 000 (MAS Notice 626) and HKD 200 000 (HKMA sandbox 2025). 额度与频率：零售每日限额 30,000 新元（参考 MAS Notice 626）及 200,000 港元（参考 HKMA 2025 沙盒）。

time_window **时间窗口闸口**	Business-hour gating: non-whitelisted institutions may only settle 09:00-17:00 SGT/HKT on business days. 时间窗口闸口：非白名单机构仅限在工作日 09:00-17:00 (SGT/HKT) 进行结算。
geography + residency **地理与居民身份**	Cross-border only permitted to approved corridors (SG-HK, SG-CH); others REJECT or HOLD. 地理与居民身份：跨境流动仅允许在获批走廊间进行（如新 - 港、新 - 瑞）；其他路径执行拒绝或挂起。

Example rule snippet
规则代码片段示例
	`# 示例：非营业时间挂起零售结算`
	`when:`
	`subject.licensing_tier == "RETAIL"`
	`and time_window.now() not in "BUSINESS_HOURS_SGT"`
	`then:`
	`hold(code="NON_BUSINESS_HOURS", reason="结算超出了准许的时间窗口 - 参考 MAS PSA-N03 第 12.4 条")`

Table 14: Singapore regulatory rules encoded using Core DSL Primitives / 表 14：使用核心 DSL 原语编码的新加坡监管规则

Taken together, the regulatory approaches of Singapore and Hong Kong illustrate a **model defined by licensing tiers, prudential guarantees, and programmable settlement constraints**. Their frameworks combine strong supervisory control with openness to tokenised financial infrastructure, producing policy obligations that are highly structured yet operationally dynamic. These characteristics map cleanly onto DSL primitives for licensing, thresholds, reserve rules, and time-window constraints, enabling consistent cross-border interpretation.

(4) United Arab Emirates - CBUAE/DFSA/FSRA regime

(example of an extended JPack such as UAE-DLT)

The UAE's financial regulatory landscape for DLT-based infrastructure in finance is characterized by a federal structure with the Central Bank of the UAE (CBUAE) overseeing national payment and settlement systems, while free zone authorities like the Dubai Financial Services Authority (DFSA) in the Dubai International Financial Centre (DIFC) and the Financial Services Regulatory Authority (FSRA) in the Abu Dhabi Global Market (ADGM) regulate activities within their jurisdictions[13,32].

This framework supports innovation in distributed ledger technology (DLT) for traditional financial systems, such as real-time gross settlement (RTGS), cross-border interbank transfers, and

香港的稳定币监管制度映射为 `token.type = stablecoin` 原语，并附加额外检查：

- 储备资产充足性。
- 发行人牌照有效性。
- 赎回政策透明度以及跨辖区合规性。

路透社报道的试点案例，可以表示为 `programmatic_use_case` 属性（如：代币化货币市场基金），该属性会触发更高的流动性和信息披露要求。

若本地实时全额结算系统 (RTGS) 规定了营业时间窗口，则可通过 `time_window` 条件建模。

MAS 守护者计划（Project Guardian）和瑞士稳定币交易代币 (SBDT) 试点强调受规管发行与赎回语义、资产隔离及运营控制 [15,31]。核心政策关注点包括：牌照分级、个人钱包限额、营业时间结算窗口及基础货币风险敞口限制。

- **核心诉求**：牌照额度限制、个人钱包上限、营业时间结算、稳定币储备合规。

tokenized securities, aligning with global standards like ISO 20022 for messaging and Principles for Financial Market Infrastructures (PFMI) for safety and efficiency[32,41-42].

Key initiatives include the Digital Dirham issuance platform for wholesale interbank settlements and Project Aber, a DLT-based cross-border settlement pilot with Saudi Arabia, emphasizing polycentric peer-to-peer transfers between commercial banks without traditional correspondent banking dependencies[4,6,21,45], enable direct settlement of cross-border payments.

Institutions adopting DLT must adhere to governance, design, and operational requirements under CBUAE's Guidelines for Financial Institutions Adopting Enabling Technologies, including auditability, business continuity, and risk management. AML/CFT obligations mirror those for traditional transfers, with mandatory KYC, sanctions screening, and suspicious activity reporting. Thresholds trigger enhanced due diligence and filings, while cross-border flows require approved corridors and data localization where applicable[1-3,8].

DSL primitives incorporate these through checks on licensing, transaction thresholds, and settlement conditions; PoPC can record compliance proof like hashed transaction metadata to verify adherence without exposing sensitive data.

- **Core Mandates**: Financial stability, ISO standard alignment, settlement finality, and corridor-based access.
- **DSL Primitive Mapping**: iso_20022_compliant (messaging standards), corridor_id (authorized compliance corridors), and edd_status (Enhanced Due Diligence status).

Dominant policy concerns: financial stability, AML/CFT enforcement, operational resilience, settlement finality, and interoperability with existing systems.

- **DSL 原语映射**：licensing_tier（牌照等级）、base_currency（基础货币限制）、time_window（时间窗口）。

综合来看，新加坡与香港的监管路径呈现出一种清晰的模式：**以牌照分级为核心，以审慎性要求为底线，并通过可编程约束管理结算行为。**其框架将强大的监管控制与对代币化金融基础设施的开放态度相结合，产生的政策义务既结构严谨，又具备运营灵活性。这些特征能精准映射到 DSL 的牌照、阈值、储备规则和时间窗口原语中，从而实现一致的跨国监管解读。

(4) 阿联酋：CBUAE/DFSA/FSRA 监管体系

（扩展型 JPack 示例：UAE-DLT）

阿联酋针对金融领域分布式账本（DLT）基础设施的监管呈现出联邦制结构：阿联酋中央银行（CBUAE）负责监督国家支付与结算系统；而迪拜国际金融中心（DIFC）的迪拜金融服务管理局（DFSA）以及阿布扎比全球市场（ADGM）的金融服务监管局（FSRA）等自贸区机构，则负责各自辖区内的业务监管[13,32]。

该框架支持将 DLT 创新应用于传统金融系统，如实时全额结算（RTGS）、跨境银行间转账和证券代币化。其设计标准与国际接轨，消息格

Core-DSL primitive 原语	Real-world mapping and example rules 现实世界映射与规则示例
residency, geography **居住地与地理**	Cross-border settlement restrictions: subject and counterparty must be in approved jurisdictions (e.g., UAE-Saudi corridor under Project Aber); otherwise HOLD + enhanced due diligence; data localization for UAE-resident transactions to ensure compliance with federal laws. 跨境结算限制：主体与交易对手必须处于获批的走廊内（如 Project Aber 框架下的阿联酋 - 沙特走廊）；否则执行挂起并触发增强型尽职调查；阿联酋居民交易需遵守数据本地化，以符合联邦法律。
asset.type, product_type **资产与产品类型**	Tokenized securities scoping under FSRA/DFSA: treated as traditional securities if exhibiting equivalent characteristics; REJECT if not compliant with FSMR prospectus requirements unless exempt (e.g., professional clients only). FSRA/DFSA 证券代币化界定：若代币具备等同特征，则视为传统证券；若不符合《金融服务与市场条例》（FSMR）的招股说明书要求则予以拒绝，豁免情形（如：仅限专业客户）除外。

amount + travel_data_present **金额与旅行规则数据**	Large-value transfer thresholds: transactions ≥ AED 3,500 require originator/beneficiary data (name, address, account identifiers) aligned with ISO 20022; missing data triggers HOLD until resolved, similar to traditional bank transfer rules. 大额转账阈值：金额 ⩾ 3,500 迪拉姆（AED）的交易必须包含符合 ISO 20022 标准的汇款人 / 收款人信息；信息缺失将触发挂起直至补全。
list_status **名单状态**	Sanctions screening: parties on UAE/UN prohibited lists trigger REJECT; assets frozen and reported to CBUAE (strict liability, no thresholds), integrating with traditional AML frameworks. 制裁筛查：涉及阿联酋或联合国禁令名单的当事人直接拒绝；资产须冻结并上报 CBUAE（此为严格责任制，无金额门槛）。
amount + frequency **金额与频率**	Reporting for aggregates: daily sums > AED 40,000 flag for suspicious activity reports; exposure limits for interbank settlements to maintain liquidity, e.g., ≤ AED 200,000/month on cross-border flows. 累计报告：日累计金额 > 40,000 AED 将标记为可疑交易报告；此外对银行间结算设置风险敞口上限（如跨境流量 ⩽ 200,000 AED/ 月）以维持流动性。
risk_score + pattern **风险评分与模式**	Unusual activity detection: patterns like repeated sub-threshold transfers elevate risk; ≥ AED 15,000 with indicators prompts HOLD and filing, drawing from CBUAE AML/CFT guidelines for traditional systems. 异常活动监测：识别拆单（分批小额转账）等模式；金额 ⩾ 15,000 AED 且伴有风险指标时触发挂起并报备。
time_window **时间窗口**	Settlement gating: non-exempt institutions may only process during business hours (e.g., 08:00-16:00 GST) on working days, aligned with RTGS availability; others REJECT or HOLD. 结算准入控制：非豁免机构仅能在工作日的营业时间内（如 08:00-16:00 GST）处理业务，以匹配 RTGS 系统的可用性；非营业时间予以拒绝或挂起。
licensing_status **牌照状态**	Mandatory licensing for DLT adopters: transactions REJECT if entity lacks CBUAE/FSRA/DFSA approval for activities like settlement or custody; governance framework must be documented and audited. DLT 准入强制许可：若实体缺乏 CBUAE/ 阿布扎比全球市场金融服务监管局（FSRA）/ 迪拜国际金融中心金融服务管理局（DFSA）针对结算或托管业务的许可，交易将予以拒绝；治理框架必须经过存档与审计。

Example rule snippet
规则代码片段示例
	`when:`
	` asset.type == "TOKENIZED_SECURITY"`
	` and subject.investor_type == "RETAIL" # 若资产为代币化证券且投资者为零售散户`
	`check:`
	` amount <= 100_000_USD # 检查金额是否在 10 万美元等值范围内`
	`then:`
	` allow() # 允许交易`
	`else:`
	` reject(code="FSMR_EXEMPTION_LIMIT") # 否则拒绝，并返回“超出 FSMR 豁免限额”代码

Table 15: UAE regulatory rules encoded using Core DSL Primitives / 表 15：使用核心 DSL 原语编码的阿联酋监管规则

These primitives allow UAE rules to be represented in a JPack such as **UAE-DLT**, with tests verifying governance, thresholds, interoperability, and resilience in cross-border workflows while ensuring alignment with traditional financial regulations[14-15,31].

式遵循 ISO 20022 报文标准，安全与效率符合《金融市场基础设施原则》（PFMI）[32,41-42]。

核心项目包括：用于批发型银行间结算的数字迪拉姆发行平台，以及与沙特阿拉伯合作的跨境央行数字货币结算试点项目（Project Aber）。后者强调商业银行间多中心化的点对点转账，旨在摆脱对传统代理行模式的依赖[4,6,21,45]，实现跨境支付的直接结清。

采用 DLT 的机构必须遵守 CBUAE《金融机构采用赋能技术指南》中的治理、设计和运营要求，涵盖可审计性、业务连续性和风险管理。在反洗钱 / 反恐怖融资（AML/CFT）方面，其义务与传统转账一致，包括强制性的 KYC、制裁筛查和可疑交易报告。当交易金额触发特定阈值时，需执行增强型尽职调查（EDD）并进行备案；跨境资金流动则必须通过获批的合规走廊，并在适用时遵守数据本地化要求[1-3,8]。

在 Policy-DSL 中，这些要求通过牌照检查、金额阈值和结算条件等原语实现；PoPC 则可以记录脱敏后的交易元数据等证明，在不泄露敏感数据的前提下验证合规性。

- **核心诉求**：金融稳定、ISO 标准对齐、结算最终性、走廊准入。
- **DSL 原语映射**：iso_20022_compliant（报文标准）、corridor_id（合规走廊）、edd_status（增强型尽职调查）。

政策关注：金融稳定、AML/CFT 执行、运营韧性、结算最终性以及与现有系统的互操作性。

通过这些原语，阿联酋的监管规则可集成至 **UAE-DLT** JPack 。JPack 可通过自动化测试，验证跨境流程中的治理、阈值、互操作性和韧性，确保与传统监管要求保持高度一致[14-15,31]。

A5.12

Summary:
From Policy Diversity to the Consensus of Governance-as-Code

The Policy-DSL and PoPC framework is far more than a simple technical plug-in; it establishes a unified and verifiable foundation for expressing and enforcing cross-jurisdictional regulatory policies on shared digital infrastructure. By directly linking governance intent with transaction execution, diverse regulatory requirements can be encoded into machine-readable rules. This not only achieves deterministic automated enforcement but also ensures the immutability and authenticity of every decision through cryptographic proofs.

The framework reconciles divergent global policy models through a verifiable technical architecture. Jurisdictions simply encapsulate their regulatory rules into formal Policy Packs (JPack), which are then enforced by a deterministic Regulatory Virtual Machine. This mechanism thoroughly **bridges the long-standing gap between high-level policy vision and low-level technical execution**. In essence, it constructs a "Constitutional Logic" for digital finance: whether it be KYC tiers, asset caps, or trading hours, these complex policy requirements are distilled into a lean DSL and deeply embedded into the bloodlines of the transaction flow, where the system automatically evaluates and generates cryptographic proofs of compliance or violation.

This deep integration of Policy-DSL and PoPC allows different jurisdictions to run their unique regulations in parallel on shared infrastructure without losing interoperability, effectively cracking the fragmentation puzzle that currently hampers cross-border tokenized markets. Crucially, every decision to approve, hold, or reject a transaction becomes reproducible and auditable, ensuring that regulators can trust that policy is not merely a "paper declaration" but is being executed and proven in real time.

By design, **Policy-DSL remains minimal and jurisdiction-neutral, which encourages regulatory convergence**: regulators define rules in a shared syntax, while the PoPC model standardizes the "standard taxonomy" of compliance reporting. This means

总结：
从政策多样性到治理即代码的共识

Policy-DSL 与 PoPC 框架并非简单的技术插件，它在共享数字基础设施上，为表达和执行跨司法辖区的监管政策奠定了统一且可验证的底座。通过将治理意图与交易执行挂钩，多元的监管要求得以被编码为机器可读的规则。这不仅实现了确定性的自动化执行，更通过密码学证明确保每一项决策的不可篡改与真实性。

该框架通过这一可验证的技术方案，巧妙地化解了全球不同政策模型之间的冲突。各司法辖区只需将自己的监管规则打包成正式的 JPack，就能由确定性监管虚拟机直接强制执行。这种机制彻底**弥合了高层政策愿景与底层技术落地之间那道长期存在的断层。从本质上讲，它为数字金融构建了一套“宪法逻辑”**：无论是 KYC 等级、资产限额还是交易时间，这些复杂的政策要求都被浓缩进精简的 DSL 语言，并深植于交易流程的血脉之中，系统会自动判定并生成合规或违规的密码学证明。

Policy-DSL 与 PoPC 的深度结合，让不同辖区在共享基础设施上并行运转各自独特的法规，同时又不失互操作性，有力地破解了阻碍跨境代币化市场发展的碎片化难题。至关重要的是，每项关于放行、挂起或拒绝的决策都变得可复现、可审计，确保监管机构相信政策不仅停留在纸面上，而是得到了实时执行与证明。

在设计逻辑上，**Policy-DSL 保持了极简且辖区中立的特性，这无形中促进了监管趋同**：监

that even widely varying paths, such as the U.S. Travel Rules, EU MiCA restrictions, or Singapore MAS conditions, can coexist and be cross-verified within one framework. In effect, this achieves "**Governance-as-Code**" (not supplanting legal authority, but operationalizing it); meanwhile, technical enforcement is elevated to a governance tool, providing unprecedented transparency and accountability for automated decisions.

This approach represents a solid step toward "Embedded Supervision." It responds to the Bank for International Settlements (BIS) vision of automatically monitoring compliance by "**reading the ledger**", enabling a "**Trust but Verify**" paradigm. This significantly lowers oversight costs, reduces reliance on traditional post hoc reporting, and utilizes selective disclosure to protect user privacy while proving compliance. In this model, the regulator's enforcement and monitoring are woven into the network's underlying operations, aligning with global initiatives for "**same activity, same risk, same regulation**" and strengthening cross-border coordination. By providing this neutral compliance layer, the framework acts much like internet protocols, harmonizing global financial communication without altering national laws.

Finally, **the long-term implications of this unified architecture for the international financial system are worth reflecting upon**. As regulatory guidelines from the BIS, IMF, and FSB become increasingly dense, a broad consensus has emerged: for digital assets and decentralized finance to achieve safe growth at scale, a more programmable and verifiable compliance regime must be established. The framework described here offers exactly such a blueprint. It serves as a "Greatest Common Denominator" for policy expression, functioning much like International Accounting Standards do for financial reporting - allowing a tokenized transaction carrying a compliance proof to be seamlessly accepted by global counterparties because its logic is transparent and its format is standardized.

Policy-DSL and **PoPC** unify governance and enforcement into a single verifiable system: one that preserves jurisdictional sovereignty while resolving fragmentation risks and enabling transparency and trust at scale. They lay a practical foundation for embedded compliance in a multipolar world, providing the technical backbone for long-term collaboration among regulators, technologists, and standard-setters.

管机构在统一语法下定义规则，而 PoPC 模型则规范了合规报告的“标准分类法”。这意味着，即便面临截然不同的路径（如美国的旅行规则、欧盟的 MiCA 限额，或新加坡的许可条件）都可以在同一个框架下并存并交叉验证。

实际上，这实现了“**治理即代码**”（并非取代法律权威，而是将其付诸实践）；同时，技术执行也上升为一种治理工具，为自动化决策提供了前所未有的透明度与问责制。

此方案更是迈向“**嵌入式监管**”的坚实一步。它响应了国际结算银行（BIS）关于“通过读取账本自动监测合规性”的愿景，让监管机构实现了**“信任但可验证”的范式**：这显著降低了监管成本，摆脱了对传统事后报表的依赖，并利用选择性披露在证明合规的同时，守住了用户隐私的底线。这种模式下监管者的执行与监测编织进网络运行的底层，契合了全球关于“**同质业务、同等风险、同等监管**”的一致性倡议，并加强了跨境协作。通过提供中立合规层，本框架正如互联网协议一样，在不改变各国法律前提下，实现了全球金融通信协调一致。

最后，**这种统一架构对国际金融系统的长远意义值得深思**。随着 BIS、IMF 及 FSB 的监管指南日益密集，业界已达成共识：数字资产若要规模化增长，必须建立一套可编程、可验证的合规体系。本文描述的框架正是一份实践蓝图。它可以作为政策表达的“最大公约数”，发挥类似于国际会计标准的作用，让一笔携带合规证明的交易，因其逻辑透明、格式标准，而能被全球对手方无缝接受。

Policy-DSL 和 **PoPC** 将治理与执行统一进一个可验证系统：它在尊重司法辖区主权的同时化解了碎片化风险，实现了大规模的透明与信任，为多极化世界的嵌入式合规奠定技术支撑。

CHAPTER A6.

Layers & Domains:

Engineering Verifiable Interoperability Across Sovereignties

A6. 章节

分层与域模型：

主权间可验证互操作的工程基础

Abstract:

At present, the global deployment of digital currencies and the digital transformation of financial infrastructure have become an established trend. Against this backdrop, the international community faces a fundamental challenge: how to design a global settlement system that meets the demands of the era - one that both fully respects and safeguards national monetary sovereignty and regulatory autonomy, while significantly enhancing the efficiency and transparency of cross-border financial activities?

In the preceding chapters, we established the core values that Sovereign-Verifiable Settlement Interface should adhere to (A2), and outlined the corresponding governance framework (A4) and the path toward rule codification (A5). This chapter takes the most critical step forward: translating the aforementioned theoretical blueprint into a globally deployable and operable engineering system.

Our basic approach is to construct a layered, open, and interoperable architecture. This architecture is intended to achieve the following objectives:

1. **Integration rather than replacement**: This framework does not seek to reconstruct or replace existing core financial infrastructures such as RTGS, CSD, or SWIFT. Instead, it provides a parallel, verifiable collaboration mechanism. It does not alter the internal structure of existing systems; rather, it establishes a neutral, standardized, and traceable system of records and proofs at key nodes of cross-system interaction, enabling relevant business processes to be independently verified, replayed, and audited. The "integration" referred to here means achieving verifiable business mapping and coordination across sovereign and system boundaries, rather than structural consolidation at the system level.
2. **Clear division of responsibilities and layered collaboration**: By introducing two foundational core functional layers, a clear separation of rights and responsibilities is achieved. As we mentioned in A5, SRH and SCEL form two coordinated layers with a clear split of responsibilities. Each jurisdiction runs its own SCEL to execute transactions under local rules and generate compliance proof. The jointly governed, technically neutral SRH then orders cross-border transactions, verifies the PoPC, and issues final settlement confirmation.
3. **Trust through proof transmission**: Through the PoPC mechanism, compliance outcomes executed locally by each country and institutional organisation can be transformed into standardized proof packages that can be securely transmitted across the global network and independently verified by other participants.
4. **Establishing a layered asset-mapping system**: At the same time, we will construct a standardized set of "S-series" accounting labels to provide a unified on-chain mapping and identification method for various categories of financial liabilities, including cash, deposits, and wholesale settlement assets. This does not create new monetary layers; rather, it is intended to make complex multi-layer clearing processes clearer, more traceable, and auditable.

Through the above design, this chapter seeks to translate the two core principles of "settlement neutrality" and "verifiable compliance" into an engineering system that can be globally deployed and that supports incremental collaboration, thereby outlining a clear and credible implementation path for the next generation of financial networks.

（本章摘要）

当前，数字货币的全球部署与金融基础设施的数字化转型已成定势。在此背景下，国际社会面临一个根本性的挑战：如何设计一套符合时代需求的全球结算系统，使其既能充分尊重并保障各国的货币主权与监管自主权，又能显著提升跨境金融活动的效率与透明度?

在之前的章节中，我们确立了主权可验证结算框架应遵循的核心价值（A2）、并为其勾勒了相应的治理框架（A4）与规则编码化路径（A5）。本章将迈出最关键一步：将前述理论蓝图，转化为一套可实际部署与运行的全球性工程体系。

我们的基本思路是构建一套分层、开放的互操作架构。这一架构旨在实现以下目标：

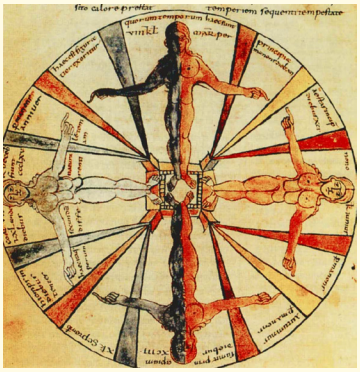
1. **整合而非取代**：本框架无意重构或替代 RTGS、CSD、SWIFT 等现有核心金融基础设施，而是提供一种并行的、可验证的协作机制：它不改变原有系统内部结构，只在跨系统交互的关键节点上建立一套中立、标准化、可追溯的记录与证明体系，使相关业务流程具备独立验证、重放和审计的能力。这里所说的整合，是指在跨主权、跨系统语境下实现可验证的业务映射与协同，而非系统结构层面的合并。
2. **清晰分工与分层协作**：通过引入两个基础核心功能层，本框架实现了明确的权责分离。正如我们在 A5 章节中所述，SRH 与 SCEL 构成了两个分工明确的协同层级。各司法管辖区负责运行各自的 SCEL，旨在根据当地规则执行交易并生成合规证明。随后，由多方共同治理且保持技术中立的 SRH 负责对跨境交易进行排序，验证正当合规证明（PoPC），并发布最终结算确认。
3. **以证明传递信任**：借助合规性证明（PoPC）机制，各国及机构组织在本地执行的合规结果，能够转化为标准化的证明包。这些证明包可以在全球网络中安全传输，并由其他参与者进行独立验证。
4. **建立资产分层映射体系**：同时，我们将构建一套标准化的“S 系列”记账标签，为现金、存款、批发结算资产等各类金融负债提供统一的链上映射与标识方法。这并非创造新的货币层级，而是为了使复杂的多层清算过程变得更为清晰、可追溯、可审计。

通过以上设计，本章致力于将结算中立 与可验证合规两大核心原则，转化为一套可供全球部署、支持渐进式协作的工程体系，从而为下一代金融网络勾勒出一条清晰且可信的实现路径。

A6.1

Settlement-Oriented Overall Layering

结算导向的总体分层



Four elements, 7th century, Isidore of Seville.

"Unity in diversity is the most perfect expression of the universe."

"多样性中的统一，是宇宙最完美的表达。"

— Gottfried Wilhelm Leibniz, Monadology (莱布尼茨·《单子论》)

From the perspective of settlement finality and process proof collection, this system is architecturally and explicitly divided into the following four layers:

1. **Domestic and Institutional Core Systems Layer**: This layer constitutes the foundation of each country's existing financial system. It is composed primarily of central banks-operated real-time gross settlement systems (RTGS), central securities depositories (CSD), fiscal and taxation systems, and the core ledgers of commercial banks. This layer operates within the national legal framework and bears ultimate legal responsibility and final funds settlement. This framework does not seek to replace this layer; rather, it aims to securely interface with it through standardized interfaces.
2. **Sovereign Compliance & Execution Layer (SCEL)**: This is a distributed ledger layer independently built and controlled by sovereign states or their authorized institutions. It connects to the aforementioned domestic and institutional

从结算最终性与过程取证的角度出发，本体系在架构上明确划分为以下四层：

1. **本地主权系统层**：这是各国现有金融体系的根基，主要由中央银行运营的大额支付系统（RTGS）、证券存管系统（CSD）、财税系统及商业银行的核心账本等构成。该层在本国法律框架下运行，承载着最终的法律责任和资金结算。本框架不寻求替代这一层，而是旨在通过标准化接口与其安全对接。
2. **主权合规执行层 (SCEL)**：这是由主权国家或其授权机构自主建设与控制的分布式账本层。它通过安全网关与上述本地核心系统连接，充当本国监管政策与

core systems through secure gateways and serves as the digital "execution terminal" for national regulatory policies and business rules. It is a critical hub linking the domestic financial system with the global collaboration network.

Its primary functions include:

- ◇ Processing financial logic within the programmable ledger layer (on-chain).
- ◇ Running a programmable policy definition language engine (Policy-DSL) to automate the execution of compliance validation.
- ◇ Generating standardized, verifiable compliance proof (PoPC) for each transaction execution.

3. **Sovereign Relay Hub (SRH)**: This is a global coordination network jointly governed by participating countries and maintaining technical neutrality. In essence, it serves as the public routing and verification layer for global settlement, ensuring that cross-sovereign transactions can be completed in an orderly and trustworthy manner. Its core positioning is very clear:
   - ◇ **Coordination only, not adjudication**: providing global ordering and final settlement confirmation for cross-border transactions originating from the SCELs of various countries.
   - ◇ **Verification of proof only, not interpretation of rules**: verifying whether the compliance proof (PoPC) submitted alongside transactions by each country is valid and complete, without intervening in or judging the content of any country's internal rules themselves.
4. **Audit & Observation Layer**: This layer is composed of independent audit institutions, regulatory nodes, research organizations, and similar entities. It typically does not directly access raw business data; instead, through standardized, privacy-preserving proof summaries and cryptographic proofs (such as zero-knowledge proofs) provided by the lower layers, it independently replays transaction logic and verifies compliance execution under strict protection of data sovereignty and commercial confidentiality. Its core function is to form an objective, third-party assessment of the neutrality, continuity, and overall trustworthiness of the entire system, and it is a key design element for maintaining transparency and enabling public oversight.

Through this four-layer division, we achieve a clear architecture

商业规则在数字世界的"执行终端"。它是连接本国金融体系与全球协作网络的关键枢纽。

其主要职能包括：

- ◇ 在链上处理业务逻辑；
- ◇ 运行可编程的规则引擎（Policy-DSL），自动执行合规审查；
- ◇ 为每一笔业务生成标准化的合规证明（PoPC）。

3. **主权中继枢纽 (SRH)**：这是一个由参与各国共同治理、并保持技术中立的全球性协调网络。它本质上是全球结算的公共路由与验证层，确保跨主权业务能够有序、可信地完成。其核心定位非常清晰：
   - ◇ **只做协调，不做裁决**：为来自各国 SCEL 的跨境交易提供全局排序和最终结算确认。
   - ◇ **只验证明，不解释规则**：验证各国随交易提交的 PoPC 是否有效、完整，但不介入或评判任何国家内部的规则内容本身。
4. **审计与观察层**：这一层由独立的审计机构、监管节点及研究机构等组成。该层通常不直接访问原始业务数据，而是通过各下层提供的标准化、脱敏的证明摘要与密码学证明（如零知识证明），在严格保护数据主权与商业隐私的前提下，独立地重放交易逻辑、验证合规执行。其核心职能是对整个系统的中立性、连续性及整体可信度形成客观的第三方评价，是体系保持透明、接受社会监督的关键设计。

通过这四层划分，我们实现了"**主权境内责任自治、跨域结算协同共治、全过程审计独立**"

of "**sovereign domestic responsibility autonomy, cross-domain settlement coordination under shared governance, and full-process independent auditing**", thereby laying a solid engineering foundation for complex inter-sovereign collaboration. As illustrated in the figure below, the off-chain portion comprises the existing financial infrastructures of various countries. These legacy services upload transaction information to the respective blockchain networks owned (or selected) by each sovereign state, which may be either public blockchains or permissioned consortium chains. Regardless of the network type chosen by a sovereign state , before conducting cross-domain (cross-border) transactions via the SRH, the transaction must first pass through the SCEL deployed on the sovereign state's own (or selected) blockchain network to complete internal compliance validation and generate the relevant compliance proofs within the originating jurisdiction.

的清晰架构，为复杂的主权间协作奠定了坚实的工程基础。如下图所示，链下的部分是各国现有的金融基础设施，这些现有服务会把交易信息上传至各个主权国家自有的（或选定的）区块链网络，这个网络可以是公链，也可以是需要许可加入的联盟链。无论主权国家选择那种类型的网络，在通过 SRH 做跨域（跨国）交易之前，都必须通过部署在主权国家自有（或选定）区块链网络上的 SCEL，完成发起国内部的合规审查，并生成相关证明。

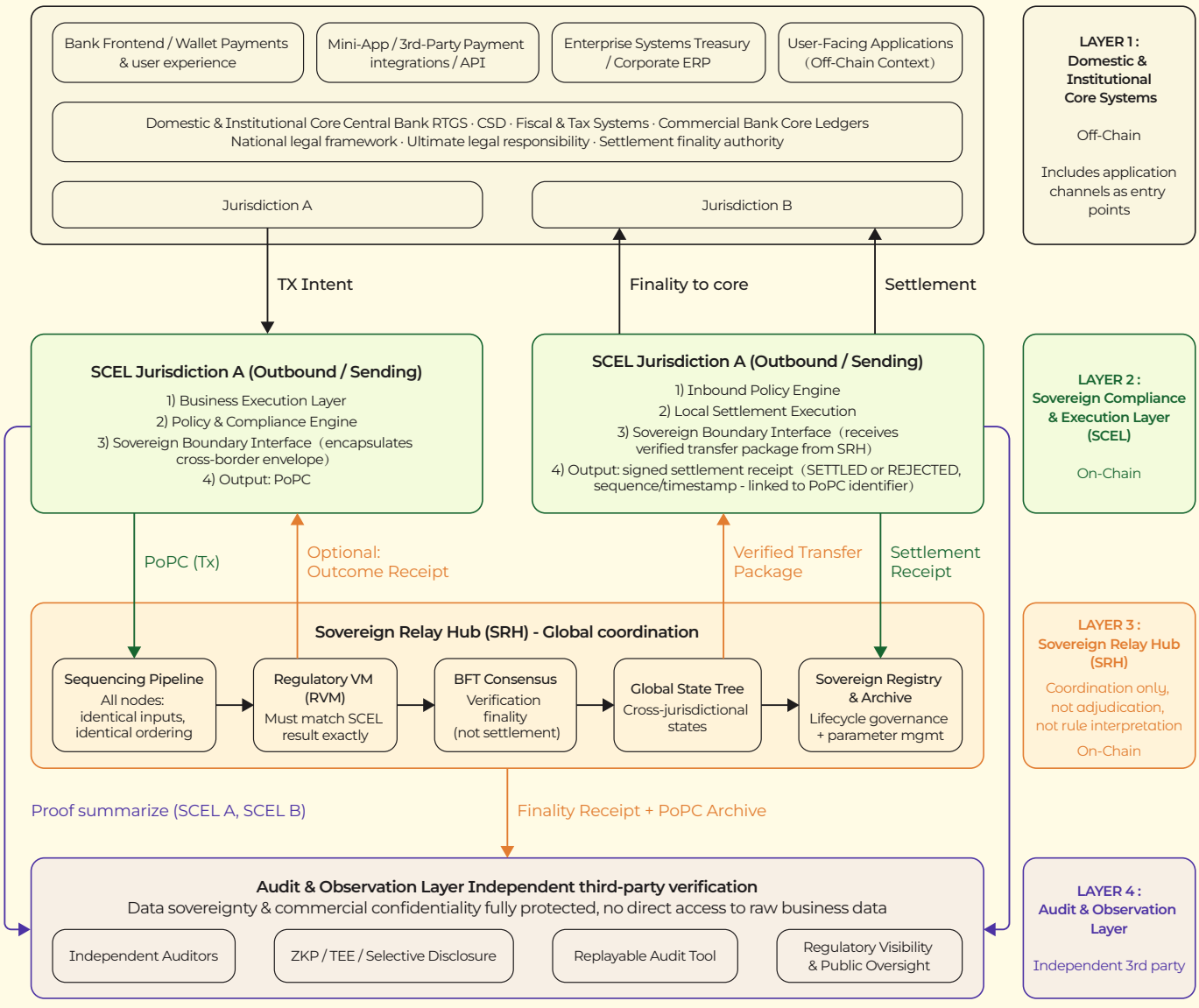


Figure 7: Overview of the Settlement-Oriented Layered Model / 图7：结算导向分层模型总览

To clearly describe and position on-chain assets within the above layered architecture, we introduce the S-series labels as a set of descriptive and functional on-chain mapping instruments. These labels are used to identify the differences among various types of on-chain assets in terms of their clearing hierarchy, settlement capability, and credit attributes. Conceptually, this system draws upon the distinctions of asset liquidity and credit hierarchy found in traditional monetary statistics - M0, M1, and M2, but it does not attempt to replicate their statistical classifications; rather, it provides an attribute identification framework for on-chain assets oriented toward settlement and legal semantics. It must first be made explicit that this labeling system is not a proposal for monetary hierarchy reform, nor does it require sovereign authorities to adjust existing statistical classifications. Its core function is to **provide a unified digital identity for various categories of financial liabilities represented on-chain**, and to establish a mappable and auditable correspondence with traditional accounting accounts.

- **S0 Cash-Type On-Chain Liabilities**:
  - ◇ Definition: Represent programmable sovereign monetary claims at the highest level of liquidity, which are directly equivalent, in both legal and accounting terms, to physical cash in digital form.
  - ◇ Examples: Retail central bank digital currencies (such as the digital RMB); legally recognized small-denomination digital bearer instruments.
  - ◇ Monetary statistical relationship: $S0 \subseteq M0$, and subject to dynamic constraints on the cash substitution ratio.
- **S1 Deposit-Type On-Chain Liabilities**:
  - ◇ Definition: Tokenized bank liabilities that are payment-capable and supported by deposit insurance or full reserve backing.
  - ◇ Examples: Tokenized demand deposits that comply with Basel III liquidity coverage ratio requirements; regulated stablecoins; prefunded account tokens within RTGS systems.
  - ◇ Monetary statistical relationship: $S1 \in [M1, M2]$, with issuance scale constrained by the applicable reserve requirement regime (see Appendix for the specific formulation).
- **S2 Structured Redeemable Liabilities**:
  - ◇ Definition: Programmable debt instruments with explicit maturity structures or redemption conditions.

为了在上述分层架构中清晰描述与定位链上资产，我们引入 S 系列标签，作为一套描述性、功能性的链上资产分类工具，用于标识不同类型链上资产在结算层级、可清偿性与信用属性上的差异。该体系在概念上借鉴传统货币统计中 M0、M1、M2 对资产流动性与信用层级的区分方式，但并不试图复制其统计口径，而是为链上资产提供一套面向结算与法律语义的属性标识框架。必须首先明确，本标签体系并非货币层级改革方案，也不要求主权机构调整现有统计口径，其核心功能是**为各类在链上表征的金融负债提供统一的数字身份标识**，并与传统会计科目建立可映射、可审计的对应关系。

- **S0 现金型上链负债**：
  - ◇ 定义：代表最高流动性层级的可编程法定债权，在法律与会计层面直接等价于物理现金的数字形式。
  - ◇ 实例：零售端央行数字货币（如数字人民币）、法定小额数字凭证。
  - ◇ 货币统计关系：$S0 \subseteq M0$，且满足现金替代率的动态约束条件。
- **S1 存款型上链负债**：
  - ◇ 定义：具备存款保险或全额准备金支持、可用于支付的代币化银行负债。
  - ◇ 实例：符合巴塞尔协议 III（Basel III）流动性覆盖率要求的代币化活期存款；受监管的稳定币；RTGS 系统的的预充值账户代币。
  - ◇ 货币统计关系：$S1 \in [M1, M2]$，其发行规模受相应的存款准备金要求约束（具体关系式见附录）。
- **S2 结构化可兑付负债**：
  - ◇ 定义：具有明确期限结构或兑付条件的可编程债权凭证。

- ◇ Examples: Tokenized money market fund units compliant with specific jurisdictional frameworks (such as the EU MMFR); time-deposit certificates embedded with smart contracts; securitized payment commitments (e.g., tokenized accounts receivable).
- ◇ Monetary statistical relationship: S2 corresponds to broad money aggregates M2+/M3 and requires adjustment using risk metrics such as duration (weighted average maturity) (see Appendix for detailed formulas).

- **S* Wholesale Settlement Assets**:
  - ◇ Definition: Digital representations of central bank monetary claims dedicated exclusively to final settlement within clearing and settlement systems.
  - ◇ Examples: Wholesale central bank digital currency; distributed RTGS settlement account units; reserve asset tokens used by cross-border multilateral clearing platforms.
  - ◇ Systemic importance indicators: As critical settlement assets, their issuance and circulation scale must satisfy system-wide risk constraints associated with network topology (see Appendix for specific conditions).

Based on the above layering and asset labeling framework, we can clearly address two concrete questions that are critical in engineering practice. These questions also mark the key transition of this framework from an "architectural concept" to an "implementation guideline".

First, compatibility with and migration from traditional banking infrastructure:
How are existing cross-border settlement processes based on SWIFT messaging and RTGS systems mapped within this framework? Which layer is involved, and which category of S-series assets is used? The answers directly determine whether existing banking operations can be smoothly migrated and integrated into the new system without service disruption. The key lies in clearly defining interfaces with existing standards such as SWIFT and ISO 20022, and in ensuring that fund movements through traditional channels can be reliably and automatically reconciled with on-chain state transitions.

Second, standardized expression of on-chain business processes:
Once retail payments, large-value transfers, securities delivery, and other transaction types are migrated to an on-chain environment, how can their inherent legal attributes, clearing hierarchy,

- ◇ 实例：符合特定司法管辖区框架（如欧盟 MMFR 等）的代币化货币基金份额；嵌入智能合约的定期存款凭证；证券化支付承诺（如应收账款代币）。
- ◇ 货币统计关系：S2 对应于广义货币 M2+/M3，需进行久期（加权平均到期期限）等风险指标调整（具体计算公式见附录）。

- **S* 批发结算资产**：
  - ◇ 定义：专门用于清算系统最终结算的央行货币债权数字化形态。
  - ◇ 实例：批发型央行数字货币；分布式 RTGS 结算账户单元；跨境多边清算平台的储备资产代币。
  - ◇ 系统重要性指标：作为关键结算资产，其发行与流通规模需满足与网络拓扑相关的系统性风险约束（具体条件见附录）。

基于上述分层与资产标签体系，我们不仅获得了一套描述资产与结算关系的抽象语言，也首次具备了将传统金融基础设施与链上系统进行一一对齐和工程化落地的条件。在此基础上，我们可以清晰回应两个在工程实践中至关重要的具体问题，这也是本框架从"架构理念"迈向"实施指南"的关键。

第一，与传统银行基础设施的兼容与迁移：
当前基于 SWIFT 报文与 RTGS 系统的跨境结算流程，在本框架中具体如何映射?涉及哪一层和哪种 S 系列资产?这直接决定了现有银行业务能否在不中断服务的前提下，平滑地迁移并融入新体系。关键在于明确如何与 SWIFT、ISO 20022 等现行标准对接，并确保传统渠道的资金变动能与链上状态实现可靠、自动化的对账。

and compliance requirements be translated into standardized and programmable transactional logic through unified S-labels and compliance proof? The ultimate objective is to enable market participants to conduct operations via clear interaction interfaces (such as APIs or front-end applications), without needing to perceive differences in the underlying payment infrastructure.

Providing answers to these two questions is precisely the point at which this framework moves from an “architectural concept” to an actionable “implementation guideline”.

第二，上链业务流程的标准化表达：
当零售支付、大额转账、证券交割等各类业务迁移到链上环境后，如何通过统一的 S 标签与合规证明，将其内在的法律属性、清算层级及合规要求，转化为标准化的、可编程的业务逻辑?其最终目标是让业务参与方能够通过清晰的交互接口（如 API、前端应用）开展业务，而无需感知底层支付基础设施的具体运作差异。

对这两个问题的回答，正是本框架从“架构理念”走向“实施指南”的关键。

A6.2

Sovereign Compliance & Execution Layer Model

主权合规执行层模型

Within this framework, the SCEL constitutes the core engineering hub through which a national financial system interfaces with the global settlement network. It is located entirely within national jurisdiction, and its primary responsibility is to transform domestic laws and regulatory rules into verifiable actions for global collaboration.

Clear jurisdictional attribution: Each instance of the SCEL is explicitly attributable to a single sovereign state or its statutory authorities, and is fully subject to that state’s legal and regulatory jurisdiction.

Deep system coupling: Through standardized and secure gateways, it is institutionally integrated with the country’s real-time gross settlement systems, central securities depositories, and fiscal and taxation systems.

Clear functional positioning: It assumes three critical functions:

- **Specific rule execution**: serving as the operational endpoint for domestically defined programmable rules.
- **proof generation**: producing auditable compliance proofs

本框架中的 SCEL，是一国金融系统通往全球结算网络的核心工程枢纽。它位于国家司法管辖之内，核心职责是将本国法律与监管规则，转化为可验证的全球协作行动。

管辖归属明确：每一套主权合规执行层都明确归属于单一主权国家或其法定机构，完全处于该国法律与监管的直接管辖之下。

系统深度耦合：通过标准化的安全网关，与本国实时全额结算系统、中央证券存管系统及财税系统实现制度化对接。

功能定位清晰：承担三项关键职能

- **执行规则**：作为本土可编程规则的运行终端。
- **生成证明**：为每笔业务处理可审计的 POPC。

for each transaction processed.

- **Global connectivity**: acting as the sole standardized ingress and egress for national transactions entering and exiting the global SRH state.

Positioned as such, SCEL is far from an abstract institutional vision; it is a deployable system characterized by well-defined engineering boundaries and operational logic. Its pivotal status is not contingent upon centralized discretion or external authorization, but is instead rooted in its minimum architecture, its integration with national core financial infrastructures, and its standardized outward-facing compliance interfaces.

To achieve the deterministic execution and verifiable expression of sovereign rules within a digital environment, SCEL must clarify - at an engineering level - the division of functional modules, the boundaries of legal validity, and the semantics of cross-domain interaction. The subsequent sections delineate the implementation path of SCEL across three dimensions: the minimum architecture, domestic system integration models, and standards-aligned interfaces.

A6.2.1 Minimal Component Architecture

To transform a conceptual design into an operational entity, the Sovereign Compliance & Execution Layer must comprise the following five core functional modules:

1. **Execution Engine**: A DLT-based smart contract execution environment, whose core purpose is to provide **deterministic and verifiable execution outcomes**. Given identical input data and rule versions, it guarantees identical outputs regardless of the execution environment, forming the foundation for full-process reproducibility.
2. **Policy-DSL Engine**: A programmable rules engine that encodes national AML/CTFrequirements, quota and geographic restrictions, business authorization rules, and similar policies into executable code via a domain-specific language. It supports automated decision-making across the full lifecycle of ex ante validation, in-process execution, and ex post review.
3. **Compliance Proof Module**: The system's "proof generator". After each rule execution, it automatically packages a compliance proof that clearly records the applicable rule version, input data, decision outcome, and associated metadata such as timestamps. These proofs are securely

- **连接全球**：成为本国业务进出全球主权中继枢纽的唯一标准化出入口。

在上述定位下，SCEL 并非抽象的制度设想，而是一套具备明确工程边界与运行机制的可部署系统。其枢纽性不依赖集中裁量或外部授权，而体现在其最小组成架构、与本国核心金融系统的集成方式，以及对外采用的标准化合规接口之中。

为实现主权规则在数字环境中的确定性执行与可验证表达，SCEL 需在工程层面明确功能模块划分、法律效力边界及跨域交互语义。下文将从最小组成架构、国内系统集成模式与标准对齐接口三个方面，对其实现路径予以界定。

A6.2.1 最小组成架构

将一个概念转化为可实际运行的实体，SCEL 必须具备以下五个最核心的功能模块：

1. **事务执行引擎**：基于区块链的智能合约执行环境，其核心在于提供**确定且可验证的执行结果**：只要输入数据和规则版本相同，无论在哪里运行，都保证输出完全一致的结果，这是实现全流程可重现性的基础。
2. **可编程规则引擎**：通过领域专用语言将本国反洗钱 / 反恐融资、额度与地域限制、业务许可等政策转化为可执行代码，支持事前校验、事中执行与事后审查的全流程自动化判断。
3. **合规证明模块**：系统的“证明生成器”。每次规则执行后，自动打包生成合规性证明，清晰记录所使用的规则版本、输入数据、决策结果以及时间戳等元数据。这些证明被安全归档，形成可供独立审计乃至司法采信的链外证明库。

archived, forming an off-chain proof repository suitable for independent audit and potential judicial admissibility.

4. **Cross-Domain Gateway**: The system's "internal–external connector". Internally, it securely interfaces with domestic payment, securities, and taxation infrastructures; externally, it connects to the SRH. Its core task is to package "transaction data" together with the corresponding "compliance proofs", transmit them securely to the global network, and retrieve settlement confirmations and finalized on-chain proofs from the ledger.
5. **Logging & Monitoring Module**: Records all critical state transitions, policy updates, and metadata related to the generation and verification of compliance proofs, providing tiered and transparent observability interfaces for system operations, compliance review, audit oversight, and policy research.

The above five modules constitute **the minimum viable and operational** backbone of the SCEL. Each country may, based on its level of digital maturity, risk appetite, and policy priorities, adopt different technological pathways and deployment cadences - for example, starting with regional pilots and gradually scaling into nationwide financial infrastructure.

A6.2.2 Coupling with Domestic Core Systems

The design objective of the SCEL is not to replace existing national core financial systems, but rather to establish flexible and reliable connections with them through standardized interfaces. Depending on business requirements and implementation pathways, there are three primary integration modes:

1. **Mirror Mode**
   - ◇ **Core Definition**: SCEL serves as a real-time, programmable mapping layer for key settlement events and legal states related to cross-sovereign settlement within core systems such as RTGS and CSDs.
   - ◇ **Operating Mechanism**: Final settlement and fund delivery in the legal sense continue to be completed within the existing traditional systems. The SCEL synchronously records key transaction events and legal states related to cross-sovereign settlement, and on this basis, generates verifiable compliance proofs to support cross-domain reconciliation, auditing, and replaying.
   - ◇ **Core Value**: Without reconstructing existing core ledgers and settlement processes, this mode provides

4. **跨域网关**：系统的"内外连接器"。对内安全对接本国的支付、证券、税务等核心金融基础设施；对外连接全球性的主权中继枢纽（SRH）。其核心任务是将"交易数据"和对应的"合规证明"打包，安全地发送至全球网络，并接收来自网络的结算结果与相关反馈证明。
5. **日志与监测模块**：记录关键状态变更、策略更新及合规证明的生成与验证元数据，为系统运维、合规审查、审计监督及政策研究提供分层透明的观测界面。

以上五个模块构成了主权合规执行层**最低限度、可运行**的骨架。各国可以基于自身的数字化水平、风险偏好和政策重点，选择不同的技术路径和建设节奏，例如从区域性试点开始，逐步扩展为全国性的金融基础设施。

A6.2.2 与国内核心系统的集成模式

主权合规执行层的设计目标不是取代各国现有的核心金融系统，而是通过标准化的接口与它们建立灵活、可靠的连接。根据业务需求与实施路径的不同，主要有三种集成方式。

1. **备份镜像模式**
   - ◇ **核心定义**：SCEL 作为核心系统（如 RTGS、CSD）中与跨主权结算相关的关键结算事件与法律状态的实时、可编程化映射层。
   - ◇ **运行机制**：法律意义上的最终结算和资金交割仍在原有传统系统中完成。主权合规执行层同步记录与跨主权结算相关的关键交易事件与法律状态，并在此基础上生成可验证的合规证明，以支持跨域对账、审计与重放。
   - ◇ **核心价值**：在不重构既有核心账本

verifiable compliance proofs for current financial operations and establishes standardized interfaces for interaction with the global network. Therefore, it is well-suited as the preferred initial deployment option for most jurisdictions.

2. **Ledger-Primary Mode**
   - ◇ **Core definition**: The SCEL becomes the legally recognized primary ledger for specific innovative business domains, such as tokenized assets and new forms of wholesale payments.
   - ◇ **Operating mechanism**: The full business logic and asset ownership are recorded and executed within the SCEL. Traditional systems are relegated to the role of settlement channels and regulatory reporting layers.
   - ◇ **Key prerequisite**: Through domestic legislation or judicial precedent, the transaction records maintained by the SCEL must be explicitly granted final evidentiary effect in legal disputes.
3. **Hybrid Mode**
   - ◇ **Core definition**: Based on the value, risk profile, and innovation requirements of different business activities, hybrid deployment and layered management are applied between traditional systems and the SCEL.
   - ◇ **Operating mechanism**: High-value, low-frequency, and systemically critical transactions (such as large-scale government bond settlement) are retained within traditional systems to ensure maximum stability; high-frequency, low-value, or cross-institutionally complex activities (such as supply chain finance) are migrated to the SCEL.
   - ◇ **Consistency assurance**: Through programmable rules and compliance proof mechanisms, final consistency of transaction states across layers is ensured. Any operation involving cross-layer fund movements must generate corresponding compliance proofs as the basis for reconciliation.

The aforementioned three integration modes are not a simple juxtaposition of technical routes, but rather realistic implementation pathways tailored to diverse legal environments, business structures, and organizational maturity levels. In practical selection, a comprehensive evaluation is typically required regarding the legal status of the SCEL, the risk attributes of the target business, as well as the stability requirements and transformation costs of the existing core systems.

与结算流程的前提下，为现有金融业务提供可验证的合规证明，并构建与全球网络交互的标准化接口。因此，该模式适合作为多数国家在初始阶段的切入路径。

2. **主业务账本模式**
   - ◇ **核心定义**：主权合规执行层成为特定创新业务（如代币化资产、新型批发支付）的法定主账本。
   - ◇ **运行机制**：业务的完整逻辑和资产所有权在主权合规执行层上记录和执行。传统系统则退化为资金结算通道和监管数据报送层。
   - ◇ **关键前提**：需通过本国立法或司法判例，赋予主权合规执行层交易记录在法律争议中的最终证明效力。
3. **混合式分层模式**
   - ◇ **核心定义**：根据业务的价值、风险与创新需求，在传统系统与 SCEL 之间进行混合部署与分层管理。
   - ◇ **运行机制**：高价值、低频率的关键性业务（如大额国债结算）保留于传统系统层层以确保绝对稳定；高频、低价值或需要复杂跨机构协同的业务（如供应链金融）迁移至主权合规执行层。
   - ◇ **一致性保障**：通过可编程规则与合规证明机制，确保跨层交易状态的最终一致性。任何涉及跨层资金流动的操作，均需生成相应的合规证明作为对账依据。

上述三种集成模式并非技术路线的简单并列，而是针对不同法律环境、业务结构与组织成熟度所提供的现实落地路径。在实际选择中，通常需要综合考量 SCEL 的法律地位、目标业务

It should be specifically noted that the "mirroring" in Mirror Mode is not equivalent to full-scale replication or disaster-recovery synchronization of the core system. Instead, it involves the minimal and structured recording of critical states related to settlement and legal validity, which are used to generate compliance proofs and support cross-domain reconciliation. In this sense, its implementation cost is primarily concentrated at the interface and event extraction layers, rather than on the reconstruction of the existing ledger architecture.

This framework does not presuppose an evolutionary sequence or hierarchy among the three modes. Its sole invariant constraint is that any critical state change involving cross-sovereign settlement, regardless of the integration mode adopted - must be encapsulated and recorded through a unified compliance proof mechanism to ensure a globally verifiable and auditable consistent view.

This framework does not impose any a priori judgment regarding the superiority or inferiority of the three modes. The sole core constraint is that any critical state change involving cross-sovereign settlement, regardless of the integration mode from which it originates, must be recorded in a verifiable and standardized manner through the compliance proof mechanism, ensuring that the SRH and the global audit layer can reconstruct a trusted global view based on a unified proof ledger.

A6.2.3 Standards Alignment and Verifiable Compliance Interfaces

At the interface level, the architecture is designed to be compatible with ISO 20022 global payment messaging standards, supporting message transformation and semantic alignment at the Sovereign Gateway layer. This design enables seamless integration with financial market infrastructures (FMIs) without requiring modifications to existing RTGS, CSD, or cross-border messaging networks.

At the compliance level, the proof generation mechanism of PoPC fully covers the requirements for key information retention, identification of responsible entities, and end-to-end traceability as prescribed by the FATF “Travel Rule”. This allows cross-border transactions to carry independently verifiable compliance proof across different jurisdictions, thereby upgrading the traditional “ex-post manual reconciliation” model into a mechanism of “interim programmable verification and ex-post automated auditing”.

的风险属性，以及既有核心系统的稳定性要求与改造成本。

需要特别说明的是，备份镜像模式中的“镜像”并不等同于对核心系统进行全量复制或灾备式同步，而是对与结算与法律效力相关的关键状态进行最小化、结构化的记录，用于生成合规证明与支持跨域对账。在此意义上，其实施成本主要集中于接口与事件抽取层，而非对既有账本体系的重构。

本框架不预设三种模式的演进顺序或优劣高低，其唯一不变的约束是：凡涉及跨主权结算的关键状态变更，无论采用何种集成方式，均须通过统一的合规证明机制进行封装与记录，以确保全局层面可验证、可审计的一致视图。

本框架对三种模式不作预设性优劣评判。唯一的核心约束是：凡涉及跨主权结算的关键状态变更，无论源于何种集成模式，均须通过合规证明机制进行可验证记录与标准化封装，以确保 SRH 与全局审计层能够基于统一的证明链，重建可信的全局视图。

A6.2.3 标准对齐与可验证合规接口

在接口层面，本架构在设计上兼容 ISO 20022 全球支付报文标准，支持在主权网关层实现报文转换与语义对齐。这一设计使系统无需改造现有 RTGS、CSD 或跨境报文网络，即可实现与金融基础设施的无缝对接。

在合规层面，PoPC 的证明生成机制，完整覆盖了 FATF“旅行规则”所规定的关键信息留存、责任主体标识与全链路可追溯性要求。这使跨境交易可在不同司法辖区之间，携带具备可独立验证性的合规证明，从而将传统的“事后人工对账”模式，升级为“事中可编程验证、事后可自动化审计”的机制。

It must be clarified that such standards alignment does not imply the unification or centralization of the rules themselves; rather, its core objective is to provide a set of verifiable technical interoperability interfaces for a multi-sovereign system. The goal of these interfaces is to systematically reduce institutional friction costs in cross-system and cross-jurisdictional collaboration, rather than serving as a mandatory access tool or a uniform compliance template.

Under this framework, nations configure and express their own legal and regulatory requirements through JPack, rather than passively accepting external rules. The role of SCEL is precisely to provide, on this basis, a more direct and efficient way for countries to confirm whether transactions comply with their locally defined compliance standards.

In this sense, deploying SCEL and specifying nationally applicable laws and policies via JPack constitutes the fundamental prerequisite for the system's operation - namely, that each participant must indicate to the system in a verifiable manner: “What is compliant for ME”.

必须明确，此类标准对齐不代表规则本身的统一或集中。其核心目的在于为多主权体系提供一套可验证的技术互操作接口。该接口的目标，是系统性降低跨系统、跨法域协作中的制度性摩擦成本，而非作为强制性的准入工具或统一的合规模板。

在这一框架下，各国通过 JPack 配置并表达自身的法律与监管要求，而非被动接受外部规则。SCEL 的作用，正是在此基础上，为各国提供一种更直接、更高效的方式，用以确认交易是否符合本国所定义的合规标准。

从这个意义上讲，部署 SCEL 并通过 JPack 明确本国适用的法规政策，构成了体系运行的基础前提：即每个参与方都需要以可验证的方式向系统表明：“对我而言，何为合规”。

A6.3

Sovereign Relay Hub: The Public Plane for Global Settlement

主权中继枢纽：全球结算的公共平面

The Sovereign Relay Hub (SRH) is a public settlement and verification plane authorized by a multilateral constitutional framework described in these Principia, and operated with technical neutrality (see A4.1 and A4.2 for detailed governance principles). Based on this positioning, its core functions and design principles are defined as follows:

Global settlement ordering and finality confirmation:

- **Ordering and batching**: Uniformly ordering and batching cross-border transaction requests submitted by SCELs, and forming immutable final settlement records through a consensus mechanism.

主权中继枢纽 (SRH) 是由多边宪章授权、以技术中立运行的公共结算与验证平面（其治理原则详见 A4.1、A4.2）。基于上述定位，其核心职能与设计原则如下：

全球结算的排序与终局确认：

- **排序与打包**：对各 SCEL 提交的跨境交易请求进行统一排序与打包，并通过共识机制形成不可篡改的最终结算记录。

- **Finality confirmation**: Providing a globally recognized final settlement confirmation for each transaction that is accompanied by valid compliance proofs.

Standardized verification of compliance proofs:

- **Proof submission**: Every cross-border transaction must be accompanied by a compliance proof generated by the originating jurisdiction.
- **Standardized validation**: The relay hub (SRH) validates compliance proofs against a jointly agreed baseline validation rule package (JPack), confirming format validity, correct versioning, and proof-chain completeness.
- **Dual confirmation**: Final settlement is confirmed only when both conditions , "transaction validity" and "compliance proof validity" , are simultaneously satisfied.

Design principle: Strict functional and institutional separation via a dual-track model:

- **Framework layer**: The founding institutional framework constrains the SRH, prohibiting any unilateral operations based on country-specific, entity-specific, or discretionary lists, sanctions, or restrictions, thereby ensuring its neutrality as shared public infrastructure.
- **Operational layer**: Focused exclusively on maintaining the technical neutrality and continuous availability of underlying protocols, codebases, and standards.

Under this design, the hub's position is unambiguous: it does not assess the content of national rules; it verifies compliance solely by applying common standards to proofs of rule execution. In essence, it functions as a "**public processing core for global settlement and compliance proofs**".

- **It does not formulate rules**, but requires that all rules participating in global settlement be translated into verifiable proofs.
- **It does not interfere with sovereign discretion**, but requires that all decisions producing cross-domain effects leave auditable and traceable proof anchors at this layer.

Through this mechanism, coordination and mutual trust in global settlement are achieved under the condition of full respect for sovereign authority and institutional autonomy.

A6.3.1 Inputs and Outputs of the Relay Hub

From an engineering implementation perspective, the core function of the SRH is to efficiently and reliably process two categories

- **终局确认**：为每一笔附带有效合规证明的交易，提供所有参与方共同认可的最终结算确认。

合规证明的标准化验证：

- **证明接收**：每一笔跨境交易必须附带由交易发起国所生成的合规证明。
- **标准化验证**：主权中继枢纽根据各国共同约定的基本法规要件集（JPack），对合规证明进行标准化校验，确认其格式有效、版本正确且证明链完整。
- **双重确认**：只有当"交易有效"与"合规证明有效"两个条件同时满足时，枢纽才会最终确认该笔结算完成。

设计原则：严格的职能与制度层面的隔离，遵循"宪章层 + 运营层"双轨模式。

- **宪章层**：通过元宪章，从制度上约束主权中继枢纽，禁止其执行任何基于国别或政治名单的单边操作，确保其作为公共基础设施的非政治性。
- **运营层**：专注于维持底层协议、代码与标准的技术中立性与持续可用性。

在此设计下，主权中继枢纽的立场非常清晰：它不判断各国规则的内容，只依据共同标准验证规则执行的证明是否合规。其本质是一个"**全球结算与合规证明的公共处理核心**"：

- **它不制定规则**，但要求所有参与全球结算的规则，必须转化为可验证的证明。
- **它不干预主权内部裁量**，但要求所有产生跨域影响的决策在此留下可审计、可追溯的证明锚点。

通过这种机制，在充分尊重主权权威与制度自治的前提下，实现了全球结算的协同与互信。

A6.3.1 主权中继枢纽的输入与输出

of critical inputs: transaction events and compliance proofs. Its operational workflow is explicitly divided into two parts: "inputs" and "outputs".

(1) Inputs: What Does the Hub Receive?

- **Standardized cross-border transaction requests**: Business requests submitted by national SCELs, such as cross-border payment instructions or securities settlement orders. Each request must be accompanied by a compliance proof autonomously generated and digitally signed by the originating jurisdiction, and must specify the applicable rule version identifier.
- **Standardized transformation of legacy messages**: Through the deployment of local SCEL adaptation gateways within each sovereign domain, the architecture parses, transforms, and semantically aligns business messages originating from traditional financial infrastructures (such as SWIFT, RTGS, and CSD systems), and generates unified and verifiable interaction results.

The SRH itself does not communicate directly with external infrastructures, nor does it perform message transformation or business interpretation. Its core responsibility is limited to **validating, ordering, and finalizing the state changes, compliance proofs (PoPC), and interaction results** submitted by SCELs. This design ensures that, in cross-sovereign collaboration, all participants can reach consensus on the fact of "how SCELs interact with external systems", and that the corresponding records can be independently reviewed and audited.

- **Governance and configuration update instructions**: Including updates to jurisdictional rule packages (JPack), adjustments to compliance proof mutual-recognition rules, node admission or exit instructions, and dynamic updates to consensus parameters and risk thresholds.

(2) Outputs: What Does the Hub Provide?

All "outputs" described in this section are derived from interaction and compliance processing already completed by the SCELs. The SRH itself does not directly connect to or process messages from traditional financial infrastructures; its responsibilities are strictly limited to validating, ordering, and confirming the state changes and compliance proofs submitted by SCELs.

- **Settlement confirmations for Sovereign Compliance & Execution Layers**: The consensus-confirmed sequence of cross-domain events, including a global order and uniform timestamps, is broadcast to the relevant sovereign

从工程实现角度看，主权中继枢纽的核心功能是高效、可信地处理两类关键输入：交易事件与合规证明。其工作流程明确划分为"输入"和"输出"两部分：

(1) 输入：枢纽接收什么?

- **标准化的跨境交易请求**：来自各国主权合规执行层的业务请求，例如跨境支付或证券结算指令。每笔请求必须附带由该国自主生成并数字签名的合规证明，并注明所依据的规则版本号。
- **传统报文的标准化转换**：架构通过在各个主权域内部署 SCEL 本地适配网关，对来自传统金融基础设施（如 SWIFT、RTGS、CSD）的业务报文进行解析、转换与语义对齐，并生成统一的、可验证的交互结果。

中继链本身不直接与外部基础设施通信，也不承担报文转换或业务理解功能。其核心职责是对 SCEL 提交的**状态变更、合规证明（PoPC）及交互结果进行验证、排序与最终性确认**。这一设计确保了在跨主权协作中，所有参与方对"SCEL 如何与外部系统交互"这一事实能够达成一致，且相关记录可被独立复核与审计。

- **治理与配置更新指令**：包括管辖规则包（JPack）的更新、合规证明互认规则的调整、节点准入或退出指令，以及共识参数与风险阈值的动态更新。

(2) 输出：枢纽提供什么?

本节所述"输出"均基于主权合规执行层 已完成的对外交互与合规处理结果。主权中继枢纽本身不直接连接或处理来自传统金融基础设施的报文，其职责仅限于对 SCEL 提交的状态变更与合规证明进行验证、排序与确认。

- **面向主权合规执行层的结算确认**：向相

compliance enforcement layers, along with verification results confirming the completeness and validity of compliance proof. Countries can use this confirmation as a reference signal for cross-domain consistency and reconciliation, completing the corresponding accounting processes in their local core systems without altering existing permissions and procedures.

- **Event summaries and proof anchors for the audit and observation layer**: Providing authorized audit and observation entities with privacy-preserving information, such as event hashes, Merkle tree roots, and statistical patterns of compliance proofs. Subject to data sovereignty and privacy protection requirements, this enables independent replay and verification of specific transaction paths.
- **State metrics and alerts for governance and operations**: Real-time outputs of network performance metrics, node behavior analysis, cross-jurisdictional rule conflict warnings, and anomalous pattern reports. These data support multilateral governance bodies in rule adjustment, protocol upgrades, risk management, and operational optimization.

Through the above concise and clearly defined interface design, the relay hub achieves technical minimalism and a high degree of specialization. Its core value lies in securely and credibly interconnecting dispersed and heterogeneous national financial systems into a collaborative network that, at the global level, exhibits global consistency, proof verifiability, operational observability, and replayability.

A6.3.2 Negative Commitments of the Relay Hub (Negative Commitments)

To ensure that the principle of technical neutrality is clear, credible, and actionable, the SRH strictly adheres to the "Three Prohibitions" established in A4.2.2 No Interpretation, No Execution, and No Ownership. Building upon this, the Hub explicitly commits to a "Negative List": it shall not hold any currency or accounts, shall not issue any form of "currency", shall not enforce unilateral political sanctions, shall not pass value judgments on the sovereign rules of any nation, and shall operate as a parallel collaborative layer rather than a replacement for existing systems.

A6.3.3 Failure and Sovereign Relay Hub (Failure, Degradation & Sovereign Continuity)

关的 SCEL 广播经过共识确认的跨域事件序列，其中包含全局排序与统一时间标记，并附带对合规证明完整性与有效性的验证结果。各国可将该确认结果作为跨域一致性与对账参考信号，在不改变既有权限与流程的前提下，于本地核心系统中完成相应的账务处理。

- **面向审计与观察层的事件摘要与证明锚点**：为获得授权的审计与观察主体提供脱敏信息，如事件哈希、默克尔树根、合规证明的统计模式等。在满足数据主权与隐私保护要求的前提下，支持对特定交易链路进行独立重放与验证。
- **面向治理与运维的状态指标与告警**：实时输出网络性能指标、节点行为分析、跨辖区规则冲突预警及异常模式报告。这些数据为多边治理委员会调整规则、升级协议、处置风险及优化运营提供决策支持。

通过以上简洁、定义清晰的接口设计，中继枢纽在技术上实现了最小化与高度专注。其核心价值在于，将分散且异构的各国金融系统，安全、可信地连接成一个在全球层面具备全局一致性、证明可验证性及运营可观测、可重放特性的协同网络。

A6.3.2 主权中继枢纽的负面清单

为确保技术中立原则清晰、可信且可操作，主权中继枢纽严格遵循 A4.2.2 所确立的三大禁令：禁止解释、禁止执行、禁止所有。在此基础上，枢纽还明确承诺：不持有任何货币或账户，不发行任何形式的“货币”，不执行单边政治制裁，不对各国主权规则进行价值判断，并行协作而非替代既有系统。

For globally critical infrastructure, designing how to survive and recover from failures is as important as designing how to operate under normal conditions. To ensure ultimate system resilience, the architecture of the SRH must satisfy the following three core requirements:

1) **Failure isolation: ensuring the continued operation of domestic and institutional systems**:
in the event of a failure in the operation of a relay hub, a fundamental principle must be upheld: only global cross-border settlement is suspended, while domestic financial systems in each jurisdiction remain unaffected. Local payment systems, central securities depositories, and their upper-layer Sovereign Compliance & Execution Layers must be able to operate independently and continuously, maintaining domestic payment, clearing, institutional regulations and compliance-proof generation capabilities. This ensures that any global technical failure does not disrupt a country's basic economic order.

2) **Ex post reconciliation: ensuring emergency transactions are traceable and bookable**:
During a failure, if necessary cross-border transactions are completed between jurisdictions through emergency bilateral channels, the system must provide a clear path for ex post reconciliation. Once the relay hub is restored, these emergency transactions can be securely "backfilled" into the global ledger on the basis of the standardized compliance proofs generated at the time, together with any supplementary attestations. This mechanism both recognizes the legal validity of emergency operations and ensures that a complete and consistent global transaction view can ultimately be reconstructed, such that no lawful transaction is lost or rendered irreconcilable due to failure.

3) **Substitutability: SRH itself can be safely replaced**:
In extreme circumstances, if the existing SRH becomes fundamentally inoperative due to technical or governance failure, contingency procedures may be triggered pursuant to decisions at the multilateral institutional framework layer to replace or rebuild a new hub instance. Provided that the new hub adheres to the same core protocols and is able to read all historically preserved compliance proofs and transaction hashes, it can, through replay mechanisms, restore a global state that is fully consistent with the prior state. This design fundamentally eliminates the possibility of any single technical facility becoming an irreplaceable single point of failure.

A6.3.3 故障应对与主权连续性

对于全球关键基础设施而言，设计“如何在故障中生存并恢复”与设计“如何正常运行”同等重要。为确保系统的终极韧性，主权中继枢纽的架构必须满足以下三项核心要求：

1) **故障隔离：保障境内系统持续运行**。
当中继枢纽发生故障时，必须确保一个基本原则，仅全球跨境结算暂停，各国国内金融系统不受影响。 各国本地的支付系统、证券存管系统及其上层的主权合规执行层必须能够独立、持续地运转，维持境内支付、清算与合规证明的生成能力。这确保了任何全球性技术故障都不会中断一国的基本经济秩序。

2) **事后调和：确保应急交易可追溯、可入账**。
故障期间，若国家间通过应急双边渠道完成了必要的跨境交易，系统必须提供清晰的“事后调和”路径。 待中继枢纽恢复后，这些应急交易可以凭其当时生成的标准化合规证明及其他补充凭证，被安全地“补录”到全球账本中。这一机制既认可了应急操作的法律效力，又能在最终重建一个完整、一致的全球交易视图，确保没有一笔合法交易因故障而丢失或无法对账。

3) **可替代性：中继枢纽本身可被安全替换**。
在极端情况下，若现有主权中继枢纽在技术或治理上彻底失效，应能依据多边宪章层的决策，启动预案，替换或重建一套新的枢纽实例。只要新的枢纽遵循相同的核心协议，并能读取历史留存的所有合规证明与交易哈希，即可通过重放机制，恢复出与之前完全一致的、可信的全局状态。这从根源上杜绝了单一技术设施成为不可替代的单点故障。

In summary, **the SRH is positioned as a "critical but non-fatal" public infrastructure**:

- Its core value lies in significantly enhancing the efficiency and transparency of cross-sovereign settlement.
- Its resilience guarantee is reflected in the fact that, in the event of failure, sovereign entities retain full control over their domestic and institutional systems and their verifiable proof chains.
- Its ultimate reliability derives from pre-defined fault-tolerance and recovery mechanisms through which the system can always return to a unique and trustworthy global state.

This design ensures that, under the principle of sovereign continuity established in Chapter A2, the overall architecture becomes a truly resilient global public good - one that delivers substantial coordination value without tying the vital interests of participating jurisdictions to any single external entity. The specific engineering details of the design are provided in Volume B of this document.

综上所述，**主权中继枢纽被定位为一个"关键但非致命"的公共基础设施**：

- 其核心价值在于显著提升跨主权结算的效率和透明度。
- 其韧性保障体现在故障时，各主权体仍保有本地系统的完整控制权与可验证证明链。
- 其终极可靠性源于通过预设的容错与恢复机制，系统总能恢复到一个唯一、可信的全局状态。

这一设计，使得整个架构在 A2 章确立的主权连续性原则下，成为一个既提供巨大协同价值，又不将各国命脉系于单一外部实体的、真正具备韧性的全球公共产品。设计的具体工程内容，在本文卷 B 提供。

A6.4

Compliance Proof Flow Across Layers (PoPC Flow Across Layers)

分层架构中的合规证明流转

Within the layered architecture, compliance proofs constitute the critical bridge linking local rule execution with global settlement finality. They transform internal compliance reviews conducted within a single jurisdiction into standardized proofs that are verifiable by all participating parties. For a typical cross-border settlement (the full lifecycle is specified in A5.3), the flow of compliance proofs follows five clearly defined stages:

在该分层架构中，合规证明是连接本地规则执行与全球结算终局性的核心桥梁。它将单一司法管辖区内部的合规审查转化为全网参与方均可验证的标准证明。对于典型的跨境结算流程（完整生命周期详见 A5.3），合规证明的流转分为以下五个明确阶段：

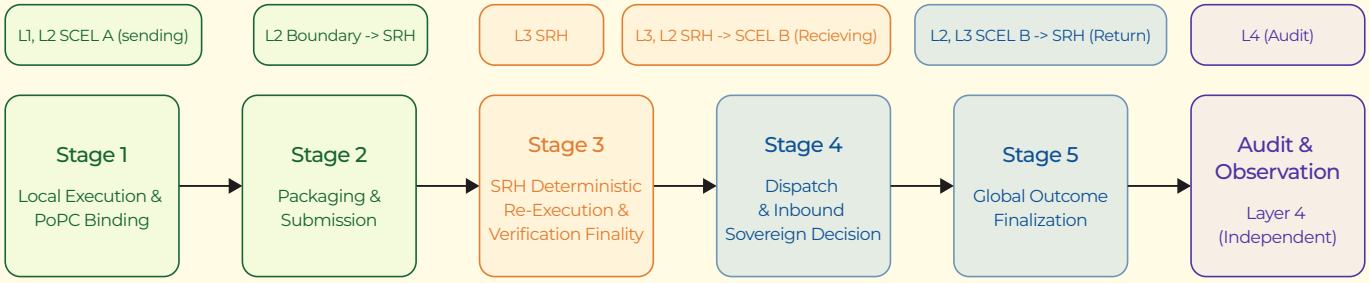


Figure 8: Cross-Layer Compliance Proof Flow (PoPC Flow) / 图8：跨层合规证明流程（PoPC 流程）

Stage One: Local Execution and Proof Generation (SCEL Execution & PoPC Binding). Within the local SCEL:

- A participating institution initiates a cross-border transaction request.
- The Regulatory VM performs automated evaluation of the request against the SCEL's active Jurisdiction Pack (JPack), deterministically producing one of three outcomes: ALLOW, HOLD, or REJECT.
- Upon an ALLOW decision, the system generates a cryptographically bound PoPC - linking the policy snapshot hash, normalized inputs, decision trace, reason codes, and a digital signature - and records it together with the transaction data on the local ledger, establishing a traceable compliance origin.
- If the decision is REJECT, the transaction is aborted locally and no cross-domain submission occurs; if HOLD, it is suspended pending resolution.
- For messages originating from legacy systems (such as SWIFT), this stage converts the embedded business intent and compliance status into the standardized compliance proof format in accordance with predefined rules.

Stage Two: Cross-Domain Message Packaging and Submission.

- The Sovereign Boundary Interface of the originating SCEL packages the transaction intent, the PoPC, and the referenced policy version information into a standardized Transfer Package.
- The Transfer Package is submitted to the SRH.
- The package enters the SRH's Sequencing Pipeline as a candidate event pending canonical ordering and validation.

Stage Three: SRH Deterministic Re-Execution and Verification Finality.

阶段一：本地执行与证明生成（SCEL 执行与 PoPC 绑定），在本地 SCEL 环境内：

- 参与机构发起跨境交易请求。
- 监管虚拟机依据该 SCEL 当前挂载的 JPack 对请求进行自动化评估，并确定性地产生三种结果之一：允许、挂起或拒绝。
- 若评估结果为允许，系统将生成一份加密绑定的 PoPC，该证明关联了政策快照哈希、规范化输入、决策轨迹、原因代码及数字签名，并与交易数据一同记录在本地账本上，建立可追溯的合规源头。
- 若结果为拒绝，交易将在本地终止，不会进行跨域流程；若为挂起，则交易暂停，等待后续处置。
- 对于来自传统系统（如 SWIFT）的报文，此阶段将根据预设规则，将其蕴含的业务意图和合规状态转换为标准化的合规证明格式。

阶段二：跨域消息封装与提交

- 发起方 SCEL 的主权边界接口将交易意图、PoPC 以及引用的政策版本信息封装为标准化的传输包。
- 传输包被提交至 SRH。
- 该包进入 SRH 的排序流水线，作为待处理事件等待规范排序与验证。

Upon receipt of the Transfer Package, the SRH performs independent verification - not by conducting supplementary compliance checks, but by deterministically re-executing the exact same policy logic:

- The SRH loads the JPack version pinned by the PoPC's policy snapshot hash and re-executes the policy evaluation.
- The re-execution result must be byte-identical to the originating SCEL's result ("mirror verification").
- Once the BFT consensus mechanism confirms the verification, the SRH anchors a verification-final event (VERIFIED / DISPATCHABLE) and archives the PoPC in the immutable compliance record.
- This stage yields verification finality - confirmation that the sending jurisdiction's compliance claim is truthful and reproducible, but does not yet constitute settlement finality.

Stage Four: Cross-Domain Dispatch and Inbound Sovereign Decision.

- The SRH forwards the Verified Transfer Package to the destination SCEL.
- The destination SCEL independently evaluates inbound compliance under its own Jurisdiction Pack (JPack-B).
- The destination SCEL makes the final ACCEPT or REJECT decision - this is the core sovereignty guarantee of the architecture.
- Settlement is executed only upon acceptance: the receiving SCEL transfers assets to the recipient and completes the corresponding asset registration and accounting entries within domestic core systems (RTGS, CSD) in accordance with national financial rules.

Stage Five: Global Outcome Finalization.

- Upon settlement (or rejection), the destination SCEL emits a signed Settlement Receipt to the SRH.
- The SRH verifies the receipt's authenticity and ordering, then commits the terminal outcome - SETTLED, REJECTED, or EXPIRED - to the Global State Tree, linking it to the prior verification record and PoPC identifier.
- The SRH optionally notifies the originating SCEL and any registered audit subscribers.
- Domestic auditors in both jurisdictions may, through the global event hash and the PoPC proof summary, fully trace

阶段三：SRH 确定性重执行与验证终局性

SRH 在收到传输包后进行独立验证。其方式并非重新开展合规检查，而是确定性地重执行完全相同的政策逻辑：

- SRH 加载由 PoPC 政策快照哈希锁定的 JPack 版本，并重新运行政策评估。
- 重执行的结果必须与发起方 SCEL 的结果在字节层面完全一致（即“镜像验证”）。
- 一旦 BFT 共识机制确认验证通过，SRH 将锚定一个验证终局事件（已验证 / 待分发），并将 PoPC 归档至不可篡改的合规记录中。
- 此阶段达成的是验证终局性，即确认发送方管辖区的合规声明真实且可复现，但这尚未构成结算终局性。

阶段四：跨域分发与入境主权决策

- SRH 将已验证传输包转发至接收方 SCEL。
- 接收方 SCEL 根据其自身的辖区规则包（JPack-B）独立评估入境合规性。
- 接收方 SCEL 做出最终的接受或拒绝决策，这是该架构对主权保障的核心体现。
- 结算仅在接受后执行：接收方 SCEL 向收款人转移资产，并根据本国金融规则，在 RTGS、CSD 等国内核心系统中完成相应的资产登记和会计分录。

阶段五：全局结果确认

- 结算（或拒绝）完成后，接收方 SCEL 向 SRH 发送一份签名的结算收据。
- SRH 验证收据的真实性与顺序，随后将最终结果（已结算、已拒绝或已过

the transaction's compliance path and settlement status - including independent replay via the Audit & Observation Layer (Layer 4) without access to raw business data.

- When using legacy systems, separate synchronization of ledgers between these systems will be required, as their registries must be updated separately.

Through the above process, this framework assigns a dual meaning to "settlement completion":

- **At the funds layer**, it signifies that the transaction has been irreversibly completed on the ledger, with the receiving jurisdiction having exercised its sovereign authority to accept the settlement.
- **At the compliance layer**, it signifies that the transaction was executed in accordance with the rules in force across the relevant jurisdictions at the time, and that the entire process has left a complete proof chain available for independent verification.

This implies that every completed cross-border settlement represents not only the final transfer of value, but also an auditable and verifiable execution of compliance.

期）提交至全球状态树，并将其与此前的验证记录和 PoPC 标识符关联。

- SRH 可选地通知发起方 SCEL 及任何已注册的审计订阅者。
- 两地管辖区的国内审计师均可通过全球事件哈希和 PoPC 证明摘要，完整追溯交易的合规路径和结算状态，包括通过，审计与观察层（Layer 4），进行独立回放，且无需接触原始业务数据。
- 在使用传统系统时，由于其登记簿需独立更新，因此需要与这些系统进行额外的账本同步。

至此，一笔跨境结算的完成即实现了 A4.8.1 所定义的双重终局性（账本终局与政策终局的双重锚定）。

A6.5

Domain Model and Allocation of Responsibilities

域模型与职责分工

In addition to the layered architecture, this chapter introduces a domain model as an auxiliary conceptual framework for system analysis and multilateral collaboration. This model does not mandate specific operational workflows; rather, by explicitly defining the actors, core responsibilities, and key interests of different professional domains, it delineates clear boundaries of collaboration and interaction interfaces for all parties. From a practical business perspective, the following six core business domains can be identified:

在分层架构之外，本章引入域模型作为辅助系统分析与多边协作的概念框架。该模型不强制规定具体操作流程，而是通过明确定义不同专业领域的行为主体、核心职责与关键利益关切，为各方划定清晰的协作边界与交互接口。基于实际业务视角，可识别以下六个核心业务域：

1） 货币与发行域

1) Monetary & Issuance Domain

- **Representative entities**: Central banks, treasury authorities, and their authorized institutions.
- **Core functions**: The issuance and redemption of sovereign currency, and the determination and maintenance of the ultimate settlement anchors of clearing systems.
- **Layered mapping**:
  - ◇ **Domestic and Local Core Systems Layer**: Operating RTGS, treasury, and other core monetary management systems.
  - ◇ **SCEL**: Deploying issuance and redemption logic to enhance the programmability and transparency of monetary policy.
  - ◇ **SRH**: By forging structured cross-domain event sequences at the protocol layer, the architecture enables sovereign jurisdictions to construct macro-level perspectives within the scope of their respective authorities.

2) Deposit & Payments Domain

- **Representative entities**: Commercial banks, payment institutions, and industry clearing organizations.
- **Core functions**: Retail and wholesale payment services, inter-institutional fund settlement, and account management.
- **Layered mapping**:
  - ◇ **Domestic and Local Core Systems Layer**: Maintaining traditional account systems and payment channels.
  - ◇ **SRH**: Migrating selected clearing processes (such as DvP/PvP) on-chain and leveraging programmable rules to enable automated compliance determination.

Core interests: Access to trusted and efficient cross-sovereign settlement channels via the relay hub, as well as standardized compliance proof anchors usable for both internal and external audit purposes.

3) Markets & Tokenised Assets Domain

- **Representative entities**: Securities exchanges, central securities depositories, custodians, registrars, and clearing and settlement institutions.
- **Core functions**: The registration, custody, trading, and settlement of securities and other financial assets, with particular emphasis on full lifecycle management of tokenised assets.

- **代表主体**：央行、财政部门及其授权机构。
- **核心职能**：主权货币的发行、赎回以及清算体系最终结算锚定的确定与维护。
- **分层映射**：
  - ◇ **本地主权系统层**：运营 RTGS、国库等核心货币管理系统。
  - ◇ **主权合规执行层**：可部署发行与赎回逻辑，提升货币政策的可编程性与透明度。
  - ◇ **主权中继枢纽**：在协议层形成结构化的跨域事件序列，使各主权可在自身权限内构建宏观视图。

2) 存款与支付域

- **代表主体**：商业银行、支付机构、行业清算组织。
- **核心职能**：零售与批发支付服务、跨机构资金结算、账户管理。
- **分层映射**：
  - ◇ **本地主权系统层**：维护传统账户体系与支付渠道。
  - ◇ **主权合规执行层**：可将部分清算流程（如 DvP/PvP）迁移至链上，并利用可编程规则实现自动化合规判断。

核心诉求：从主权中继枢纽获得可信、高效的跨主权结算通道，以及可用于内外部审计的标准化合规证明锚点。

3) 市场与资产域

- **代表主体**：证券交易所、中央证券存管机构、托管行、登记结算机构等。
- **核心职能**：证券及其他金融资产的登记、托管、交易与结算，特别是代币化资产的全生命周期管理。

- **Layered mapping**:
  - ◇ **SCEL**: Reconstructing processes such as “positions–collateral–settlement” into programmable state machines, and generating fine-grained compliance proofs for complex financial products.
  - ◇ **SRH**: Providing a trusted technical foundation for true cross-market settlement finality through cross-sovereign compliance proof mutual-recognition mechanisms.

4) Compliance & Supervision Domain

- **Representative entities**: Financial regulatory authorities, financial intelligence units, tax authorities, and prudential supervisors.
- **Core functions**: Rule-making, oversight of execution, and proof retrieval, ensuring that system operations comply with domestic and international legal and regulatory requirements.
- **Layered mapping**:
  - ◇ **SCEL**: Deeply integrating domestic and institutional compliance regimes with on-chain infrastructure by configuring programmable rules and defining the generation and reporting logic of compliance proofs.

Core interests: The ability to verify the validity of cross-sovereign transaction compliance proofs without penetrating granular business details, and to support prudential analysis of specific risk patterns (such as suspicious fund flows).

5) Technology & Operations Domain

- **Representative entities**: Infrastructure operators, cloud service and hardware providers, development and operations teams, and open-source technology communities.
- **Core functions**: Ensuring the secure, stable, and high-performance operation of infrastructure across all layers, and maintaining public verifiability of system parameters and software versions.
- **Layered mapping**:
  - ◇ Responsible for the engineering implementation, day-to-day operations, and continuous optimization of the SCELs and the SRH.
  - ◇ At the governance level, participating in technical decision-making related to relay network operations, without intervening in any sovereign policy or business rule formulation.

- **分层映射**：
  - ◇ **主权合规执行层**：将“持仓 - 抵押 - 结算”等流程重构为可编程状态机，为复杂金融产品生成细粒度合规证明。
  - ◇ **主权中继枢纽**：通过跨主权合规证明互认机制，为真正意义上的跨市场结算终局性提供可信的技术基础。

4）合规与监管域

- **代表主体**：金融监管机构、金融情报中心、税务机关、审慎监管部门等。
- **核心职能**：规则制定、监督执行与证明调取，确保系统运行符合本国及国际法律与监管要求。
- **分层映射**：
  - ◇ **主权合规执行层**：通过配置可编程规则、定义合规证明的生成与上报规则，将本国合规体系与链上基础设施深度融合。

核心诉求：具备在不穿透具体业务细节的前提下，验证跨主权交易合规证明有效性的能力，并支持对特定风险模式（如可疑资金流）进行审慎分析。

5）技术与运维域

- **代表主体**：基础设施运营商、云服务与硬件供应商、开发运维团队、开源技术社区。
- **核心职能**：保障各层基础设施的安全、稳定、高性能运行，确保系统参数与版本的可公开验证性。
- **分层映射**：
  - ◇ 负责主权合规执行层与主权中继枢纽的工程实现、日常运维与持续优化。

6) Audit & Observation Domain

- **Representative entities**: Independent audit firms, credit rating agencies, academic research institutions, and authorized observer nodes.
- **Core functions**: Within the scope of authorization, independently verifying system behavior for compliance and consistency by replaying key business paths, and producing objective assessments.
- **Layered mapping**:
  - ◇ Utilizing publicly available or access-controlled data and proofs to perform recomputation-based verification and sampling inspections.
  - ◇ Providing independent third-party attestation to the Monetary & Issuance Domain and the Compliance & Supervision Domain, and external feedback on system reliability and resilience to the Technology & Operations Domain.
  - ◇ 在治理层面，参与中继网络运营的技术决策，但不介入任何主权政策与业务规则的制定。

6) 审计与观察域

- **代表主体**：独立审计机构、信用评级机构、学术研究机构、授权观察节点。
- **核心职能**：在授权范围内，通过重放关键业务路径，独立验证系统行为的合规性、一致性，并形成客观报告。
- **分层映射**：
  - ◇ 利用各提供的公开或受控数据与证明，进行重算验证与抽样检查。
  - ◇ 为货币与发行域、合监管域提供独立第三方鉴证，为技术与运维域提供系统可靠性与韧性的外部反馈。

Business Domain 业务维度	Domestic & Institutional Core Systems Layer 国内及机构核心系统层	Sovereign Compliance & Execution Layer (SCEL) 主权合规执行层 (SCEL)	Sovereign Relay Hub Layer (SRH) 主权中继枢纽层 (SRH)	Audit & Observation Layer 审计与观察层
Monetary & Issuance Domain **货币与发行域**	RTGS / Treasury systems RTGS / 财政库管系统	Programmable issuance and redemption rules, enhancing transparency in monetary policy execution 可编程发行与赎回规则，提升货币政策执行的透明度	Maintaining a global settlement state tree that enables visibility into cross-sovereign fund flows 维护全球结算状态树，实现跨主权资金流动的可见性	Independent verification that issuance and redemption events comply with published policy packs across jurisdictions 独立验证发行与赎回事件是否符合各辖区发布的政策包
Deposit & Payments Domain **存款与支付域**	Account systems / payment channels; intra-bank and inter-bank settlement 账户系统 / 支付渠道；行内及行间结算	On-chain DvP / PvP execution and automated compliance checks 链上 DvP / PvP 执行及自动化合规检查	Providing cross-sovereign verification routing and immutable compliance proof anchoring 提供跨主权验证路由及不可篡改的合规证明锚定	Replaying payment compliance proofs to independently confirm settlement integrity 通过回放支付合规证明，独立确认结算的完整性
Markets & Assets Domain **市场与资产域**	Reliant on domestic and institutional systems; on-chain migration not mandatory 依赖国内及机构系统；不强制要求链上迁移	Implementing position–collateral–settlement state machines and generating fine-grained compliance proofs for complex products 实现持仓 - 抵押 - 结算状态机，并为复杂产品生成细粒度的合规证明	Enabling cross-market compliance proof mutual recognition and providing cross-market verification finality 实现跨市场合规证明互认，提供跨市场验证终局性	Sampled re-execution of complex product compliance paths using archived PoPC and policy snapshots 利用存档的 PoPC 和政策快照，对复杂产品的合规路径进行抽样重执行

Compliance & Supervision Domain **合规与监管域**	Offline / traditional supervisory processes based on domestic and institutional regulations 基于国内及机构法规的线下 / 传统监管流程	Executing programmable rules (JPack) and generating compliance proofs (PoPC) and reporting artifacts 执行可编程规则 (JPack)，生成合规证明 (PoPC) 及报告产物	Deterministic re-verification of compliance proofs and immutable archiving for supervisory access 对合规证明进行确定性重验证，并为监管准入提供不可篡改的归档	Objective third-party assessment of system-wide compliance neutrality and rule execution consistency 对全系统合规中立性及规则执行一致性进行客观的第三方评估
Technology & Operations Domain **技术与运营域**	Integration and operation of domestic and local systems 国内及本地系统的集成与运维	Engineering implementation and operation of SCEL, ensuring verifiability of versions and parameters SCEL 的工程实现与运营，确保版本与参数的可验证性	Implementation and operation of the relay network, without involvement in policy content 枢纽网络的实现与运维，不介入政策内容	Toolchain maintenance (popc-replay) and verification of version/parameter integrity across layers 维护工具链 (popc-replay)，验证跨层版本与参数的完整性
Audit & Observation Domain **审计与观察域**	Accessing authorized local data for consistency checks 访问授权的本地数据以进行一致性检查	Replaying critical business paths and performing sampled verification of compliance execution 重放关键业务路径，并对合规执行进行抽样验证	Archiving compliance proofs and logs and providing structured access for external audit 归档合规证明与日志，为外部审计提供结构化访问	Providing independent third-party attestation of system trustworthiness, continuity, and regulatory neutrality 提供独立的第三方鉴证，涵盖系统可信度、连续性及监管中立性

Table 16: Mapping of Responsibilities of the Six Domains Across the Layered Architecture / 表 16: 分层架构中六大域职责的映射关系

A6.6

Positioning and Mapping of S-Series Assets within the Layered Architecture

S 系列资产在分层架构中的定位与映射

Sections A6.1 through A6.3 establish the technical layered architecture; Section A6.4 describes the cross-layer flow mechanism of compliance proofs; and Section A6.5 clarifies the responsibility boundaries of participating parties from a functional domain perspective. To construct a complete engineering implementation framework, this section systematically elaborates the specific positioning and mapping relationships of different asset categories, identified by the **S-series labels**, within the above multi-layer architecture.

As set forth in Section A6.1, the **S-series labels (S0/S1/S2/S*)** as

A6.1 至 A6.3 节确立了技术分层架构，A6.4 节阐述了合规证明的跨层流转机制，A6.5 节则从职能领域视角明确了各参与方的职责边界。为构建完整的工程实现框架，本节将系统阐述不同资产类别（以 **S 系列标签**标识）在上述多层架构中的具体定位与映射关系。

如 A6.1 所述，**S 系列标签（S0/S1/S2/S*）**是对主权负债在链上映射后的金融与法律属性的

taxonomic identifiers for the financial and legal attributes of on-chain mapped sovereign liabilities, explicitly defining their issuing entities, clearing layers, allocation of responsibility, and regulatory authority. To achieve comprehensive verifiability of a cross-sovereign settlement system at both the engineering implementation and policy supervision levels, this section establishes a clear mapping between the S-series and the three-layer architecture, addressing the following core questions: where transactions involving different tiers of on-chain assets are executed, where compliance proofs are generated, where finality is obtained, and where independent audit is performed.

A6.6.1 Overall Mapping Framework

The complete lifecycle of S-tier assets within the system can be abstracted as mappings across the following four key stages:

1. **Execution and accounting layer**: where asset transactions are natively executed and ledger records are completed.
2. **Compliance proof layer**: where compliance proof for the transaction is generated and undergoes initial validation.
3. **Finality anchoring layer**: where transaction irreversibility is formally declared.
4. **Audit and verification layer**: where compliance and consistency across the full transaction lifecycle can be independently replayed and verified.

A6.6.2 Mapping of Layer Responsibilities by S-Series

(1) Role of the Sovereign Compliance & Execution Layer (SCEL)

Within SSI, the S-series labels essentially map the intrinsic risk structures, regulatory logic, and clearing attributes of the financial system into their objective representations in the digital domain. The liability characteristics, compliance depth, and privacy requirements of each tier jointly determine the complexity of state machines and the design of proof structures within the SCEL. This differentiation in technical implementation constitutes the inevitable engineering expression of traditional financial rules within a programmable environment.

- For **S0 (retail cash, M0)**, the SCEL typically only needs to enforce lightweight rules such as transaction limits and frequency controls. Owing to its characteristics of instant settlement and absence of counterparty risk, compliance

分类标识，明确了其发行主体、清算层级、责任归属及监管权限。本节将建立 S 系列与三层架构的清晰映射，回答以下核心问题：不同层级的链上资产在何处执行交易、在何处生成合规证明、在何处获得最终性确认，以及在何处接受独立审计。

A6.6.1 总体映射框架

各 S 层级资产在系统中的完整生命周期，可抽象为在以下四个关键环节的映射：

1. **执行与记账层**：资产交易在何处被原生执行并完成账本记录。
2. **合规证明层**：该交易的合规性证明在何处生成并完成初步验证。
3. **终局性锚定层**：交易的不可撤销性在何处被最终宣告。
4. **审计与验证层**：交易全流程的合规性与一致性在何处可被独立重放与验证。

A6.6.2 各层职责映射

(1) 主权合规执行层的角色

在主权可验证结算框架中，S 系列标签本质上映射的是金融制度内在的风险结构、监管逻辑与清算属性在数字空间的客观呈现。各层级的负债性质、合规深度与隐私要求，共同决定了其在主权合规执行层中的状态机复杂度与证明结构设计。这种技术实现的区分，是传统金融规则在可编程环境中必然的工程化表达。

- 对于 **S0（零售现金，M0）**，主权合规执行层通常只需执行限额、频次等轻量规则。由于其即时结算和无对手风险的特性，合规判断重点在验证交易未触及监管门槛，同时生成最小化的合规证明以保护用户隐私。

determination focuses on verifying that transactions do not breach regulatory thresholds, while generating minimal compliance proofs to protect user privacy.

- For **S1 (deposit liabilities, M1)**, the relatively unified global regulatory frameworks render the applicable rules highly structured. The SCEL can execute these rules through standardized processes (such as anti-money laundering checks), generating replayable compliance proofs that primarily demonstrate the compliance of transaction participants and fund flows.
- For **S2 (broad credit and market assets, M2+)**, compliance assessment becomes significantly more complex, involving multi-stage events such as issuance, trading, collateralization, and redemption. The compliance proofs generated by the SCEL must be capable of continuously reflecting the evolution of asset states, ensuring that cross-market state consistency remains verifiable.
- For **S* (wholesale central bank money, wCBDC)**, operations are directly linked to monetary policy and financial stability and therefore exhibit extremely high policy sensitivity. The SCELmust ensure absolute precision in rule execution and generate compliance proof chains that are complete, auditable, and non-repudiable, thereby achieving the highest level of trustworthiness in cross-sovereign environments.

To this end, the compliance proofs generated by the SCEL for each tier contain a set of structured elements that together constitute the technical and institutional anchors for cross-sovereign mutual recognition:

- **Rule version**: explicitly identifies the policy rule version applied during execution, ensuring that all verifiers can reproduce the decision process within the same policy context.
- **Rule hash**: a cryptographic hash of the rule set content, ensuring the post hoc immutability of rule configurations.
- **Verification auxiliary data**: carries the minimal data required to recompute compliance conclusions, supporting independent third-party verification while preserving the privacy of business details.
- **Decision outcome**: explicitly records the final determination of the compliance engine (ALLOW or REJECT), representing the deterministic outcome of rule execution for a given input and serving as the definitive policy execution artifact.

- 对于 **S1（存款负债，M1）**，全球相对统一的监管框架使其规则高度结构化。主权合规执行层能够以标准化流程执行这些规则（如反洗钱检查），生成可重放的合规证明，重点在于证明交易参与方及资金路径的合规性。
- 对于 **S2（广义信用与市场资产，M2+）**，合规判断的复杂度显著上升涉及发行、交易、抵押、兑付等多阶段事件。主权合规执行层生成的合规证明必须能够连续反映资产状态的演进，确保跨市场状态的一致性可被验证。
- 对于 ***S**（批发央行货币，wCBDC）**，其操作直接关联货币政策与金融稳定，具有极高的政策敏感性。主权合规执行层必须确保规则执行的绝对精确，并生成具备完备性、可审计性与不可抵赖性的合规证明链，使其在跨主权环境中具备最高等级的可信度。

为此，主权合规执行层为每个层级生成的合规证明均包含一系列结构化要素，共同构成跨主权互认的技术与制度锚点：

- **规则版本**：明确标识执行所依据的策略规则版本，确保所有验证方能在同一政策语境下复现判断过程。
- **规则哈希**：对规则集内容生成密码学哈希值，以此保证规则配置的事后不可篡改性。
- **验证辅助信息**：承载为复算合规结论所必需的最少数据，在保护业务细节隐私的前提，为独立第三方验证提供支持。
- **决策结果**：明确记录合规引擎的最终判定（ALLOW 或 REJECT），这是规则在特定输入下执行的确定性结论，构成最终的政策执行凭据。

- **S-series label**: indicates the financial liability tier involved in the transaction, enabling verifiers to interpret the compliance proof using the correct clearing semantics.
- **Timestamp and digital signature**: jointly ensure the temporal ordering of events, attribution of responsibility, and non-repudiation of actions, providing a unified and trusted temporal and identity foundation for cross-institution audit and cross-sovereign recomputation.

(2) Validation Logic of the Sovereign Relay Hub

The core function of the hub layer is not to directly "execute" financial rules, but to focus on two specific tasks: **verifying the compliance proofs submitted by participating jurisdictions, and providing global final ordering and confirmation for cross-sovereign settlement events**. In this process, there exist systematic differences in validation logic and processing intensity across compliance proofs corresponding to different S-series asset tiers.

- **S0 (retail cash)**: Typically adopts a "**summary verification**" mode. The hub does not penetrate granular transaction details; it verifies only the validity of the transaction hash summary and digital signature submitted by the originating jurisdiction. This approach ensures baseline consistency while maximizing privacy protection.
- **S1 (deposit-type liabilities)**: Adopts a "**full replay**" verification mode. Validation nodes within the hub can independently and completely re-execute the compliance logic based on standardized rule versions, recompute the compliance outcome, and confirm its correctness. This provides a solid technical foundation for cross-jurisdictional mutual recognition of account-based transactions.
- **S2 (structured assets)**: Adopts a "**collaborative verification**" mode. For complex assets, the hub acts as a coordinator, requiring transaction-related parties to provide corresponding state proofs. The hub's core responsibility is to complete the final ordering and confirmation of events based on the verifiable proof provided by multiple parties, while fine-grained state consistency is ensured by the relevant business domains through bilateral or multilateral coordination mechanisms.
- **S* (wholesale settlement assets)**: Must achieve "**strong finality**" at the hub layer. The hub is required not only to verify compliance proofs, but also to incorporate such settlement events into the global consensus ordering and record them on the immutable relay ledger, thereby granting

- **S 系列标签**：标明该业务所涉及的金融负债层级，使验证者能够依据正确的清算语义解读该合规证明。
- **时间戳与数字签章**：共同确保事件发生的先后顺序、责任主体来源以及操作的不可抵赖性，为跨机构审计与跨主权复算提供统一、可信的时间基准与身份认证基础。

(2) 主权中继枢纽的验证逻辑

枢纽层的核心职能并非直接"执行"金融规则而是聚焦于两件事：**验证各国提交的合规证明，并为跨主权结算事件提供全局性的最终性排序与确认**。在此过程中，不对同 S 层级资产所对应的合规证明，其验证逻辑与处理强度存在系统性差异。

- **S0（零售现金）**：通常采用"**摘要验证**"模式。枢纽不穿透具体交易细节，仅验证由来源国提交的交易哈希摘要与数字签章是否合法有效。在确保基本一致性的同时，最大限度保护隐私。
- **S1（存款类负债）**：采用"**完整重放**"验证模式。枢纽内的验证节点可依据标准化的规则版本，独立、完整地重新执行合规逻辑，复算并确认合规结果。为账户类业务的跨国互认提供坚实技术基础。
- **S2（结构化资产）**：采用"**协作验证**"模式。对于复杂资产，枢纽作为协调者，要求交易相关方提供对等的状态证明。枢纽的核心职责是基于多方提供的可验证证明，完成事件的最终排序与确认，而细粒度的状态一致性由相关业务域通过双边或多边协作机制确保。
- **S*（批发结算资产）**：必须在枢纽层达

them the highest level of final and authoritative effect in cross-sovereign environments.

Reaffirmation of critical boundaries: The hub is consistently positioned as a "verifier of compliance proofs" and a "provider of cross-domain finality", rather than an executor of national financial activities or a rule-making authority. This clear technical and governance boundary constitutes the fundamental guarantee of system neutrality, scalability, and sovereign autonomy.

A6.6.3 Asset Identification within Compliance Proofs (S-Series Inside PoPC)

As detailed in Section A5.7, each PoPC incorporates a suite of core fields. To ensure predictability and verifiability in cross-sovereign transactions, this framework embeds a standardized metadata structure within each compliance proof, enabling precise five-dimensional binding across **asset class, clearing tier, issuing entity, policy domain, and business scenario**. Each compliance proof must include the following core metadata fields:

- **s_series (asset tier)**: Identifies the compliance tier of the underlying asset (S0/S1/S2/S*), explicitly defining its monetary attributes, risk characteristics, and applicable statistical classification (e.g., M0, M1).
- **clearing_tier (clearing tier)**: Specifies the clearing layer applicable to the transaction (such as retail, general wholesale, or final settlement), corresponding to different timeliness, finality requirements, and clearing networks.
- **issuer_type (issuer type)**: Denotes the category of the liability issuer (e.g., central bank, commercial bank, or designated financial institution), linking the asset to its credit basis, regulatory jurisdiction, and repayment responsibility framework.
- **policy_domain (policy domain)**: Indicates the primary compliance domains governing the transaction (such as AML/CTF, prudential regulation, securities regulation, or cross-border data controls).
- **business_scenario (business scenario)**: Defines the specific transaction type (such as retail payments, trade finance, DvP settlement, or cross-border remittance), serving to bind the applicable rule sets and validation logic for that scenario.

Through this design, the workload of the SRH in validating cross-domain transactions is significantly simplified and

成"**强最终性**"。枢纽不仅需要验证合规证明，更必须将此类结算事件纳入全局共识排序，并记录于不可篡改的枢纽账本之中，使其获得跨主权环境下最高置信度的终局效力。

关键边界重申：枢纽的定位始终是"合规证明的验证者"与"跨域终局性的提供者"，而非各国金融活动的执行主体或规则制定者。这一清晰的技术与治理边界，是保障体系中立性、可扩展性与主权自主性的根本。

A6.6.3 合规证明中的资产标识

如 A5.7 所述，每份 PoPC 包含一系列核心字段。为确保跨主权业务的可预期与可验证，本框架在此基础上进一步嵌入了标准化的元数据结构，以实现"**资产、清算层级、发行主体、政策领域与业务场景**"的五维精确绑定。每份合规证明必须包含以下核心元数据字段：

- **s_series（资产层级）**：标识底层资产的合规层级（S0/S1/S2/S*），明确其货币属性、风险特征及所属的统计口径（如 M0、M1 等）。
- **clearing_tier（清算层级）**：指明该笔业务适用的清算层级（如零售、一般批发、最终结算），对应不同的时效性、终局性要求及清算网络。
- **issuer_type（发行方类型）**：标注负债发行主体类别（如中央银行、商业银行、特定金融机构），关联其信用基础、监管归属及偿付责任框架。
- **policy_domain（政策领域）**：指向交易所需遵循的核心合规范畴，（如反洗钱 / 反恐融资、审慎监管、证券法规、数据跨境管制等）。

standardized. The hub is not required to interpret complex, jurisdiction-specific business details; it need only formally verify that the declared asset class and business scenario are logically consistent with the rules claimed to have been applied, and that the associated proof chain is complete. Once validation is successful, the hub's core task is focused on providing global ordering and an immutable finality anchor for these transactions that have already been proven compliant.

Accordingly, within this architecture:

- **The S-series labels** constitute the "liability language" at the financial layer, defining the forms and tiers of on-chain value.
- **The layered and domain models** provide the "settlement language" at the engineering layer, specifying the paths, boundaries, and modes of finality for value flows.
- **The compliance proof mechanism** functions as the "common grammar" that enables reliable interoperability between these two languages in a cross-sovereign environment. Through standardized proof encapsulation, it allows heterogeneous rules and assets to be understood, verified, and ultimately settled within a unified framework, thereby achieving global coordination while respecting institutional and jurisdictional differences.

- **business_scenario（业务场景）**：定义具体的业务类型（如零售支付、贸易融资、DvP 结算、跨境汇款），用于锁定该场景下适用的具体规则集与校验逻辑。

通过这一设计，主权中继枢纽在验证跨域交易时的工作得以大幅简化与标准化：SRH 无需解析各主权内部复杂的业务细节，只需形式化验证"所申报的资产类别与业务场景"是否与"所声称遵循的规则"在逻辑上自洽，并确认其证明链完整。验证通过后，SRH 的核心任务便聚焦于为这些已被证明合规的交易事件提供全局排序与不可篡改的终局性锚定。

因此，在本架构中：

- **S 系列标签**构成了金融层面的"负债语言"，定义了链上价值的形式与层级。
- **分层与域模型**提供了工程层面的"结算语言"，规定了价值流转的路径、边界与终局方式。
- **合规证明机制**则充当了使上述两种语言在跨主权环境中可靠互操作的"通用语法"。它通过标准化的证明封装，使异构的规则与资产能够在统一的框架下被理解、验证与最终结算，从而在尊重差异的前提下实现全球协同。

A6.7 Summary

本章小结

The "layered and domain models" proposed in this chapter are not intended to define an entirely new global financial architecture, nor to reshape existing sovereign systems. Rather, their core objective is to provide a systematic, implementable engineering interpretation and realization path for the three fundamental principles established

本章提出的"分层与域模型"，其核心目标并非定义一套全新的全球金融架构，亦非重塑各主权现有制度，而是为前文确立的**结算中立、可验证性、主权连续性**三大核心原则，提供一

earlier: **settlement neutrality, verifiability, and sovereign continuity**.

Within this framework, each sovereign, through its autonomously controlled **SCEL**, fully retains ultimate governance authority over its local rules, liabilities, and business processes. At the same time, through a multilateral co-governed **SRH**, constrained by the foundational principles established in these Principia, cross-sovereign scenarios achieve settlement finality anchoring in which transactions are orderable, compliance is verifiable, and system state is replayable. **Compliance proofs**, as a trusted medium traversing all layers, leverages standardized proof interfaces to forge a verifiable connection between rule execution outcomes and ledger update events, thereby constructing a complete evidentiary path that is falsifiable and independently verifiable for audit, supervision, and judicial traceability.

The layered design supports **incremental evolution**, allowing system upgrades without requiring "one-time, system-wide replacement", while the domain model ensures that all participants can collaborate on the basis of shared technical semantics within clearly defined responsibility boundaries. Together, they form a "**public grammar layer**" that both acknowledges real-world heterogeneity and enables interoperability, laying a solid abstract foundation for the subsequent design of concrete engineering standards, governance interfaces, and mutual-recognition protocols.

More importantly, the framework articulated in this chapter is not a simple patch to existing international settlement arrangements, but rather advances a new paradigm termed "verifiable interoperability". It does not seek global unification of rules, but instead focuses on the standardization of compliance proofs; it does not aim to replace traditional systems, but concentrates on constructing a trusted coordination layer across systems. In a world that is deeply interconnected yet highly differentiated, this paradigm offers a fundamentally new, system-level approach to balancing efficiency, sovereignty, and security.

On this basis, subsequent discussion can proceed to the concrete engineering standards, governance interfaces, and collaboration protocols under this paradigm, thereby transforming an architecture that is conceptually complete and logically coherent into a practical collaborative network that can be adopted incrementally on a global scale, mutually recognized layer by layer, and capable of maintaining evidentiary continuity even under extreme conditions.

个系统化、可落地的工程解释与实现路径。

在这一框架中，各主权通过其自主控制的**主权合规执行层**，完全保留了对本国规则、负债及业务流程的最终治理权。同时，借助一个受宪章约束、由多边共治的**主权中继枢纽**，在跨主权场景中实现了交易可排序、合规可验证且状态可重放的结算终局锚定。**合规性证明**作为贯穿各层级的可信媒介，通过标准化证明接口，将规则执行结果与账本更新事件进行可验证关联，从而为审计、监管与司法追溯构建了可证伪、可独立验证的完整证明路径。

分层设计支持**渐进式演进**，允许系统升级无需"全系统一次性替代"；域模型则确保各参与方在明确职责边界的前提下，能基于共同的技术语义实现协作。二者共同构成了一套既承认现实差异、又支持互操作的"**公共语法层**"，为后续具体的工程标准、治理接口与互认协议设计奠定了坚实的抽象基础。

更重要的是，本章所阐述的框架，并非对现有国际结算体系的简单修补，而是提出了一种名为"可验证互操作"的新范式。它不追求全球规则的统一，而是致力于实现合规证明的标准化；不寻求对传统系统的替代，而是专注于构建跨系统的可信协同层。在一个深度互联却又高度分化的世界中，这一范式为如何平衡效率、主权与安全这一根本性难题，提供了一个全新的系统性解题思路。

基于此，后续的探讨得以深入该范式下的具体工程标准、治理接口与协作协议，从而将一个理念上完备、逻辑上自洽的架构，转化为可供全球渐进采用、逐层互认、且能在极端条件下保持证明连续性的现实协作网络。

1. The total issuance scale of S1 liabilities, denoted as S1totalS1_{total}S1total, is constrained by the traditional deposit reserve regime. Its relationship with the corresponding reserve requirement ratio rdr_drd can be expressed as:

S1 负债的总发行规模 $S1_{\text{total}}$ 受传统存款准备金制度的约束，其与相应的存款准备金率 r_d 的关系可表述为:

$$S1_{total} \leq \frac{\text{Total Amount of Eligible Reserves}}{r_d}$$

2. The duration D(S2)D(S2)D(S2) of S2 liabilities is calculated using the Macaulay duration formula and is defined as the present-value–weighted average maturity of all future cash flows:

S2 负债的久期 $D(S2)$ 采用麦考利久期公式计算，其定义为所有未来现金流的现值加权平均到期时间:

$$D(S2) = \sum_{t=1}^{n} \left[\frac{CF_t \cdot t}{(1+y)^t} \right]$$

3. To ensure financial system stability, the total scale S∗S^*S∗ of S* assets within the clearing network must satisfy the following inequality constraint:

为确保金融系统的稳定性，S^* 资产在清算网络中的总规模 $S*$ 需满足以下不等式约束:

$$\text{CLS} \geq S^* \geq \sum \text{Credit Exposure}$$

CHAPTER A7.

SSI Interoperability & Mutual Recognition

A7. 章节

主权协同结算层互操作与互认框架

Abstract:

Sovereign EVM-compatible Compliance & Execution Layers (SCELs) for CBDCs and digital assets create an inherent tension between regulatory autonomy and interoperability. Each SCEL operates under a Jurisdiction Pack (JPack), defined in a Policy-DSL, which encodes immutable mandates (e.g., residency requirements, transaction limits, and sanctions enforcement) to preserve local sovereignty.

Modern finance, however, requires cross-chain compliance portability: payments must settle and assets must transfer across domains while preserving their compliance context. Without a shared constitutional framework, SCELs risk becoming isolated, creating opportunities for arbitrage, enforcement gaps, and opaque audit trails that weaken the rule of law. This fragmentation undermines trust and widens the mismatch between universal ledger execution and jurisdiction-specific policy enforcement (refer to A5).

Layered attestation and standardized cross-domain messaging protocols can bind ledger finality to policy finality across SCELs. Each cross-domain message is verifiable under the trust-tier model and executed within each SCEL's Regulatory VM. This approach preserves JPack autonomy: policies remain intact, transparently composable, and enforceable, with PoPC proofs (A5) providing an immutable compliance record.

Regulators gain access to a unified audit plane: transaction flows can be reconstructed back to their originating JPack and context, ensuring accountability without forcing convergence to a lowest common denominator.

(本章摘要)

面向央行数字货币（CBDC）与数字资产的主权合规执行层（SCEL），在兼容 EVM 灵活性的同时，必须解决监管自主性与全球互操作性之间的结构性博弈。通过将基于 Policy-DSL 的司法辖区法规要件集（JPack）锚定于执行内核，SCEL 将居民身份、限额控制及制裁过滤等不可变的监管指令铸造为底层执行逻辑，从而确立了本域政策的绝对主权。

然而，现代金融的本质逻辑在于合规效力的跨域互认：在支付跨链结算与资产跨域转移的过程中，合规效力必须实现无损穿透。若缺乏一套宪制级的协调框架，各 SCEL 势必沦为相互隔绝的数字孤岛，不仅会滋生套利黑洞与执法断层，更将加剧全球统一账本与本地政策执行之间的本质冲突（见 A5 章）。

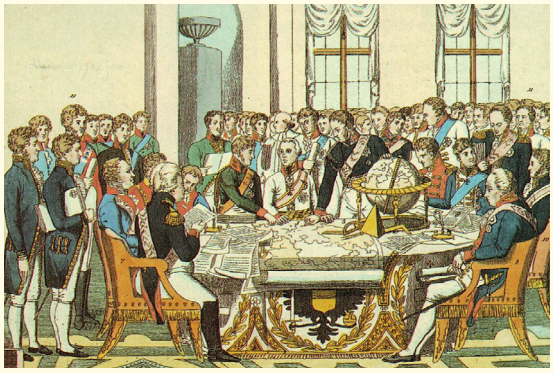
主权协同结算层（SSI）构建了一套分层证明机制与标准跨域通讯协议，实现了异构 SCEL 间“账本最终性”与“政策最终性”的强力耦合。在信任分级模型的严苛校验下，每一条跨域消息都具备可验证性，并由各辖区 SCEL 内置的监管虚拟机闭环执行。该路径捍卫了 JPack 的主权自治：政策不被外部逻辑穿透、而是以透明、可组合的方式被精准引用，并以政策合规证明（PoPC）的形式固化为不可篡改的合规账本（见 A5 章）。

监管机构由此获得全局审计视界，实现资金流转与原始政策语境的实时溯源。在尊重各国管辖差异的同时，实现了高度的可问责性。

A7.1

Cross-Domain Messaging Invariants

跨域消息传递的不变量



Wiener Kongress, Europas Wiedergeburt durch den groBen Herrscherverein zu Wien,1814

"The law of nations shall be founded on a federation of free states."

"国际权利应以自由国家的联邦制为基础。"

— Immanuel Kant, Perpetual Peace: A Philosophical Sketch (1795) 康德《永久和平论》

Cross-domain messaging is required where coordinated execution must occur across sovereign enforcement boundaries. Clearly delineating these boundaries is a core prerequisite for preventing "logical entanglement" between intra-domain operations and inter-jurisdictional dependencies. Cross-domain messaging shall be defined such that domestic policy enforcement remains isolated and sovereign, independent of external domains.

The A7 framework shall restrict cross-domain messaging to the following interaction classes:

1. **Functional operational vertical connections with SRH.**
2. **Strengthening vertical interactions between participants thanks to SSI.**

As the neutral nexus for multi-domain coordination, the SRH facilitates three primary types of cross-domain interactions:

- **Value Transfers**: The system shall permit the transfer of tokens across distinct residency identities and/or jurisdictions.

凡涉及跨主权执行边界的协同任务，皆须经由跨域通讯协议。主权边界的清晰划定，是防止"域内操作"与"跨境依赖"逻辑纠缠的根本。跨域通讯协议须遵循主权隔离原则：国内政策的执行应保持独立自主，并在逻辑上彻底脱离对外部域的依赖。

A7 框架严格限定跨域通讯的交互范畴，仅涵盖以下类别：

1. **与 SRH 之间具备功能运行属性的纵向连接。**
2. **借助 SSI 强化参与方之间的纵向交互。**

主权中继枢纽作为多域协调的中立枢纽，SRH 承载的交互类型主要包括：

- **Data Attestations**: Secure propagation of compliance-relevant information (e.g., KYC credentials) shall be supported across domains.
- **Conditional Executions**: Conditionally triggered automated regulatory actions (e.g., transaction re-screening against updated sanctions lists) shall be supported.

All cross-domain interaction types shall invoke the Regulatory VM and all cross-domain interaction types shall generate dual-end verifiable Proof-of-Policy-Compliance (PoPC) artifacts.

In contrast, intra-domain messaging, such as communication between an SRH and its SCELs, remains entirely sovereign and is exempt from A7 constraints. Similarly, legacy financial protocols (e.g., SWIFT messages and ISO 20022) are handled by sovereign-specific gateways at the domain boundary. These gateways translate external messages into A7-compliant message frames without affecting core invariants, preserving the Hub's neutrality and minimalism.

This scoped architecture safeguards sovereignty while enabling compliant interoperability. The SRH validates cross-domain messages without interpreting payloads; policy composition and execution occur within SCEL Regulatory VMs. Replay protection is anchored to the Hub's versioned state, ensuring cross-domain messages remain verifiable against archived JPacks.

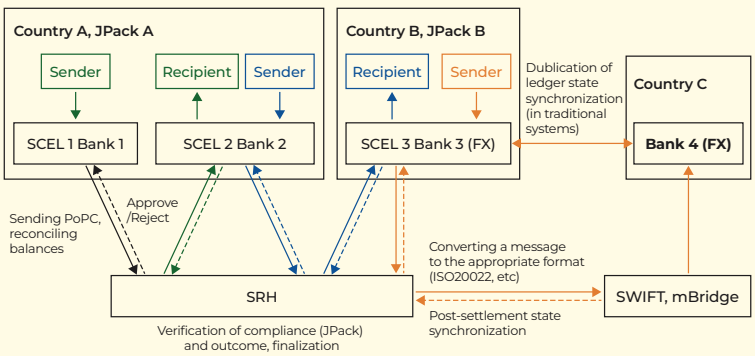


Figure 9: General SSI Cross-Domain Compliance and settlement Flow

Three **constitutional invariants** govern all cross-domain messages:

- **Uniqueness / Idempotence**: Each message or transaction must carry a globally unique identifier (e.g., a nonce or UUID) to prevent duplication or replay.
- **Ordering**: Each message or transaction must include sequencing or timestamp metadata to enable deterministic ordering across domains, with final resolution determined by the receiving policy.

- **价值转移**：支持代币在不同居民身份及司法辖区间的跨域流转。
- **数据证明**：支持合规关联信息（如 KYC 凭证）在不同域间的安全传播与校验。
- **条件性执行**：支持由特定条件触发的自动化监管响应（如针对更新后的制裁名单进行二次实时筛查）。

所有跨域交互均强制经由监管虚拟机处理，并以生成双端可验证的政策合规证明（PoPC）为唯一合法凭据。

相对而言，域内通信（如 SRH 内部组件或特定 SCEL 内部模块间的通信）属于绝对主权内部事务，不受 A7 协议约束。相应地，传统金融消息协议（如 SWIFT 报文、ISO 20022）由主权边界处的专用网关处理。这些网关承担“协议转换器”的职责，负责在不穿透核心不变量的前提下，将外部报文转换为符合 A7 协议规范的消息帧，以此捍卫 SRH 的中立性与极简架构。

这种“有边界”的架构在捍卫主权的同时，实现了合规层面的深度互操作：SRH 仅对跨域消息执行合法性校验，而不对载荷内容进行解释；政策组合逻辑始终在 SCEL 的监管虚拟机内部完成。消息的可重放性锚定于枢纽的版本化状态，确保即便在多年后的审计中，基于历史 JPack 的跨域行为依然具备确定的可验证性。

所有跨域消息必须严格满足以下三项**宪制级不变量**：

- **唯一性与幂等性**：每条消息必须携带全局唯一标识符（如 Nonce 或 UUID），从协议层彻底杜绝重复执行或重放攻击。

- **Timeliness / Boundedness**: Each message or transaction must specify an expiration window; undelivered or unprocessed messages trigger policy-defined timeouts.

In implementation, SCELs shall enforce these guarantees by including, within each message, a nonce, a source-domain sequence identifier, and an expiration window. The SRH or the receiving domain shall maintain canonical message ordering (e.g., through global mempools, priority queues, or equivalent mechanisms). SSI shall require that all participating domains strictly adhere to these constraints.

- **确定性排序**：消息必须包含序列号或时间戳，以实现跨域语境下的统一排序，由接收方的策略引擎进行线性解析。
- **时效性与有界性**：每条消息必须声明显式的有效期窗口，超时未处理的指令将根据既定策略自动触发失效或逻辑回滚。

在工程实现层面，SCEL 应通过在每条消息中强制嵌入随机数、源域序列标识以及失效窗口，来确保上述安全属性的硬性执行。SRH 或接收域应通过全局内存池、优先级队列或同等机制，确立规范的消息定序。SSI 协议强制要求所有参与域必须严格遵守此类约束。

A7.2

Message Format and Metadata

消息格式与元数据

All cross-domain requests are encapsulated in an A7 message format with standardized metadata (the exact wire format is not prescribed here). Each packet shall include the following mandatory metadata fields:

- **Chain Identity**: A source-domain identifier and a target-domain identifier drawn from the global Sovereign Registry. Each SCEL shall have a unique chain ID registered with the SRH. Messages shall carry these identifiers to ensure correct routing and interpretation across domains.
- **Routing Metadata**: Additional routing and sequencing fields required by the Hub (e.g., channel index, priority flags). This enables the L1 Hub and the target SCEL to determine the applicable protocol path or application context without embedding policy content.

所有跨域请求均须采用 A7 消息格式进行封装，并携带标准化元数据（此处不对具体线路传输格式做强制约束）。每一数据包皆须包含以下元数据字段：

- **主权域身份标识**：基于“全球主权注册表”定义的源域与目标域唯一标识。每个 SCEL 均在主权中继枢纽上注册专属的链 ID，作为跨域路由发现与政策逻辑解释的基准索引。
- **路由元数据**：包含枢纽节点所需的排序字段、通道索引及优先级标记。该字段确保 SRH 与目标 SCEL 能在不触碰载

- **Trust Tier Indicator**: A field indicating which attestation tier applies to the message (refer to Attestation Model, below). This indicator enables receivers and auditors to determine whether the message is supported by cryptographic proof, a committee signature, or a single-gateway signature.
- **PoPC Reference**: A reference to the Proof-of-Policy-Compliance (PoPC) artifact generated by the sending SCEL. This reference typically includes a Merkle root or digest of the PoPC data (i.e., verifiable proof of policy evaluation), together with any required signatures. The Hub's verification VM uses this reference to retrieve and validate the corresponding PoPC record.
- **Policy Snapshot Hash**: A hash (or version identifier) of the specific Policy-DSL pack (JPack) under which the transaction was executed. This binds the message to a specific policy version on the sender's chain. During SRH verification, the Hub loads the JPack referenced by this hash to support compliance re-evaluation and auditability.
- **Payload**: The transaction data or settlement instruction, as generated by the sending SCEL.

By convention, the message header may carry these fields, and the payload may contain a native token transfer and/or an encoded smart-contract call. Critically, legacy message formats are out of scope for A7: ISO 20022 or SWIFT flows are handled outside SSI by domain gateways.

荷内容的前提下，精准识别消息所属的协议路径与应用上下文，实现底层传输与高层政策的逻辑解耦。

- **信任等级标识**：显式声明该消息所采用的证明强度级别（见以下鉴证机制）。接收方与第三方审计机构据此即时确认该消息是由加密证明、委员会共识还是单一网关背书提供信任支撑，从而触发相应的风险处置逻辑。
- **合规性证明引用**：指向发送方 SCEL 生成的“政策合规证明”数据块指针。该引用通常包含 PoPC 的默克尔根或加密摘要及关联签名。枢纽节点的监管虚拟机将通过此引用调取完整的执行证明，启动合规性核验。
- **策略快照哈希**：交易执行时所依据的特定 JPack（Policy-DSL 规则包）的版本指纹。该哈希值将消息与发送方特定时刻的法律规则集进行强绑定。在重放校验过程中，枢纽节点依据此哈希精准加载对应的法规要件集，重新展开合规性评估。
- **负载数据**：由发送方 SCEL 确定的核心交易数据或结算指令，如代币转账证明或经编码的智能合约调用数据。

按照设计惯例，消息头承载上述治理与验证元数据，而负载数据则负责具体的结算逻辑。需要明确的是，传统金融消息格式（如 ISO 20022 或 SWIFT 消息）不属于 A7 协议的直接处理范畴。此类信息流由域边界处的网关在 SSI 系统外部完成预处理，仅将其逻辑映射结果转化为 A7 兼容的封装格式，从而确保主权中继枢纽的架构极简性与技术中立性。

A7.3

Attestation & Trust-Tier Model

In a heterogeneous network, security postures can vary widely - from trusted execution environments to multi-signature committees. Cross-domain attestations may therefore become a systemic weak point: mismatched trust assumptions can enable capture, collusion, or degradation into opaque oracle dependencies. Without a formal trust hierarchy, sovereign chains (SCELs) risk forming brittle interoperability arrangements that undermine the mutual recognition required for sovereign collaboration.

A7 defines a **three-tier trust model** for attestations, providing progressively weaker assumptions but still verifiable guarantees:

Tier 1 - Proof-Based Attestation:

The sender attaches a verifiable cryptographic proof of the relevant state transition (e.g., a Merkle proof of a state commitment, a light-client block attestation, or an on-chain commitment published by the SCEL). These proofs enable the L1 Hub or the receiving SCEL to validate the transaction independently, without reliance on external trust intermediaries. Tier 1 attestation is preferred and shall be used whenever the chain's consensus and/or light-client capabilities support it.

Tier 2 - Committee-Signed Attestation:

Where direct proofs are infeasible (e.g., due to incompatible virtual machines or the absence of light-client support), a multi-sovereign validator committee attests the cross-domain message. A quorum of validators, using a BFT mechanism or an N-of-M threshold signature scheme, co-signs a cross-domain certificate confirming transaction validity. This joint signature distributes trust across jurisdictions and provides institutional accountability. Tier 2 attestation shall be used only where supported by multi-party governance and formally defined institutional rules.

Tier 3 - Single-Gateway Fallback:

As a last resort under degraded conditions (e.g., during initial bootstrap, emergency recovery, or committee downtime), a single designated gateway (such as a bridge

鉴证机制与信任层级模型

在异构主权网络生态中，各司法辖区的安全架构存在显著差异：从基于可信执行环境（TEE）的硬件合规方案，到基于多签委员会的社会共识方案不一而足。在这种高度多样化的背景下，跨域证明极易成为系统的安全性洼地：一旦信任假设发生错配，可能诱发恶意合谋、系统控制权篡改等风险，甚至导致高度多中心化的架构退化为不透明的中心化预言机。若缺乏明确的信任分级与制度化约束，主权链间的协作基础将变得极度脆弱。

为化解这一风险，A7 引入了一套三**层信任分级模型**，为跨域消息提供递进式的可验证保障：

第一层 - 基于证明的认证：

这是信任最小化的首选方案。发送方需随消息附带可独立验证的加密证明（如状态承诺的 Merkle 证明、轻客户端区块证明或链上状态承诺）。该层级允许主权中继枢纽（SRH）或接收方在不依赖任何第三方中介的情况下，通过数学手段自行验证消息的真实性。在底层共识与技术规范允许的前提下，第一层核验被视为跨域交互的强制性准则。

第二层 - 委员会签名认证：

作为技术妥协方案，适用于直接加密证明不可行（如虚拟机不兼容或缺乏轻客户端支持）的场景。由多主权验证委员会通过拜占庭容错（BFT）或（N-of-M）

contract, registrar, or authorized relay) may attest to the message. This mode shall be explicitly flagged as Tier 3 and is inherently less trust-minimized. Tier 3 messages carry a gateway signature and timestamp, and each instance shall be immutably logged. Flagged transactions shall be subject to heightened audit review. Tier 3 attestation shall be permitted only when Tier 1 and Tier 2 methods are unavailable.

Escalation and Auditability

Attestation selection shall follow a strict hierarchical escalation path: where Tier 1 proof-based attestation is unavailable, the system shall fall back to Tier 2 committee attestation; where Tier 2 is unavailable, it may fall back to Tier 3 single-gateway attestation. Any downgrade in the trust tier shall require explicit authorization within the applicable JPack and shall be audit-logged.

The SRH shall mediate attestation transitions neutrally, ensuring that no trust tier overrides local policy and that all attestations remain jurisdictionally compliant. All cross-domain messages and attestation records shall be cryptographically committed.

The SRH shall anchor PoPC records (e.g., by committing Merkle roots of received PoPC references into block headers), enabling auditors to replay and verify historical compliance states. Tier 3 events shall include distinguishing metadata to make trust degradations explicit and machine-detectable.

阈值签名机制对消息进行联合背书。这种分布式签名的本质是将单点信任风险分摊至跨司法辖区的共识主体中，其启用必须获得多方治理框架的显式授权。

第三层 - 单一网关回退机制：

在系统退化或应急情形下（如网络初始化部署或委员会停运期间），允许由单一指定网关（如可信的桥接合约或注册机构）对消息进行认证。由于其信任强度本质较低，所有此类消息必须被明确标记为“第三层”，且须附带严格的时间戳与网关数字签名，供审计方进行穿透式复核。第三层机制仅在前两层均不可用时方可启用。

升级与可审计性

鉴证机制遵循严格的阶梯式回退原则：仅当第一层（Tier 1）加密证明不可达时，系统方可回退至第二层（Tier 2）委员会鉴证；同理，仅在第二层失效时，方可降级至第三层（Tier 3）单一网关鉴证。任何信任能级的跌落，均须获得对应法规要件集（JPack）的显式授权，并存入全量审计日志。

主权中继枢纽（SRH）应作为中立实体调配鉴证模式的转换，确保任何信任层级均不得凌驾于本地政策之上，且所有鉴证行为必须严格符合司法管辖合规。所有跨域消息及鉴证记录均须执行加密存证。

SRH 负责对合规性证明（PoPC）记录执行锚定（如：将已接收 PoPC 索引的 Merkle 根嵌入区块头），以确保审计方能够回溯并验证历史合规状态。第三层级事件必须包含特定的标识性元数据，以确保信任降级逻辑显性化，并具备机器可检测性。

A7.4

Governance Model and Transition Path

In the initial stage, the cross-domain relay network operates under a Bootstrap Governance Mode, managed by a custodial validator set to enable rapid deployment and early-stage network optimization. During this phase, both Hub validators and bridging authorities between SCELs operate as known entities under Foundation oversight or a regulated consortium, thereby establishing stable centralized trust anchors during the network's "cold-start" period.

As the ecosystem matures, the governance architecture is designed to evolve toward a Multi-Sovereign Co-Governance Model. The system includes an automated upgrade path that enables a controlled transition of the validator set from single-entity oversight to governance by a Council of Sovereign Institutions. As the network of interconnected SCELs expands, the validator set may scale to incorporate representatives nominated by participating jurisdictions and/or regulated entities, thereby establishing a more distributed equilibrium of consensus authority.

In the steady-state governance model, the cross-chain governance framework shall operate as institutionally governed digital infrastructure. In this state, the Hub's consensus protocols and cross-domain committees shall be composed exclusively of validator nodes approved by sovereign regulators and subject to public oversight. No single chain or entity shall retain permanent control over the system.

This design aligns with the Layered Sovereignty Framework (A5 & A6): Tier 1 (S1) actors (Domain Governance Authorities) define jurisdictional policy and governance decisions, while Tier 0 (S0) - the SRH - maintains neutral consensus execution. Critical transition mechanisms, including validator set upgrades, hard-fork authorizations, and governance votes, are codified via on-chain smart contracts and embedded within the system's Meta-Constitution. This "Code-as-Constitution" model ensures that the transition from centralized bootstrapping to distributed governance remains predictable, auditable, and legally resilient.

治理模型与过渡路径

在系统启动初期，跨域中继网络采取引导期治理模式，由项目方托管的验证节点集进行统一管理，以确保快速部署与网络调优。在此阶段，枢纽节点及各 SCEL 间的桥接中介均作为受基金会或受监管联盟管理的已知实体运行，从而在网络冷启动期形成稳定的集中式信任锚点。

随着生态系统的日益成熟，治理架构必须向多元主权共治模式演进。系统内置了自动化的治理升级路径，支持验证节点集从单一实体管控平滑过渡为由多国主权机构组成的共治委员会。随着接入网络的 SCEL 数量增加，验证节点集合将通过动态扩展机制，引入由各司法辖区或受监管机构提名的代表节点，实现共识权力的分布式平衡。

在常态化治理模型下，跨链治理框架应作为受制度约束的数字基础设施运行。枢纽节点的共识协议与跨域委员会，将完全由经主权监管机构核准、并接受公众监督的验证节点构成。在此终局状态下，任何单一链或特定实体均不具备对系统的永久控制权。

这一设计与分层主权框架（A5 & A6）高度逻辑契合：S1 层（域治理机构）负责政策制定与辖区内治理决策，而 S0 层（主权中继枢纽）则专注于中立的共识执行。诸如硬分叉授权、治理投票等关键过渡机制，均以链上智能合约的形式进行逻辑固化，并深度嵌入系统《元宪章》之中。这种"代码即宪法"的治理模式，确保了从集中式引导向分布式治理转型的每一路径都具备可预期性、可追溯性与法治韧性。

A7.5

Policy Finality and Proof-of-Policy -Compliance

The substantive completion of cross-domain operations shall be predicated on two concurrent conditions: Ledger Finality and Policy Finality. Every cross-domain transfer shall carry a PoPC attestation issued by the originating SCEL. Upon message delivery, the Sovereign SRH or the destination SCEL shall initiate an independent Deterministic Replay Verification using the policy pack index referenced in the message.

Within this workflow, the Regulatory VM shall load the historical rule set identified by the policy_snapshot_hash and deterministically re-execute the relevant Policy-DSL scripts. Transaction compliance shall be considered validated only if the Regulatory VM's replay result is bit-identical to the submitted PoPC proof.

Accordingly, final settlement shall be defined as the intersection of two conditions: **ledger inclusion and successful policy verification**. Until the SRH reaches Byzantine Fault Tolerant (BFT) consensus on compliance validation, the transaction shall remain in a Pending state. Upon final confirmation, the SRH shall issue a Regulatory Finality Receipt, which encapsulates the originating and destination block references (where applicable), validation parameters, the policy version identifier, and the PoPC digest. This receipt shall be archived by the SCELs on both ends.

This mechanism establishes a Dual Finality Architecture:

- **User Dimension**: Settlement finality is achieved on the originating SCEL according to its ledger consensus rules.
- **Regulatory Dimension**: Policy finality is achieved via immutable compliance confirmation notarized by the SRH.

This verifiable compliance framework ensures that no cross-domain transaction can violate policy without detection. Auditors and counterparties may replay archived PoPC records to validate compliance under historical rules. Any mismatch between SCEL and SRH records is deterministically detectable, rendering the system auditable and tamper-evident.

政策最终性与政策合规证明（PoPC）

跨域操作的实质性完成，必须建立在账本最终性与政策最终性的双重约束之上。每一笔跨域转账均须携带由发起方 SCEL 签发的政策合规证明。在消息送达后，主权中继枢纽（或目标 SCEL）将依据消息引用的法规要件集索引，对交易启动独立的“重放验证”。

在此流程中，监管虚拟机根据策略快照哈希（policy_snapshot_hash）加载对应的历史规则集，并以确定性方式重新执行 Policy-DSL 脚本。只有当重放结果与提交的 PoPC 证明达成位级一致时，该交易的合规性方可获得确认。

因此，最终结算定义为两个并行条件的交集：**资产入账与全局政策校验通过**。在枢纽节点确认之前，交易将维持“挂起”状态。一旦触发最终性确认，枢纽节点将签发一份“监管终局性回执”。该回执完整封装了区块高度、校验因子、政策版本及 PoPC 摘要，由交易双方的主权合规执行层实时存档。

这一机制构筑了独特的双重最终性架构：

- **用户侧**：在发起域 SCEL 上获得即时的结算确定性。
- **监管侧**：通过中继枢纽的公证机制，获得不可篡改的政策合规确认。

这种基于证明的合规机制，确保了任何跨链交互无法绕过政策约束。审计机关或交易对手方可随时调用存档证明，基于历史政策基准追溯验证。SCEL 记录与枢纽公证数据之间的任何细微偏差都将被精准识别，从而在底层协议层面保障了系统极强的可审计性与防篡改能力。

A7.6

Integration with Layered Sovereignty (A5&A6)

SSI complements the Policy-DSL and Layered Sovereignty frameworks:

A7.6.1 Deep Integration of Proof-of-Policy-Compliance (PoPC)

Each cross-domain message shall originate from a SCEL that has executed the applicable Policy-DSL rule set and shall carry the corresponding PoPC output. For every cross-domain message, SCELs shall include complete PoPC artifacts, including decision traces, rule identifiers, and reason codes.

- **Dual-Finality Validation**: The SRH shall permit a cross-domain message to advance to the finality stage only when it is accompanied by valid PoPC proof. Inter-jurisdictional interoperability shall be considered valid only upon the concurrent satisfaction of ledger finality and policy finality.
- **Rule Consistency Assurance**: Since SCEL JPacks are referenced on-chain via versioned pointers, policy upgrades achieve global visibility through the Sovereign Registry. This mechanism ensures that cross-domain execution references explicit policy versions and remains consistent under deterministic replay.

A7.6.2 Layered Sovereignty Integration

SSI delineates responsibilities across sovereignty layers, establishing a strict separation between policy decision-making and neutral protocol execution:

- **Tier 0 (S0) Sovereign Relay Hub**: Operates as a minimal consensus layer responsible for message ordering, attestation verification, and cross-domain finality confirmation.
- **Tier 1 (S1) Sovereign Domain**: SCELs generate policy-attested messages, produce PoPC artifacts, and finalize transactions locally under their jurisdictional mandates. Cross-domain contracts operate at the S0/S1 interface: S0 validators execute the interoperability protocol, while S1

与分层主权模型的集成（A5&A6）

SSI 是对 Policy-DSL（A5）与分层主权框架（A6）的系统性整合与功能闭环。通过这种集成，系统确立了跨域协作的最终规范：

A7.6.1 政策合规证明（PoPC）的深度集成

所有跨域消息必须由发起方 SCEL 启动，且该层级须预先完成 Policy-DSL 规则的本地判定。每一条流向外部的消息均须挂载详尽的 PoPC 凭证，涵盖决策轨迹、规则指纹及判定逻辑码。

- **双重最终性校验**：SRH 仅允许与 PoPC 匹配的消息进入最终性阶段。跨域互操作的法律效力，仅在“账本最终性”与“政策最终性”高度同步时方告成立。
- **规则一致性保障**：由于 SCEL 各域 JPack 均通过主权注册表进行链上版本化引用，任何政策升级均具备全局可见性，确保了跨域执行逻辑的原子性与一致性。

A7.6.2 分层主权集成

SSI 清晰划分了各主权层级的职责边界，实现了“决策与执行”的逻辑分离：

- **S0 层（主权中继枢纽）**：作为“极简共识层”，专注于消息排序、证明核验与跨域终局性确认。
- **S1 层（主权域层）**：SCEL 负责生成经政策鉴证的消息，产出合规性证明

validators ensure outbound conformance and enforce local policy constraints through replay and verification.

- ***Tier * (S) Regulatory Coordination Layer***: Serves as a governance oversight layer that may influence macro-policy direction through participation in Hub governance. Such actions shall remain external to protocol execution logic and shall not interfere with the neutral operation of S0.

This architecture ensures that cross-domain interactions follow a unified protocol while preserving execution autonomy and governance pluralism across participants.

A7.6.3 Sovereign Chain Identity and Registration

To mitigate forgery risks and accountability gaps associated with temporary identifiers, SSI defines a hierarchical and versioned sovereign identity registration scheme (e.g., jurisdiction:SCEL:instance).

- **Sovereign Chain Identity & Registry**: Chain identities shall be registered through multi-sovereign consensus and anchored in the global state of the S0 layer. The registry shall support Merkle proofs (or equivalent commitments) for direct on-chain verification and invocation.
- **Source Authentication**: By embedding sovereign identity references within message metadata, recipient SCELs can perform endogenous authentication of message origins without reliance on off-chain oracles. This framework functions as an on-chain Domain Name System (DNS) for sovereign domains, ensuring that Regulatory VM queries remain globally deterministic during cross-domain instruction resolution.

（PoPC）凭证包，并在司法授权下完成本地交易终局性结算。跨域合约运行于 S0/S1 界面：S0 验证者执行互操作协议，而 S1 验证者则通过回溯验证机制，确保出境合规并强化本地政策约束。

- ***S 层 *（监管协同层）***：作为“治理监督层”，通过参与 SRH 治理影响宏观政策，但其治理行为被限制在底层协议逻辑之外，无法干涉 S0 的中立执行。

这种架构确保跨域交互在遵循统一协议的同时，捍卫了各参与方执行自主权与治理多元化。

A7.6.3 主权链身份与注册机制

为消除临时标识符带来的伪造风险与追溯断层，SSI 构建了分层级、带版本号的主权身份注册系统（如 jurisdiction:SCEL:instance）。

- **主权链身份与注册表**：链身份标识须经由多主权共识核准注册，并锚定于 S0 层的全局状态。注册表须支持 Merkle 证明（或同等效力的承诺机制），以实现直接的链上鉴证与契约调用。
- **来源验证**：将主权身份引用嵌入消息元数据封装，接收方 SCEL 无需依赖链下预言机，即可实现对消息来源的一致性验证。这为主权域构建了一套“链上域名系统（DNS）”，确保监管虚拟机在解析跨域指令时具备全局唯一的确定性。

A7.7

Infrastructure Principles

The cross-domain fabric is intentionally neutral, minimal, and auditable. It is analogous to an interbank messaging network (e.g., SWIFT) or a real-time gross settlement (RTGS) system in that it does not introduce application-specific business logic or jurisdiction-specific policy. Instead, it transports cross-domain messages and associated compliance proof between SCELs under agreed constitutional constraints. Accordingly, the following infrastructure principles apply:

1. **Neutrality of the Sovereign Relay Hub (SRH)**
   The SRH shall provide consensus ordering and cross-domain finality only. It shall not interpret, transform, or modify message payloads, except as required to verify associated attestations and Proof-of-Policy-Compliance (PoPC) proof. This design prevents jurisdiction-specific preferences from being embedded at the SRH layer. Gateways to external systems (e.g., SWIFT, ISO 20022) are out of scope for A7; such integrations shall be implemented at SCEL boundaries and shall preserve A7 invariants without introducing protocol-specific dependencies into the Hub.
2. **Protocol-Level Transparency and Auditability**
   All protocol-relevant steps shall be transparently recorded on-chain. As described in A5, the Hub's validation outcomes for each cross-domain message shall be committed to the global state (e.g., via commitments to a Global State Tree and/or a transaction archive). This enables full auditability of cross-domain activity, including transaction provenance, referenced policy versions, and compliance outcomes. The resulting audit trail replaces opaque correspondent banking workflows with cryptographically verifiable protocol proof.
3. **Minimal Governance and Layered Execution**
   Governance shall remain minimal and constitutionally bounded. A7 defines core invariants and trust-tier requirements, while deferring implementation-specific details to subordinate protocol specifications (the B-volume). A7 therefore does not mandate a specific wire format or

基础设施设计原则

跨域通信架构的设计遵循中立、极简、可审计三大核心原则。其角色类似于银行间消息网络（如 SWIFT 或 RTGS）：不内置任何业务逻辑或政策规则，也无需对每笔转账进行复杂治理，仅在既定宪制规则下传递交易与证明。具体设计原则如下：

1. **主权中继枢纽的中立性与纯粹性**
   主权中继枢纽（SRH）仅提供共识与最终性服务。该模块必须保持技术中立，除验证附带的政策合规证明（PoPC）外，它不对交易内容作任何解释或修改。这一设计确保了任何单一司法辖区的偏好都不会嵌入系统底层。此外，与 SWIFT 或 ISO 20022 等外部系统的对接网关被明确排除在 A7 设计范畴之外。此类网关由各主权域在边界自行实现，与枢纽交互时必须遵守 A7 不变量。
2. **全流程透明化与协议级审计**
   正如 A5 章节所述，对每条跨域消息的验证结果都会写入全局状态（如全局状态树或交易归档）。因此，任何人都可对跨链账本进行审计：所有跨域交易记录、政策版本迭代、合规校验结果，均通过加密方式完整留存。这一结构用协议级的审计追踪机制，取代了传统代理行模式下不透明的操作流程。
3. **极简治理与分层架构设计**
   A7 明确界定了核心约束条件与信任层级

cryptographic primitive. This separation preserves stability at the constitutional layer while enabling iterative adoption of improvements (e.g., new proof constructions or encryption mechanisms) without requiring changes to A7 semantics.

4. **Lightweight Protocol and the "Trusted Black Box" Model**
   The SRH shall implement only the minimum functionality required for cross-domain coordination: message ordering, attestation verification, and finality confirmation. This design aligns with mature financial infrastructure models (e.g., RTGS and clearing systems), enabling regulators to treat the Hub as a "trusted black box" in the operational sense: it processes legally sealed and verifiable messages and issues legally final receipts, while neither holding funds nor acting as a counterparty. Cryptographic verification provides enforcement guarantees, and the on-chain record provides auditability.

框架，但将具体实现细节交由次级协议规范。A7 不锁定任何特定的消息格式或加密算法，相关技术细节由配套协议（B 卷）定义。这种分层设计，既保障了宪制层的稳定性与前瞻性，又使得新型证明方案或加密技术可在不改变 A7 逻辑的情况下引入。

4. **轻量化协议层与可信黑盒模型**
   整体设计致力于打造轻量化的协议层：主权中继枢纽只承载共识与验证的最低必要功能，运作方式类似于央行之间的 RTGS 或清算系统。与成熟金融基础设施的对标，有助于监管机构将枢纽节点视为可信黑盒：它接收经法律与加密封装的消息，并输出具备法律效力的最终回执，但不持有资产、也不充当交易对手。加密技术为协议执行提供刚性约束，链上记录则为审计工作提供完整依据。

A7.8

Compliance with Policy-DSL and Sovereign Frameworks

与 Policy-DSL 及分层主权框架的合规性适配

The design of the Sovereign Settlement Interoperability (SSI) layer preserves the policy sovereignty of each participating domain. No jurisdiction is required to accept extraterritorial rule enforcement; rather, each domain independently verifies that cross-domain interactions conform to its domestic policy constraints. When assets, obligations, or regulatory actions cross domain boundaries, the originating SCEL asserts compliance by issuing Proof-of-Policy-Compliance (PoPC), while the Sovereign Relay

主权协同结算层 SSI 的设计核心在于尊重各主权域的政策自主权。任何司法辖区均无义务接受域外规则，仅需核验交互行为是否符合本地政策。当资产或交易跨域流转时，发起方 SCEL 通过 PoPC 为其合法性背书，而主权中继枢纽（SRH）负责验证这些声明，在保障账本最终性的同时，维持跨域政策的终局性。

Hub (SRH) validates the associated proof and coordinates policy finality alongside ledger finality.

Accordingly, SSI enforces the following compliance properties:

1. **Proof-chain integrity and dual-finality constraints**
   Interoperability introduces a fundamental risk: if the evidentiary chain linking outcomes to their regulatory origin is broken, compliance decisions become unverifiable and incompatible with audit-based enforcement. To mitigate this risk, each cross-domain message shall be accompanied by PoPC attesting to JPack integrity, the jurisdictional constraints traversed, and dual-policy execution where applicable. Settlement shall require both ledger finality and policy finality; neither condition alone is sufficient. Messages shall be considered invalid or voidable if deterministic replay diverges from the JPacks referenced at execution time.
2. **Deterministic Execution via the Regulatory VM**
   The Regulatory VM enforces compliance verification through deterministic replay. Upon message ingress, the receiving domain composes a transient, auditable superset of the relevant JPacks and re-executes the applicable Policy-DSL logic. Merkleized PoPC commitments embedded in cross-domain message metadata enable consistent reproduction of compliance outcomes across domains. The SRH timestamps and anchors these commitments to support synchronized inter-domain validation and post hoc auditability.
3. **Paradigm Shift: From Message Exchange to Verifiable Compliance**
   By integrating Policy-DSL and PoPC into cross-domain message semantics, SSI elevates interoperability from mere message exchange to verifiable regulatory compliance. Mutual recognition among sovereign participants is therefore grounded in reproducible, attestable policy outcomes rather than trust in delivery mechanisms alone. In cross-border clearing and settlement workflows, each state transition is thereby associated with a traceable legal basis and an auditable compliance fingerprint.

据此，SSI 协议强制执行以下合规特性：

1. **证明链完整性与双重最终性约束**
   互操作性引入的核心风险在于，若交易结果与监管源头之间的证明链断裂，将导致决策不可核验，进而与基于审计的监管体系相冲突。为规避此风险，每份消息均需生成关联的 PoPC 凭证，以佐证 JPack 法规集的完整性、司法辖区约束的有效性以及双重政策执行的结果。跨域交易的最终结算必须同时满足“账本最终性”与“政策最终性”；若回溯重放结果与原始法规要件集不符，该消息将自动判定为失效。
2. **监管虚拟机的确定性执行环境**
   监管虚拟机通过确定性重放强化合规鉴证：消息接入阶段，系统会自动构造一个临时且可审计的 JPack 执行环境，重新执行关联的 Policy-DSL 逻辑。通过在跨域消息元数据中嵌入 Merkle 化的 PoPC 承诺值，系统实现了合规结果的跨域一致性复现。主权中继枢纽（SRH）负责为此类承诺加盖时间戳并执行全局锚定，从而将跨域消息转化为政策原生的合规载体，确立了基于可验证证明的跨主权互认机制。
3. **从消息互换到合规互认的范式转移**
   通过将 Policy-DSL 与 PoPC 深度集成至跨域消息语义中。SSI 将互操作性从单纯的消息交换，提升至可验证的监管合规层面。主权参与方之间的相互承认，由此根植于可复现、可鉴证的政策结果，而非仅依赖对传输机制的单方面信任。在跨境清算与结算流程中，每一项状态转换均关联着可溯源的法律依据，以及具备审计效力的合规指纹。

CHAPTER A8.

Transparency and Privacy:

Institutional Boundaries in a Verifiable System

A8. 章节

透明与隐私：

可验证体系中的制度性边界

Abstract:

In sovereign-level settlement infrastructures, verifiability functions simultaneously as the foundation of trust and as a design constraint. The system must therefore establish clear institutional boundaries between audit transparency and the necessary protection of sensitive data.

Traditional financial infrastructures rely on institutional trust and ex post supervisory review. Many details required for audit purposes are not disclosed at the system layer, because regulatory frameworks presume that authorized authorities possess statutory powers of penetrative access. Under the paradigm of verifiable execution enabled by sovereign distributed ledger systems, however, the locus of trust is fundamentally reconfigured. The authenticity and compliance of cross-domain interactions must be independently reproducible by any authorized verifier. Proof thus ceases to serve merely as an internal record and instead becomes a prerequisite for cross-sovereign cooperation: it must support transferability, deterministic recomputation, and formal adjudication.

A critical baseline principle must therefore be made explicit: verifiability is not equivalent to unrestricted data exposure. Any attempt to achieve transparency by disseminating raw transactional or identity data immediately collides with the institutional red lines of sovereign collaboration. Cross-border settlement processes involve not only personal privacy, but also commercial confidentiality, financial intelligence, supervisory strategies, and sovereignty-sensitive information. Such data does not acquire legal legitimacy for transnational disclosure solely by virtue of audit requirements. Jurisdictions impose stringent and non-uniform obligations concerning data minimization, purpose limitation, and cross-border transfer controls. Systems that depend on large-scale propagation of raw data to achieve auditability inevitably amplify compliance risk and political friction as they scale.

Accordingly, the central objective of this chapter is the construction of institutional transparency: the disclosure of the minimal necessary information required to provide verifiers with cryptographically conclusive proof that rules were executed under the correct jurisdiction, temporal context, and policy version, and that resulting outputs achieved settlement finality. Transparency thus becomes a mechanism for enforcing credible constraints, while privacy - subject to the satisfaction of verifiability requirements - strictly bounds information exposure within the overlapping limits permitted by regulatory and audit frameworks.

This chapter therefore focuses on proof engineering under sovereign and legal constraints: the design of mechanisms for proof generation, handling, and disclosure that simultaneously support cross-domain auditing and dispute adjudication while remaining compatible with heterogeneous data-protection regimes. This includes the systematic integration of techniques such as proof minimization, controlled redaction, cryptographic anchoring, and selective disclosure.

This represents the critical transition of verifiable systems from technical feasibility to institutional practice.

（本章摘要）

在主权级结算体系中，可验证性既是信任的基础，也构成设计约束：系统必须在审计透明与数据必要保护之间，建立清晰的制度界限。

传统金融基础设施的运行依赖机构信任与事后审查。审计所需的许多细节无需在系统层面公开，因为制度默认了监管者拥有法定的穿透式调阅权。而在 SSI 构建的“可验证执行”范式中，信任的重心发生了转移：跨域协作的真实性与合规性，必须能让任何授权方独立复验。自此，证明不再仅是内部留痕，而是转变为跨域协作要件：它必须具备可传递、可复算、可裁断的制度化能力。

然而，我们必须明确一个底线原则：可验证性绝不等于授权数据的无限暴露。任何试图通过广播原始数据来营造“透明”的做法，都会即刻触碰主权协作的制度红线。跨境结算涉及的不只是个人隐私，还包括商业机密、金融情报、监管策略与主权敏感信息。这些信息绝不因为审计需要，就自动获得跨境披露的合法性。各司法辖区对数据最小化、目的限定与跨境流动都有严格且不统一的合规要求。如果一套系统必须依赖原始数据的广泛传播来实现审计，其规模越大，所诱发的合规风险与政治摩擦就越不可控。

因此，本章的核心是构建制度性透明：以最小必要的信息披露，为验证者提供证明，证明规则在正确的辖域、时间与版本下已被执行，且其输出的结果具备结算终局效力。透明于是成为构建可信约束的过程，而隐私则在满足可验证性的前提下，将信息暴露严格限定在合规与审计双重逻辑所共同允许的框架内。

本章将聚焦于主权与法律约束下的证明工程：如何设计证明的生成、处理与披露机制，使其既能支撑跨域审计与争议裁决，又能与多元的数据保护制度逻辑兼容?这涉及证明的最小化构造、可控脱敏、哈希锚定与选择性披露等机制的系统化集成。

这是可验证体系从技术可行性迈向制度实践的关键跨越。

A8.1

The Failure Path of Excessive Transparency:

Log-Centric Design, Full Disclosure, and the Collapse of Compliance

过度透明的失败路径：

日志化、全量披露与合规性失效

Reagan and Gorbachev Sign Missile Treaty and Vow to Work for Greater Reductions, 1987, David K. Shipler, nytimes.com

"Trust, but verify."
"信任，但要验证。"

— Russian proverb, popularized by Ronald Reagan. 俄国谚语，由罗纳德·里根推广使用

Equating verifiability with expanded data disclosure represents one of the most hazardous engineering instincts in sovereign settlement infrastructures. Its common manifestation is the attempt to render system behavior "fully transparent" by recording and publicly exposing complete transaction contents, operational logs, and rule-execution traces. This reduction of verifiability to data visibility systematically produces three layers of structural failure.

First Failure: Logging Does Not Constitute Proof

Operational logs exist to support system runtime and troubleshooting; they are incidental byproducts of execution. Proof, by contrast, exists to support responsibility attribution and formal adjudication, and must therefore be intentionally structured. The distinction does not lie in the volume of recorded information, but in whether outputs satisfy strict constraints of deterministic replayability and cryptographic anchoring.

将可验证性等同于更多数据披露，是主权结算体系中最危险的工程直觉之一。它的典型表现，是试图通过记录并公开完整的交易细节、操作日志与规则执行路径，使系统行为"完全可见"。这种将可验证性简化为数据可见性的做法，将直接导致三重系统性失效：

第一重失效：日志化不等于证明化

日志服务于系统运维，是运行的副产物；证明则面向责任裁定，必须是结构化的输出。两者的根本差异，不在于记录的详略，而在于是否能满足可复算、可锚定的刚性约束。日志常混杂着非确

Logs routinely intermix non-deterministic intermediate states, diagnostic artifacts, and implementation-specific details, making consistent reproduction across software versions inherently unstable. More fundamentally, they lack a definition of minimal completeness for external verifiers: third parties cannot determine which fields constitute materially relevant facts, which represent engineering noise, or whether records have been selectively truncated or curated. The paradoxical outcome is that broader disclosure expands, rather than reduces, the interpretive surface for dispute. Verifiability does not emerge from data accumulation.

Second Failure: Direct Incompatibility Between Full Disclosure and Data-Protection Regimes

Participants in sovereign DLT systems operate across heterogeneous legal jurisdictions that uniformly enforce principles of data minimization, purpose limitation, and controlled access. Full disclosure transforms information that could otherwise remain confined within sovereign domains into normalized cross-border circulation, converting isolated compliance risks into systemic institutional exposure.

As operational scale increases, the expanding data surface rapidly outpaces the feasibility of managing authorization boundaries, retention constraints, and erasure obligations. Once leakage, misuse, or regulatory breach occurs, liability chains propagate transnationally, progressively eroding institutional credibility and long-term system viability.

Third Failure: Excessive Transparency Generates Sovereign Information Leakage and Structural Power Asymmetry

Within cross-sovereign collaboration, informational visibility itself constitutes strategic leverage. Full exposure of transaction flows, risk-control thresholds, and regulatory trigger conditions effectively reveals national enforcement postures, financial sensitivities, and macro-risk preferences to the global competitive environment.

The deeper structural contradiction arises from inherently asymmetric disclosure capacities among participants. **Jurisdictions constrained by strict institutional obligations are often compelled to disclose more, while actors with regulatory flexibility or technical dominance retain fine-grained control over outbound information**. When system design implicitly equates increased disclosure with

定性的中间状态与调试细节，在不同版本的系统间难以稳定复现。更关键的是，它缺乏对外部验证者的“最小完备性”定义：外部验证者无法判断哪些字段构成关键事实、哪些属于工程噪声，亦无法确认日志是否被选择性截取。结果是系统披露越多，争议的解释空间反而越大。真正的可验证性，并未在数据洪流中浮现。

第二重失效：全量披露与数据保护法规的直接冲突

主权体系参与者分属于不同司法辖区，各法域普遍遵循数据最小化、目的限定与访问控制原则。全量披露使原本可被约束在主权域内的数据，转变为常态化的跨境传播，将个案合规风险提升为结构性的制度风险。随着系统规模的扩大，数据面越广，越难以满足跨域授权、限期留存、删除权响应等刚性要求。一旦发生数据泄露或滥用，责任链条将跨域蔓延，最终侵蚀系统的制度公信力与可持续性。

第三重失效：过度透明导致主权信息外溢与结构性不对称

在跨主权协作中，信息可见性本身就是一种战略权力。交易流向、风控阈值、监管触发模式等数据一旦全量暴露，无异于将一国的金融态势图、执法敏感区乃至宏观风险偏好，置于全球博弈的显微镜下。更深层的矛盾在于，各参与方在信息披露的权能与意愿上存在天然的不对称：**受制度刚性约束的一方往往被迫披露更多，而具备制度柔性或技术优势的一方则可精密控制信息出口**。若系统设计隐含“披露越多、可信度越高”

increased credibility, it hard-codes this asymmetry into permanent competitive disadvantage. The more constrained participants incur higher compliance burdens while simultaneously surrendering strategic autonomy.

Such an imbalanced structure is inherently unstable. Its long-term outcomes converge either toward network hollowing, where collaboration persists only nominally under dominance by a small number of powerful actors, or toward the reintroduction of centralized authorities to rebalance information rights. Both trajectories fundamentally contradict the premise of polycentric, sovereign interoperability.

In sovereign settlement contexts, expanded disclosure does not produce verifiability. Instead, it accelerates systems toward institutional unsustainability, simultaneously undermining trust formation and amplifying irreducible regulatory and geopolitical risk.

Verifiability must therefore be conceptually reconstructed. Transparency should not seek to make data visible; it must seek to render critical facts cryptographically certain. Genuine auditability means that authorized external verifiers can, within institutionally defined permissions, conclusively validate the core determinants of settlement finality and responsibility attribution. The value of transparency lies not in informational breadth, but in the provision of enforceable, verifiable constraint.

Accordingly, the remainder of this chapter adopts minimal exposure as a foundational design principle and systematically addresses the following questions:

- What indispensable elements must a proof contain?
- How should proofs be structured through layered composition?
- How can cryptographic anchoring and desensitized summaries enable verification without disclosure?
- How can conditional revelation be employed for dispute resolution and regulatory access?

The objective is not to reduce transparency, but to elevate it from low-dimensional data exposure into verifiable structural constraint - enabling sovereign DLT systems to scale while maintaining institutional legitimacy and long-term operational sustainability.

的逻辑，便会将这种天然不对称固化为制度性的博弈劣势。弱势方不仅承担更高的合规成本，更在战略层面陷入被动。这种权力失衡的结构难以维系。其结果，要么是协作网络退化为少数强权主导的象征性框架，参与度持续流失；要么是不得不引入一个新的中心化权威来重新分配信息权利。而这，已完全背离了多中心化互操作的初衷。

综上，在主权级结算语境中，更多披露不仅无法通向可验证性，反而是一条加速系统走向不可持续的歧途。它既无法构建真正的可信根基，又注定会积累难以消解的合规与政治风险。

因此，我们必须重构“透明”的指向：它不应是让数据“被看见”，而应致力于让关键事实“被确信”。真正的可审计性，意味着外部验证者能在制度划定的权限范围内，对决定结算终局与责任归属的核心要素形成确证。透明度的价值，不在于呈现细节的广度，而在于提供可验证的约束力。

本章后续将以最小暴露原则为根本约束，系统阐述以下问题：

- 证明应包含哪些不可或缺的要素？
- 如何通过分层结构组织证明？
- 如何借助哈希锚定与脱敏摘要实现可验证性？
- 如何在必要时通过条件披露完成争议处置与监管调阅？

这一路径的关键，不在于降低透明度，而在于将透明从低维的数据暴露升维为可验证结构，使系统在扩展规模的同时，始终保持制度的可接受性与运行的可持续性。

A8.2

The Principle of Minimal Exposure: Necessary Elements of Verifiability

Since excessive transparency is infeasible, the question necessarily converges to a minimal form: under the constraint of not disclosing raw data, what is the minimal and sufficient information set that enables independent verification? The objective of transparency thus shifts from displaying data to proving facts. Proof design, in turn, shifts from recording detail to establishing a clear, enforceable boundary of disclosure.

This chapter therefore adopts the principle of minimal exposure as a foundational constraint for proof design. Its purpose is not merely information compression, nor a blanket prioritization of privacy, but the institutional definition of a necessary-and-sufficient disclosure boundary. Along the default path, the system discloses only those elements required to support cross-domain consistency verification and responsibility anchoring. Raw data, sensitive fields, and inferable context should, to the maximum extent feasible, remain within the local sovereign domain or be placed under strictly controlled conditional-disclosure mechanisms. Higher-resolution disclosure is activated only when strictly required, such as for dispute resolution, supervisory investigation, or authorized audit, and only pursuant to explicit institutional authorization.

Implementing this principle requires a clear separation between two fundamentally different categories of information.

The first category is raw business data: the identity details of participants, account identifiers, commercial context, contractual terms, source-of-funds documentation, and related materials. Such data may be indispensable for domestic compliance determinations by executing parties, but it is typically not a necessary input for cross-domain verifiers to confirm settlement finality and rule-consistent execution.

The second category is verifiable facts required for audit. What

最小暴露原则：可验证性的必要要素

既然过度透明并不可行，核心问题得以收敛：在不暴露原始数据的前提下，支撑独立验证的最小充分信息集是什么?透明性的目标已从展示数据转向证明事实。证明设计的任务，也因此从记录细节，转变为划出一条明确的、可执行的暴露边界。

本章据此确立最小暴露原则，作为证明设计的根本约束。该原则的核心并非简单的信息压缩或隐私优先，而是在制度层面寻求必要且充分的暴露边界：在默认路径上，系统仅暴露足以支撑跨域一致性与责任锚定的关键要素；而原始数据、敏感字段及可被推断的上下文，应尽可能保留在本地主权域内，或置于严格受控的条件披露机制之下。只有在争议处置、监管调查或授权审计等必要场景下，才依据制度授权，启动更高层级的定向披露。

落实这一原则，首先必须厘清两类本质不同的信息：

第一类是业务原始数据。包括交易参与方的身份细节、账户信息、商业背景、合同条款、资金来源凭证等。这些信息对于交易执行方的合规判断可能至关重要，但对于跨域验证者而言，它们通常并非验证结算终局性与规则一致性的必要输入。

第二类是审计所需的可验证事实。验证者真正

verifiers require is not raw detail, but a set of constraints that can be independently replayed. This includes: *when the cross-domain event was evaluated under which version boundary of the rule system; which abstracted attribute commitments represented the inputs; which deterministic conclusions were produced by rule execution; and how those conclusions were cryptographically bound to subsequent confirmations of settlement finality.* In other words, verification is not about "whether all details were visible", but whether "the required rule path was followed under the applicable conditions".

Accordingly, sufficiency for verification should not be measured by field count, but by whether disclosed proofs satisfy three institutional requirements:

1. **Rule determinacy**: verifiers can confirm the semantic content and version boundary of the rules applied - i.e., under which rules execution occurred at the time.
2. **Input integrity**: verifiers can confirm that execution inputs were semantically complete and untampered with - i.e., on what asserted facts the determination was based.
3. **Output binding**: verifiers can confirm a non-separable proof binding between execution conclusions and settlement actions - i.e., why a given settlement confirmation is valid in proof.

Only when these three requirements are satisfied simultaneously can proofs provide a trusted basis for cross-domain collaboration without requiring raw-data disclosure.

From an engineering perspective, minimal exposure shifts proof design from recording factual detail to recording verifiable constraints. Verifiability should be constructed from structured commitments rather than direct data output. A reasonable minimal proof set typically includes, while avoiding direct exposure of sensitive fields, fingerprints of rule versions and key parameters, identifiers of execution environments and issuers, commitments or summaries over input attributes, verifiable constraints over conclusions and key decision branches, and cryptographic anchoring relationships to subsequent settlement events.

The common property of these elements is that they allow verifiers to assess consistency without access to raw inputs and, where necessary, to obtain higher-resolution information through controlled mechanisms for dispute resolution, without exposing sensitive data to irrelevant parties along the default path.

It should be emphasized that **minimal exposure does not deny**

需要的，并非原始细节，而是能够被独立复验的约束集合。它包括：*该跨域事件在何时、被纳入何种版本的规则体系；其输入被抽象为哪些可验证的属性摘要；规则执行得出了何种确定的结论；该结论如何通过密码学绑定至后续的结算终局性确认*。换言之，验证者验证的不是"是否看到了所有细节"，而是"是否遵循了当时必须执行的规则路径"。

因此，足够被验证的信息不应以字段多寡衡量，而应满足三项制度性要求：

1. **规则确定性**：验证者能确认执行所依据的规则语义与版本边界（即"当时按什么规则执行"）；
2. **输入完整性**：验证者能确认执行输入在语义层面完整且未被篡改（即"当时基于什么事实做判断"）；
3. **输出绑定性**：验证者能确认执行输出与结算动作之间存在不可拆分的证明绑定（即"为何该结算确认在证明上成立"）。

只有同时满足这三项要求，证明才能在不暴露原始数据的前提下，承担跨域协作的可信基础。

工程实现上，最小暴露原则推动证明设计从记录事实细节转向记录可验证的约束。可验证性应建立在结构化承诺之上，而非数据直出。一个合理的证明最小集合通常包括（同时应避免直接暴露敏感字段）：规则版本与参数指纹、执行环境与签发主体标识、输入属性的承诺或摘要、执行结论与关键分支的可验证约束、以及与后续结算事件的哈希锚定关系。

这些要素的共同特点是：它们允许验证者在不接触原始输入的情况下判定一致性，并在必要时通过受控方式补充更高分辨率信息以解决争议，而无需在默认路径上向无关方暴露敏感数据。

differentiated information-resolution requirements across risk levels and scenarios. Operational compliance often requires risk-based tiering: low-risk activity may rely on coarse-grained attribute proofs; medium- and high-risk activity may require finer-grained proofs and may, in narrowly scoped cases, trigger conditional disclosure of specific fields. Regardless of scenario variation, however, the principle remains binding. The system must first define the lowest necessary proof form on the default path, and then specify explicitly under which trigger conditions, through which authorization mechanisms, and to which parties higher-resolution disclosure may occur. Tiered disclosure is the dynamic implementation of minimal exposure, not an exception to it.

At the intersection of institutional design and engineering practice, minimal exposure must be concretized as a verifiable boundary. For sovereign-level settlement systems, minimal verifiable proof is not the compressed recording of all "relevant" information; it is the retention - on the default collaboration path - only of elements indispensable to cross-domain consistency verification and responsibility anchoring. Concretely, proofs must explicitly include:

1. **Rule-boundary traceability**: verifiable fingerprints of rule versions and key parameters.
2. **Execution-subject authenticity**: identities and authorization sources of executing parties and execution environments.
3. **Input-condition commitment**: complete, non-separable semantic commitments over input conditions, preventing selective deletion or alteration.
4. **Output-binding provability**: a definite, non-repudiable binding between execution conclusions and subsequent settlement or state-transition finality.

Conversely, the principle delineates information that should not appear by default. The default proof path should exclude: raw personally or commercially identifying information; background materials without direct causal relevance to the settlement at issue; and redundant fields that enable reverse inference of behavioral patterns, business strategies, or regulatory parameters. Even if such information is relevant to domestic compliance assessment, it should not systematically spill over due to cross-domain verification requirements.

This positive–negative boundary is grounded not in engineering convenience, but in the long-established principle of data

需特别指出，**最小暴露原则并不否认不同风险等级与场景对信息分辨率的差异化需求**。现实合规往往要求基于风险进行分级审查与披露：低风险业务可使用粗粒度属性证明；中高风险业务则需更细粒度证明，甚至触发特定字段的条件披露。但无论场景如何变化，最小暴露原则仍构成约束：系统应先定义默认路径上的最低必要证明形态，再明确在何种触发条件下、以何种授权方式、向何种对象披露更高分辨率信息。分级披露是最小暴露原则的动态实现，而非对其的例外豁免。

在制度与工程交汇处，最小暴露原则必须具体化为一条可检验的边界。对于主权级结算体系而言，最小可验证证明并非对一切相关信息进行压缩记录，而是在默认协作路径上，仅保留那些对跨域一致性验证与责任锚定不可或缺的要素。具体而言，证明必须明确包含：

1. **规则边界可定位**：规则版本与关键参数的可验证指纹；
2. **执行主体可认证**：执行主体与执行环境的身份与权限来源；
3. **输入条件可承诺**：对输入条件形成完整且不可拆分的语义承诺，确保其未被选择性删改；
4. **输出绑定可证明**：执行结论与后续结算或状态变更之间存在确定、不可否认的绑定关系。

与此同时，该原则也明确划定了不应默认出现的信息。系统在默认路径下不应包含：可识别个人或企业的原始身份信息；与本次结算缺乏直接因果关系的背景材料；可用于反向推断行为模式、商业策略或监管参数的冗余字段。这些信息即便在本土合规判断中有意义，也不应因跨域验证需求而系统性外溢。

minimization within data-protection and financial compliance frameworks[1]. Institutional legitimacy does not depend on informational breadth, but on the system's ability to constrain exposure while satisfying verifiability - demonstrating that any cross-domain data flow is necessary for verification and no more than necessary. Only with this boundary clearly specified can layered proof structures, conditional-disclosure mechanisms, and lifecycle governance be built on a stable institutional foundation.

Once the principle is operationalized, the tension between transparency and privacy shifts from debates about how much data to disclose to an engineering question about how proof structures should be designed. The system no longer trades full exposure for trust; instead, *it demonstrates through verifiable constraints that rules were followed and settlement finality is legitimate even when raw data remains undisclosed.* Only under such a proof paradigm can sovereign settlement infrastructures achieve the transparency required for large-scale collaboration while preserving the privacy and compliance acceptability necessary for long-term operation.

这一正反边界的划定，其依据并非工程便利，而是数据保护与金融合规框架中早已确立的数据最小化原则 [1]。主权级结算体系的制度正当性，不取决于信息覆盖的广度，而在于能否在满足可验证性的同时，严格约束暴露范围，使任何跨域流动的信息都能被证明“为验证所必需，且未超出验证所需”。只有在这一边界被清晰界定的前提下，后续的分层证明结构、条件披露机制与生命周期治理，才具备稳定的制度基础。

当这一原则落地后，透明与隐私之间的张力，便从公开多少数据的争论，转向证明结构如何设计的工程命题。系统不再以全量暴露换取可信，而是凭借可验证的约束集合证明：*即使无法看见原始数据，你仍能确信我未偏离规则；即使敏感信息不越境，你仍可复验结算终局性的正当性*。只有在这样的证明观之下，主权级结算体系才能同时获得规模化协作所需的透明度，以及长期运行所必需的隐私与合规可接受性。

A8.3

Layered Proof Expression:
Desensitized Summaries, Cryptographic Anchoring, and Conditional Visibility

证明的分层表达：
脱敏、哈希锚定与条件可见性

The principle of minimal exposure clarifies the objective. The remaining problem is structural: how can cross-domain verifiability be achieved while systematically avoiding full disclosure?

In sovereign settlement infrastructures, proof cannot be carried

最小暴露原则明确了目标，随之必须解决证明的结构问题：如何在实现跨域可验证的同时，系统性地避免全量披露？

by a single artifact, file, or log stream, because verification requirements are inherently tiered. In routine operation, participants typically need only confirm that a transaction was executed under the applicable policy version and remains traceable. In the minority of cases, such as audits, investigations, or dispute resolution, higher-resolution information may be required to re-examine specific details.

If these requirements are collapsed into a single proof carrier, system design becomes trapped in a false binary: either excessive disclosure becomes the default, or verification becomes insufficient when escalation is necessary. A layered proof architecture resolves this tension by separating default verifiability from conditional deep verification, thereby preserving institutional acceptability at scale.

Layering is not a simple partition of the same proof material. Rather, it assigns distinct visibility boundaries to different verification objectives. An operable layered structure should define, at a minimum, the following tiers:

1. **Default visibility tier**: the minimal information that must traverse the cross-domain path to support independent verification under standard permissions;
2. **Abstract commitment tier**: desensitized and semantically refined attribute commitments that allow verifiers to confirm condition satisfaction without access to underlying content;
3. **Conditional disclosure tier**: institutionally authorized release of higher-resolution information to designated parties, with the disclosure action itself remaining verifiable and accountable.

Within this structure, cryptographic anchoring and desensitized summaries are not auxiliary privacy tools; they are foundational proof primitives.

Cryptographic anchoring separates existence and consistency from content visibility. By producing deterministic commitments over raw inputs, key state transitions, or rule-execution conclusions, the system can prove, without revealing content, *that certain facts were fixed at a specific time and cannot be substituted or altered during later verification*. The system does not offer "what can be seen", but rather "what cannot be rewritten after the fact". This property is central to cross-sovereign trust, precisely because it eliminates the space for ex post reinterpretation and selective reconstruction.

在主权级结算体系中，证明无法由单一文件或日志条目承担全部功能。因为验证需求天然具有层次性：

- **常规场景**：绝大多数情况下，参与方仅需确认该交易已在当时的规则下正确执行且可追溯；
- **争议场景**：仅在审计、调查或纠纷处置等少数情况下，才需调用更高分辨率的信息来复核细节。

若将两类需求混于同一载体，系统将陷入两难：要么默认暴露过多，要么在必要时证明不足。分层证明架构通过将默认可验证性与条件式深度验证相剥离，确保系统在规模化运行中仍能保持制度可接受性。

证明分层并非简单的逻辑切分，而是基于不同的验证目标，为各层设定清晰的可见性边界。一套可操作的分层结构，同时界定以下三层：

1. **默认可见层**：哪些信息必须在跨域路径上公开，以构成最小化的独立确信；
2. **抽象承诺层**：哪些信息应被脱敏或提炼为属性承诺，使验证者只能判定是否满足条件，而无法窥探具体内容；
3. **条件释放层**：在何种授权与审计框架下，允许向特定对象释放更高分辨率信息，且释放行为本身可被追溯。

在这一框架中，哈希锚定与脱敏摘要不再是附加的隐私增强技巧，而是证明分层的基础构件。哈希锚定的本质，在于将存在性与一致性从内容可见性中分离。通过对原始输入、关键状态或输出结论生成确定性承诺，系统可在不公开内容的前提下，向外界证明：*某些事实已在特定时点被固定；其在后续验证中不可被篡改或替换*。它提供的不再是“你看见了什么”，而是“你可以确信我无法事后篡改什么”。对主

Desensitized summaries enable verifiers to reconstruct the logical trajectory of rule execution without accessing sensitive details. They are not mere field masking; they are semantic refinement: transforming identity attributes, commercial data, or sovereignty-sensitive parameters into verifiable statements that preserve compliance meaning while preventing unnecessary disclosure.

In practice, a verifier may need to confirm that a subject satisfies a specified KYC tier, that a transaction falls within a defined compliance category, or that a source-of-funds process met prescribed due diligence requirements - without learning names, addresses, identification numbers, or full contractual text. The objective is to make rule execution replayable at the level of decision logic rather than at the level of original documentation. **Institutionally, third-party verification must center on verifiable attributes, not raw personal or commercial data**.

Cryptographic anchoring and desensitized summaries, however, do not exhaust real-world requirements. In dispute handling or supervisory investigation, access to specific details may be unavoidable. This introduces the third tier: conditional visibility, the proof-level realization of conditional disclosure.

Conditional visibility is not discretionary disclosure. It is an institutionalized triggering mechanism. When defined conditions are satisfied, such as arbitration, law-enforcement requests, supervisory inspection, or risk escalation, the system may, within an explicit authorization scope, release higher-resolution information to designated parties. Crucially, the disclosure itself must leave verifiable traces so that its scope, recipient, timing, and justification are auditable after the fact. The system must therefore prove not only that policy execution was correct, but also that disclosure was properly triggered and minimized.

A common misconception is to treat layered proofs as a simple public–private split. For sovereign settlement infrastructures, a more robust conception is to treat proof as an upgradable verification path:

- **Default path**: provides minimal, broadly applicable verification capabilities for high-frequency cross-domain collaboration;
- **Upgrade path**: releases additional information under strict conditions to resolve low-frequency but high-importance disputes.

To preserve replayability under escalation, tiers must be

权级系统而言，这类承诺的价值尤其关键，因为跨域信任的基石，恰恰在于消除事后解释与选择性披露的空间。

脱敏摘要旨在让验证者能够重构规则执行的逻辑脉络，而不必接触敏感细节。它超越简单的字段遮盖，是一种语义提炼：将身份信息、商业数据或主权参数，转化为具备验证价值却无窥探意义的属性表达。

例如，验证者只需确认：某主体已达到特定 KYC 等级、某交易归属于某一合规类别、资金来源已完成相应尽调流程。而无需知晓该主体的姓名、地址、证件号或合同全文。脱敏摘要的目标是使规则执行可被复现至决策逻辑层面，而非原始材料层面。**它的制度意义在于：第三方验证应围绕可验证属性展开，而非围绕原始个人数据展开**。

然而，仅有哈希锚定与脱敏摘要仍无法覆盖现实中的所有需求。在争议处置或监管调查等场景中，特定细节的调阅不可避免。这便引出了分层结构的第三个关键：选择性可见性，即条件披露的证明化实现。

选择性可见性并非随意的信息公开，而是一套制度化的触发机制。当特定条件满足时（例如争议仲裁、执法请求、监管检查、风险升级），系统可在授权范围内向特定对象释放更高分辨率信息，并确保披露行为本身留下可验证的痕迹，使披露范围、对象、时间及理由均可被事后审计。这意味着系统不仅证明规则被正确执行，还需证明披露为正当触发且最小化实施 。

一种常见误解是将证明分层视为公开层与私密层的二元对立。对于主权级结算体系，更稳健的思路是将证明视为一条可升级的验证路径：

- **默认路径**：提供最小且普适的验证能力，支撑高频跨域协作；

cryptographically linkable. Higher-resolution disclosures must be demonstrably expansions of previously anchored commitments, not ex post assembled narratives. Cryptographic anchoring provides precisely this linkability, ensuring that escalation refines prior commitments rather than rewriting history.

Under such a layered design, auditing practice also changes. Traditional auditing often presumes that rigor requires broader material access. In a verifiable DLT system, auditing begins with a structural examination: whether proofs are complete, consistent, linkable, and upgradeable. In most cases, auditors need only confirm:

- that policy versions are correctly bound;
- that executing subjects and environments are authenticable;
- that input commitments are complete;
- that conclusions are non-separably bound to settlement finality events;
- and that any escalation follows institutionalized triggers and authorization.

Only when structural verification cannot resolve doubts does review proceed to higher-resolution materials. This does not weaken audit rigor; it reorients audit from voyeuristic inspection toward structural verification, maintaining strong constraints while protecting privacy and sovereign boundaries.

In summary, layered proof expression is not a compromise but a necessary architecture for scaling sovereign verifiable systems. It achieves this by:

- **Desensitized summaries**: shifting verification from raw data to verifiable attributes;
- **Cryptographic anchoring**: shifting trust from content visibility to non-repudiable consistency commitments;
- **Conditional visibility**: placing necessary detail access within an institutionalized and accountable framework.

Only within such a proof structure does transparency mean demonstrability and privacy mean minimal exposure under verifiable constraint, enabling cross-domain collaboration to remain institutionally acceptable and politically sustainable over the long term.

- **升级路径**：在严格条件下释放额外信息，解决低频但高重要性的争议。

为确保升级可行性且不破坏可重放性，各层证明之间必须具备可验证的链接：高层级披露的细节必须能证明其对应于此前已锚定的承诺，而非事后拼凑的解释材料。哈希锚定所提供的正是这种可链接性，使后续披露成为对既有承诺的展开与证实，而非对历史的改写。

在这种分层结构下，审计形态也将迭代。传统审计常以获取更多材料为前提，而在本体系中，审计首先是对证明结构是否完备、一致、可升级的审视。在多数情况下，审计者只需确认：

- 规则版本是否被准确绑定；
- 执行主体是否可被认证；
- 输入承诺是否完整；
- 结论是否与结算事件不可拆分；
- 升级披露是否遵循制度化触发机制。

仅当结构性检查无法消除疑点时，才进入更高分辨率的材料调阅。这并非降低审计强度，而是将审计从窥视转向结构式验证，在保护隐私与主权边界的同时，保持对系统行为的强约束。

综上，证明分层并非折中，而是主权级可验证体系实现规模化运行的必要架构。它通过：

- **脱敏摘要**：将验证对象从原始数据转向可验证属性；
- **哈希锚定**：将可信基础从内容可见性转向一致性承诺；
- **选择性可见性**：将必要的细节调阅纳入制度化、可追责的轨道。

唯有在这样的证明结构下，“透明”才意味着能够被证明，“隐私”才体现为在可验证约束下的最小暴露，从而使跨域协作在长期运行中，同时具备制度的可接受性与政治的可持续性。

A8.4

Replayable but Not Inspectable:

Boundary Conditions for Third-Party Verificationand Conditional Visibility

可重放而不可窥视：

第三方验证的边界条件

In verifiable systems, replayability is often treated as the highest-order property: any authorized third party should be able to recompute rule execution in an independent environment and thereby confirm the correctness of the outcome. When replayability is misconstrued as the reproduction of all underlying raw data, however, the system re-enters the failure path of excessive transparency, indeed in a stronger form, by implicitly equating audit rights with a perpetual entitlement to full informational access.

The core claim of this section is that **replayability concerns the deterministic reproduction of decision logic, not the reconstruction of full business reality**. Genuine replayability does not require third parties to handle raw data. Accordingly, the system must define explicit boundaries: which information verifiers require, what they are permitted to observe by default, which sensitive fields are prohibited, and under which institutional conditions higher-granularity verification materials may be authorized.

Replayability as Deterministic Semantic Reproduction

Replayability is a property of deterministic rule-execution semantics, not of data visibility. Determinism implies that, under the same policy version boundary, rule parameters, and abstracted inputs, any compliant execution environment will converge on the same conclusions and produce verifiable proofs consistent with the original outcome. The emphasis is on semantic consistency and recomputability, not on exposure of underlying materials.

Institutional transparency is achieved when authorized third parties can independently validate, at minimum, that:

- the rule version boundary applied at execution time is unambiguous;
- inputs were semantically complete and not selectively substituted;

在可验证性体系中，可重放往往被赋予最高权重：任何被授权的第三方，都应可以在独立环境中复算规则执行过程，从而确认结论的正确性。但若将其误解为复现全部原始数据，系统将重蹈过度透明的覆辙，甚至更甚：这无异于将审计权等同于对全量信息的持久索取权。

本节的核心论点是：**可重放的本质在于复现决策逻辑，而非再现业务全貌**。真正的可重放，并不要求第三方触及原始数据。系统因此必须明确：验证者究竟需要哪些信息、能够看到哪些内容、禁止接触哪些敏感字段，以及在何种条件下可被授权获取更高粒度的验证材料。

可重放的本质：是对规则执行语义的确定性复现，而非数据可见性。

确定性意味着：在相同规则版本、政策参数与抽象输入下，任何合规执行环境都将得出相同结论，并提供可验证的证明链。这一要求强调的是语义一致性与可复算性，而非输入材料的可见性。第三方验证者需要确认只要以下要素被独立复验，系统便实现了制度上的透明：

- 执行时所依据的规则版本是否明确且不可混淆；
- 输入是否完整且未被选择性替换；
- 执行过程是否遵循确定的语义逻辑；
- 输出是否与结算事件建立了不可拆分的绑定关系。

- execution followed deterministic rule semantics;
- conclusions are non-separably bound to settlement-finality events.

Minimal Verification Privilege: Constraints Over Materials

The minimal privilege set for third-party verification should be defined in terms of verifiable constraints rather than unrestricted access to materials. Verifiers require recomputable structures - not free-form inspection of raw fields. Along the default path, third-party verification should typically rely only on: locatable policy versions and key-parameter fingerprints; authenticated execution subjects and execution environments; commitments or summaries over input attributes; verifiable constraints over conclusions and critical decision branches; and cryptographic anchoring relationships to subsequent settlement events.

Under this model, inputs are presented as verifiable attributes rather than raw data, and outputs appear as verifiable conclusions rather than narrative reports. Assurance is obtained through recomputation and validation, not through inspection.

From Perceptual Transparency to Structural Transparency

"Replayable but not inspectable" does not weaken transparency; it elevates transparency from perceptual visibility to structural provability. In sovereign settlement infrastructures, this is the only sustainable form, because cross-domain collaboration cannot be built on indefinite exposure of sensitive data. The system must provide a verification mode that imposes strong external constraints on execution behavior while preventing cross-border propagation of raw sensitive information. This is the proof-layer extension of the minimal auditable closed loop: the closed loop requires a verifiable relationship between execution and proof, not the dissemination of underlying data.

Role Separation and Visibility Scopes

To make these boundaries operational, the system must distinguish actor categories and associated visibility scopes.

- **Routine verifiers**: cross-domain participants or relay hubs on the default collaboration path, whose objective is to confirm that transactions satisfy the compliance preconditions required for settlement.

验证的最小权限：约束优先于材料。

第三方验证的最小权限集合应围绕验证约束而非获取材料来设计。验证者需要的是可复算与核对的结构性要素，而非调阅的原始字段。具体而言，第三方验证在默认路径上只应依赖以下信息：可定位的规则版本与参数指纹、执行主体与执行环境认证信息、输入属性的承诺或摘要、执行结论及其与关键约束的可验证链接、以及与结算事件的锚定关系。在此，输入以可验证属性呈现，而非原始数据；输出以可验证结论呈现，而非叙述性报告。验证者通过复算与核对获得确信，而非通过窥视细节。

从感知透明到结构透明。

可重放而不可窥视并非削弱透明度，而是将其从感知层面看见更多转向结构层面证明更强。在主权级体系中，后者才是可持续的路径，因为它承认一个现实：跨域协作不可能建立在各方无限制暴露敏感数据的基础之上。系统必须提供一种验证方式，使得参与者能够在不扩散原始敏感信息的前提下，仍然接受外部对其执行行为的强约束。这也是最小可审计闭环在证明层面的延伸：闭环要求的是执行与证明之间的可验证关系，而非原始数据的外溢。

为使边界可执行，系统需在验证模型中明确区分三类角色及其可见性范围：

- **第一类是常规验证者**，即跨域参与方或中继枢纽在默认协作路径上的验证主体，其验证目标是确认交易或事件满足结算所需的合规前置条件。
- **第二类是授权审计者**，即在特定场景下

- **Authorized auditors**: entities empowered in specific scenarios to conduct deeper review, including sampling of attribute formation processes, higher-resolution analysis of execution paths, and investigation of potential abuse.
- **Law-enforcement and judicial authorities**: entities acting under statutory mandates for investigation, proof collection, and responsibility adjudication.

The default path need satisfy only the minimal verification requirements of routine verifiers. The requirements of authorized auditors and judicial actors are satisfied through conditional disclosure and authorization chains, and the disclosure acts themselves must be recorded as auditable, attributable events.

This separation establishes institutional boundaries for replayability: by default, replay verifies rule logic and abstract attributes without exposing raw data; only when defined conditions are met and authorization is complete may higher-granularity disclosure be triggered. The design mirrors layered proof structures and adheres to the minimal-necessity principle in data protection. Its deeper significance is to eliminate a persistent misconception: verification rights are not equivalent to panoramic data-access rights. Otherwise, audit mechanisms themselves become channels of privacy leakage and sovereign information spillover.

Risk-Based Disclosure: Alignment with Established Compliance Frameworks

Cross-border disclosure has long operated under risk-differentiated principles. This chapter does not introduce a novel doctrine, but aligns with established international compliance frameworks, including FATF's risk-based approach[2]. In practice, proportionality is often implemented unevenly across jurisdictions. The system therefore adopts an alignment rather than reconstruction strategy: it reuses established risk-assessment dimensions (such as value, frequency, and counterparty characteristics) and converts risk-control outputs into machine-executable disclosure logic, avoiding subjective redefinition of risk and instead emphasizing deterministic and verifiable compliance actions.

This risk-driven tiering already has clear regulatory precedents. For cross-border transfers, FATF's Travel Rule introduces a widely adopted threshold (USD 1,000 or EUR-equivalent), below which only baseline originator/beneficiary information is typically required, while higher-value or higher-risk patterns trigger enhanced retention and disclosure procedures[3]. The tiered disclosure mechanism here draws on this threshold logic rather than introducing arbitrary standards.

被授权进行更深度复核的主体，其验证目标可能包括对输入属性形成过程的抽查、对执行路径的更细粒度解释、以及对系统行为是否存在滥用的审计。

- **第三类是执法与司法主体**，验证目标是满足法定调查、取证与责任裁定需要。

系统在默认路径上只需满足第一类的最小验证要求，而后两类的验证需求必须通过条件披露与授权链条实现，并且必须把披露行为本身纳入可追责与可审计的轨迹之中。

三类角色划分的核心，是为可重放确立清晰的制度边界：默认情况下，重放仅验证规则逻辑与抽象属性，不触及原始数据；仅当满足特定条件且授权完备时，方可触发更细粒度的信息揭示。该设计不仅与证明分层结构同构，更坚守数据保护的最小必要原则。其深远意义在于杜绝一个根本性误解：验证权不等于数据全景浏览权。从而防止审计机制本身成为隐私泄露与主权信息外溢的渠道。

基于风险的信息披露：与现有合规框架的衔接。

跨境结算中的信息披露长期遵循基于风险差异化处理原则，这并非本系统独创，而是源于国际金融合规框架（如 FATF 的风险为本方法）[2]。值得注意的是，FATF《建议 1》所倡导的风险相称原则，在实践中常面临执行尺度不一的问题。为此，本系统在设计上采取了一种衔接而非重构的思路：直接沿用已形成的风险评估维度（如交易金额、频率、对手方属性等），将既有的风控输出转化为机器可执行的披露逻辑，从而避免系统自身陷入对风险的主观界定，聚焦于合规动作的确定性与可验证性。

这种风险驱动、分级披露的逻辑，在国际监管实践中已有明确先例。以跨境转账为例，FATF 在旅行规则中设定了一条广为接受的红

Accordingly, along default low-risk collaboration paths, the system generates and shares only the minimal proof set required for verifiability. When risk indicators cross predefined thresholds, the system transitions, under predefined rules, into conditional disclosure paths that provide higher-resolution attribute proofs or targeted compliance materials. Importantly, escalation does not imply indiscriminate publication. It entails graduated release of necessary information under risk-driven, scope-limited, purpose-specific conditions.

Conditional disclosure further concerns not only what may be revealed, but under what triggers and under whose authorization disclosure occurs. All disclosure acts must be recorded as auditable events, ensuring that any access beyond the default minimal-exposure scope has explicit triggers, authorization sources, and responsibility attribution. This aligns with FATF's emphasis on traceable and accountable risk responses and prevents risk mitigation from degenerating into uncontrolled information diffusion.

Finally, replayability must be distinguished from interpretive authority. Authorized third parties may recompute compliance conclusions, but should not possess unrestricted rights of reinterpretation. Interpretive latitude reopens the space for narrative contestation of rule application and proof meaning, a space that readily produces new disputes in cross-sovereign environments. The objective is not to enable each verifier to supply its own interpretation, but to ensure that all verifiers converge on the same conclusion within a unified proof framework. Replayability is therefore anchored in deterministic semantics and structured proofs, while minimal privileges, layered proofs, and conditional disclosure constrain information exposure within institutionally permissible boundaries.

In sum, replayability does not require exposing everything to third-party control. It requires enabling third parties to validate that the system did not deviate from rules without accessing sensitive detail. This is a core distinction between sovereign verifiable settlement infrastructures and traditional centralized audit regimes: structured proof replaces full disclosure; deterministic semantics constrain ex post interpretation; authorization chains bound necessary access. Together, these establish a scalable and sustainable institutional balance between transparency and privacy that remains compatible with data-sovereignty constraints.

线：1000 美元（或等值欧元）。低于此阈值的交易，通常只需传输最基础的身份与交易要素；一旦触及或超过该门槛，或出现高频、异常等风险特征，则须启动更严格的信息留存与披露程序 [3]。本系统在设计分级披露机制时，正是参考了这一已被广泛采用的阈值逻辑，而非自行设定任意标准。

因此，在默认的低风险协作路径下，系统仅生成并共享满足可验证性的最小证明集合；当交易金额、频率或其他风险指标达到既定阈值时，系统才会依据预先定义的规则，进入条件披露路径，提供更高分辨率的属性证明或合规材料。需要强调的是，这一升级过程并不意味着对所有信息的无差别公开，而是在风险驱动、范围受限且目的明确的前提下，逐级释放必要信息。

另外，条件披露不仅涉及披露哪些信息，还涉及在何种条件下、由谁被授权进行披露。相关披露行为本身必须被记录为可审计事件，以确保任何超出默认最小暴露范围的信息访问，都具有明确的触发依据、授权来源与责任归属。这一做法与 FATF 所强调的可追溯、可问责的风险响应机制保持一致，避免将风险应对转化为不受约束的信息扩散。

最后，必须明确区分重放能力与解释能力。第三方验证者虽可复算合规结论，却不应享有无限制的解释权。解释权意味着对规则适用、事实认定与证明意义进行重新演绎的空间，而这种空间在跨主权体系中极易催生新的争议。主权级系统的目标，并非让每个验证者给出自己的解释，而是使所有验证者在同一证明框架下达成一致的结论。为此，系统将可重放性锚定于确定性语义与结构化证明之上，并通过权限最小化、证明分层与条件披露，将信息窥视风险压制在制度允许的边界内。

综上所述，可重放并非将一切呈现给第三方审视，而是让第三方在不触及敏感细节的前提下，依然能够验证系统未偏离规则。这正是主权级可验证体系与传统中心化审计体系的根本分野：它以结构化证明取代全量披露，以确定性语义遏制事后解释，以授权链约束必要调阅，从而在透明与隐私之间，建立起一种可持续、可扩展且符合数据主权要求的制度平衡。

A8.5

The Proof Lifecycle:
Governance Boundaries Under Data-Protection Constraints

The preceding sections established the structural design of proofs in space, enabling a principled balance between transparency and privacy. For this design to remain institutionally sustainable, however, it must also be evaluated along the temporal dimension. The full proof lifecycle - from generation to retirement - must be compatible with the internal logic of global data-protection regimes.

Lifecycle governance is not merely a technical operational concern. It is an institutional prerequisite for sustained sovereign participation and durable cross-domain mutual recognition. The central tension is straightforward: data-protection regimes focus less on whether information exists and more on why it is retained, for how long, who may access it, when it must be disposed of, and how misuse is prevented.

Before specifying lifecycle mechanics, one foundational distinction must be stated explicitly: **proof immutability is not equivalent to perpetual readability of proof content**.

What data-protection and financial-compliance frameworks require to be retained over time is the verifiable capacity to confirm that relevant facts occurred and were not tampered with - not

证明生命周期：
数据保护语境下的治理边界

前述各节完成了证明的空间结构设计，使其得以在透明与隐私之间建立平衡。然而，若要该结构在制度中长久存立，就必须将其置于时间维度中考量：证明从生成到退场的完整生命周期，必须与全球数据保护法规的内在逻辑相容。

证明生命周期的治理，绝非单纯的技术运维，而是决定体系能否获得持续主权参与及跨域互认的制度性前提。其核心矛盾在于：数据保护法规关注的焦点，往往并非证明是否存在，而是为何保存、保存多久、谁可访问、何时销毁、如何防止滥用。

在展开生命周期的具体设计前，必须首先澄清一个根本性区分：**证明的不可篡改性，不等于证明内容的永久可读性**。

数据保护与金融合规框架所要求的长期留存，本质是事实曾确定发生且未被篡改的可验证能

the indefinite availability of raw sensitive information. This distinction is reflected in existing regulatory principles. For example:

- GDPR's storage-limitation principle requires personal data to be retained no longer than necessary for the purposes of processing[4].
- FATF guidance, while emphasizing record-keeping obligations, also points to proportionality and disposal mechanisms[2].

These frameworks do not reject ex post audit; they require systems to constrain retention scope and duration while still supporting audit and adjudication. From an engineering standpoint, this yields a core operational paradigm: content retires; commitments persist.

- **Commitments persist**: at the moment of execution, the system generates and anchors compact cryptographic commitments associated with rule execution and settlement finality (e.g., hashes, timestamps, and policy-version fingerprints). These commitments are non-identifying and minimal in size, yet remains sufficient to verify, even years later, under which policy boundary execution occurred and what deterministic conclusions were produced.
- **Content retires**: raw sensitive inputs supporting the determination (e.g., identity details and full documentation) remain readable only for the period necessary to complete processing purposes (e.g., settlement completion and the applicable dispute or audit window). After that period, technical controls, such as key destruction, access revocation, or cryptographic re-wrapping under restricted custody - remove such content from default accessibility.

This paradigm allows the system to satisfy two requirements that otherwise appear in conflict: long-term verifiability of historical facts and time-bounded protection of personal, commercial, and sovereignty-sensitive data. Proof-lifecycle governance is the process of translating this paradigm into executable and auditable technical rules.

It should be emphasized that lifecycle governance does not erase or conceal history. It applies differentiated preservation according to institutional function:

- Fact anchors and execution conclusions, as commitments supporting responsibility attribution and cross-domain state consistency, must persist on a long horizon, potentially indefinitely.

力，而非对原始敏感信息的无限期暴露。这一原则在现行法规中有明确依据：

- 欧盟《通用数据保护条例》（GDPR）第 5 条第 1 款第 (e) 项（存储限制原则）规定，个人数据的保存时间不得超过实现其处理目的所必需的期限 [4]。
- 金融行动特别工作组（FATF）建议在强调交易记录保存义务的同时，亦指出信息保存应符合比例原则，且应有明确的处置机制 [2]。

这些框架均不否定事后审计的必要性，而是要求系统在满足审计目的同时，严格约束数据的留存范围与期限。由此，在工程实践中衍生出“内容退场，承诺永驻”的核心范式：

- **承诺永驻**：在交易发生时，系统即生成并永久锚定与规则执行、结算终局性相关的密码学承诺（如哈希值、时间戳、规则版本指纹）。这些承诺体量极小、不含敏感信息，却足以在多年后独立验证当时依据何规、得出何果。
- **内容退场**：支撑当次判断的原始敏感数据（如身份细节、完整文书），则仅在实现处理目的（如结算、争议期审计）所必需的期限内保持可读。期满后，通过技术手段（如密钥销毁、访问权限撤销）使其退出默认可访问状态。

这一范式确保系统在时间线上同时满足两项看似冲突的要求：对历史事实的长期可验证性，与对个人及主权数据的最小化、限期化保护。证明生命周期的管理，正是将此范式转化为可执行、可审计技术规则的过程。

必须明确，证明的生命周期管理并非对历史的销毁或掩盖，而是根据信息的不同制度角色，实施差异化的保存策略：

- High-risk, identifiable raw content, once it has fulfilled its institutional purpose (e.g., domestic compliance determination or dispute adjudication), should progressively expire, be desensitized, or become accessible only through strictly governed escalation paths.

This approach is consistent with established compliance and privacy practices, including irreversible hashing, tokenization, and dynamic access-control regimes that preserve auditability while adhering to minimization and retention constraints.

Accordingly, the objective of lifecycle governance in this system is not to extend retention indiscriminately, but to define, with institutional clarity, the temporal role of each information category. The system must remain capable of supporting post hoc third-party replay verification while avoiding the cumulative privacy, compliance, and sovereignty-friction risks that arise from indefinite retention of sensitive content.

Primary Lifecycle Tension: Permanent Traceability Versus Bounded Data Retention

Sovereign verifiable settlement infrastructures typically require long-term stability and traceability of records, while modern data-protection regimes emphasize purpose limitation, minimization, and bounded retention periods. Across most jurisdictions, retention must serve a clear and necessary legal purpose, and excessive or indefinite storage is itself treated as a compliance risk. At the same time, cross-domain settlement requires accountability and dispute-resolution capacity, which in practice demands that proofs remain retrospectively usable for audit, arbitration, and judicial procedures over an adequate horizon.

Resolving this tension requires a more precise definition of immutability. Immutability should be understood as a rigid commitment to the integrity and consistency of generated proofs, not as a mandate that all associated information remain perpetually readable. Certain components of proof may safely retire under institutional rules; as long as their core commitments - cryptographic anchors and conclusion summaries - remain durable, the legal and technical force of the underlying facts remains intact.

Having established the principles of minimal exposure and layered proof expression, proof design must therefore extend into lifecycle governance. This is not mere data management. It is the institutional process of internalizing constraints - data protection obligations, audit requirements, and sovereign boundaries - into executable system rules. The objective is to maintain an

- 事实锚点与执行结论作为责任归属与状态一致的密码学承诺，须长期乃至永久存续。
- 高风险、可识别的原始数据内容，则在履行其制度使命（如完成合规校验、支持争议裁定）后，依据预设规则逐步失效或脱敏。

这一原则已在金融合规与隐私保护领域形成成熟实践：通过不可逆哈希、标记化技术或动态访问控制，在维系审计可行性的同时，严格遵循数据最小化与保存期限的监管要求。

因此，本体系中生命周期管理的核心目标，并非无条件延长所有数据的留存时间，而是清晰界定不同信息在时间维度上的制度使命，使系统既能支撑事后的第三方重放核验，又可规避因无限期数据保留所累积的隐私、合规与主权摩擦风险。

生命周期的首要矛盾：永久可追溯性与数据有界留存的对立。

主权级可验证体系往往追求记录的长期稳定与可追溯，而现代数据保护框架则强调目的限定、最小化与保存期限合理。多数司法辖区要求，数据留存必须具备明确、必要的法定目的，过度或无限期的保存本身即构成合规风险。然而，跨域结算所需的可追责性与争议处置能力，又天然要求证明具备足够的留存期与可回溯性，以应对审计、仲裁及司法程序。

化解这一矛盾的关键在于重新理解不可篡改的内涵：它应被定义为对已生成证明的完整性与一致性的刚性承诺，而非对所有关联数据必须永久可读的强制要求。证明的某些组成部分可以依据制度规则安全“退场”，但只要其核心承诺（哈希锚点、结论摘要）永久存续，其作为法律与技术事实的效力便始终成立。

institutional balance between long-horizon trustworthiness of proofs and timely retirement of sensitive information.

Principle One: Purpose-Driven Layered Retention

The first lifecycle principle is purpose-driven layered retention. Different proof tiers serve different institutional purposes. The minimal proof set used on the default verification path exists to support long-term traceability for cross-domain consistency and settlement finality. Higher-resolution materials that appear only under conditional disclosure are typically associated with supervisory investigations, dispute resolution, or judicial proceedings and are therefore more likely to contain personal, commercially sensitive, or sovereignty-sensitive content.

Under this structure, the system must define, with precision, which proof tiers require long-term preservation and which must progressively reduce accessibility - or, where legally required, undergo controlled expiration or deletion - once their purpose is fulfilled. Lifecycle governance is therefore not a uniform retention policy applied to all proofs; it is a structural and permission-based separation between long-term institutional needs and short-term operational needs.

Principle Two: Erasure as Control of Readability, Not Destruction of Consistency

A second core issue is how to interpret erasure within a verifiable system. In data-protection regimes, erasure rights are often framed as a strict requirement. Within sovereign settlement infrastructures, however, complete removal of historical traces is not feasible: it would eliminate the proof foundation necessary for reconciliation, audit, and dispute adjudication.

The workable resolution is to redefine erasure in layered terms. Erasure should be implemented as institutional control over content readability and access availability, rather than physical destruction of historical consistency. Proof commitments may persist as long-horizon structural anchors, while sensitive content exits default visibility through mechanisms such as key destruction, access revocation, controlled invalidation, or restricted re-wrapping. The institutional objective is not to erase the fact of execution, but to ensure legal non-identifiability and non-reusability of sensitive content outside lawful, purpose-bound access paths.

This approach aligns naturally with layered proof design: the system maintains cryptographic anchoring of historical facts while allowing highly sensitive details to transition from readable to conditionally readable to effectively unreadable, producing a

在确立了最小暴露与分层表达原则后，证明的设计必须进一步延伸至其完整生命周期的制度化治理。这并非单纯的技术数据管理，而是将数据保护、审计需求与主权边界等制度性约束，内化为证明系统可执行逻辑的关键环节。其核心在于实现证明的长期可信与信息的适时退场之间的制度性平衡。

因此，证明生命周期管理的第一原则应当是目的驱动的分层留存。

不同层级的证明对应不同的制度目的：默认可验证所需的最小证明集，其保存目的是支持跨域一致性与终局确认的长期可追溯；条件披露层所涉的高分辨率材料，其保存往往与监管调查、争议处置或司法取证相关，且更易触及个人信息与敏感数据。

在这一结构下，系统应清晰界定：哪些证明层级需长期保存，哪些应在目的达成后逐步降低可访问性，乃至在合规要求下实现可控删除或失效。简言之，生命周期治理不是对所有证明“一刀切”，而是将长期制度需求与阶段性操作需求在结构与权限上彻底分离。

第二个核心问题在于，如何在可验证体系中理解可抹除的真实意涵。

在数据保护框架下，删除权常被视为刚性要求。但在主权级结算体系内，将历史痕迹彻底清除并不可行，那将直接摧毁对账、审计与争议解决所需的证明基础。

真正的解决之道在于重新定义可抹除的层次：它应是对内容可读性与访问可得性的制度化控制，而非对历史一致性的物理销毁。这意味着，证明本身可以作为一种结构承诺被长期保留，但其承载的敏感信息，可通过密钥销毁或受控失效等方式，退出默认可见状态，达到法律意义上的不可再识别与不可再使用的标准。

sustainable equilibrium between compliance constraints and system trustworthiness.

Principle Three: Auditable Authorization and Access-Responsibility Trails

A third challenge concerns the auditability of access control and authorization. In many regulatory contexts, the questions "who accessed" and "was access necessary and lawful" are institutionally more sensitive than whether data was retained at all. To withstand compliance control and mitigate privacy and political risk, access and disclosure processes must themselves be incorporated into the proof framework. The system must demonstrate not only correct rule execution, but also that any access beyond the default scope was lawful, traceable, and minimized.

A sustainable design therefore maintains two interlocked trails over time:

1. **Business-fact trail**: the trace of transaction execution and settlement-finality state transitions;
2. **Access-responsibility trail**: a record of each viewing, copying, transmission, or export of proof materials, bound to an authorization basis, acting subject, timestamp, and declared access purpose.

Principle Four: Cross-Temporal Interpretability and Regulatory Adaptation

A fourth challenge is cross-temporal interpretability under evolving regulatory expectations. Data-protection rules evolve, privacy standards change, and national supervisory interpretations may shift. If proof structures cannot accommodate such evolution, systems face institutional risk in which historical proof is retrospectively questioned for legal adequacy.

Two frequently conflated concepts must therefore be separated: long-term existence of proof does not imply long-term readability of proof content. Long-term existence means historical consistency remains verifiable; long-term readability implies that raw content can always be fully decoded and interpreted in the future. For personal identity data, commercial confidentiality, and sovereignty-sensitive information, perpetual readability is neither a necessary nor a reasonable institutional objective.

A more resilient design ensures that the minimal verifiable core of proof remains usable long term, while highly sensitive details gradually exit default readability after defined periods and can be recovered only under lawful conditions through controlled processes, or interpreted by authorized parties under bounded permissions. This avoids both the compliance risk of perpetual exposure and the loss of historical verifiability.

这一思路与证明分层设计一脉相承：系统始终维护对历史事实的密码学锚定，同时允许高敏感细节从可读逐步过渡至受控可读乃至不可读，从而在制度合规与系统可信之间取得可持续的平衡。

第三重挑战在于，访问控制与授权轨迹的可审计性。

在数据保护领域，“谁有权访问”以及“访问是否合规且必要”，往往是比数据是否留存更敏感的制度性问题。主权级系统若要在满足合规审查的同时，有效对冲隐私与政治风险，就必须将信息调阅与披露的全过程同样纳入可验证的证明框架。不仅要证明规则执行无误，也要证明任何超出默认范围的“窥视”行为本身合法、可溯且受控。

一个制度上可持续的设计，往往需要在证明生命周期中维护两条并行且互锁的记录轨迹：

1. **业务事实轨迹**：用以追溯交易结算的执行过程与最终状态；
2. **访问责任轨迹**：用以记录对证明材料的每一次调阅、复制、传递或导出，并关联其授权依据、操作主体、时间戳及访问目的。

第四个挑战，是跨时间的可解释性与合规适配。

数据保护法规会演进，隐私标准会更新，各国监管口径也可能调整。若证明结构无法随之适应，系统将面临历史证明的合法性被追溯性质疑的制度性风险。

这里必须区分两个常被混淆的概念：证明的长期存在，不等于证明的长期可读。长期存在，指历史一致性始终可被证明；长期可读，则意味着原始内容在任何未来时刻都能被完整解码与理解。对于涉及个人身份、商业机密或主权敏感信息的字段而言，后者并非合理的制度目标。

sure and the operational risk of irrecoverable trace loss.

Governance Boundary: Lifecycle Orchestration as Data-Sovereignty Engineering

Finally, sovereign settlement infrastructures face a governance boundary that cannot be treated as a purely technical question. Proof lifecycle governance must align with the legal responsibilities of participating entities. In layered architectures, certain core content must remain within sovereign domains under domestic jurisdiction; summarized or anchored commitments may flow cross-domain to support global consistency verification; and highly sensitive supplementary materials must be accessible only under specific authorization and compliance procedures.

In effect, lifecycle governance is an institutional orchestration of data sovereignty. It binds retention, access, disclosure, and retirement to clearly assigned responsible parties and judicial boundaries. This ensures that, over long-term operation, the system neither loses credibility through proof gaps nor forfeits legitimacy and political sustainability through excessive retention, uncontrolled access, or misuse of sensitive information.

更具韧性的设计是：确保证明的最小可验证核心长期可用，而高敏感细节在合理期限后，逐步退出默认可读状态；仅在符合法定条件的情形下，通过受控流程恢复可读，或由授权主体执行受限解读。如此，系统既能避免永久暴露带来的合规风险，也不落入无法追溯的工程陷阱。

最后，主权级结算体系还有一个不容忽视的治理边界。

证明的生命周期管理不能被简化为纯技术策略，而必须与各参与方的法定责任相匹配。在分层架构中，某些核心数据应留存在主权域内，受本土法律直接管辖；某些摘要或锚定数据可跨域流转，以支撑全局一致性验证；而更高敏感度的补充材料，则只能在特定授权与合规流程下被调阅。简言之，生命周期治理是一种制度化的数据主权编排。它将数据的保存、访问、披露与销毁，明确绑定至对应的责任主体与司法边界，从而确保系统在长期运行中既不会因证明缺失而丧失可信性，也不会因数据过度留存与滥用而失去制度正当性与政治可持续性。

CHAPTER A9.

Risk & Resilience
in Sovereign Settlement Interface

A9. 章节

主权可验证结算框架的风险与系统韧性

Abstract:

In the Sovereign Settlement Interface (SSI), risk management and system resilience are grounded in constitutional design principles that preserve jurisdictional sovereignty, programmable compliance, and neutral global coordination. Rather than relying on generic blockchain notions, SSI's architecture (as defined in Chapters A7 and A8) delineates clear layers and roles, from domestic Sovereign Compliance & Execution Layers (SCELs) to the global Sovereign Relay Hub (SRH), to ensure that cross-border settlement remains robust against failures and compliant under stress.

This chapter analyzes SSI's risk surface and the mechanisms for graceful degradation, continuity, and governance that together form a principled framework for institutional resilience.

As referred to in this chapter, "degradation" by no means implies a dilution of settlement semantics, a compromise on finality, or a substantive lowering of regulatory standards. Rather, degradation is defined as a controlled fallback in execution strength, trust hierarchy, or service boundaries necessitated by force majeure or technical constraints.Every form of degradation must be explicitly flagged, remain logically replayable, and be fully transparent to audit. The fundamental bottom line remains: degradation alters only the "container" of execution, while the determinism of rule outcomes remains inviolable.

（本章摘要）

在主权结算层（SSI）中，风险管理和系统韧性被置于核心地位。它的设计原则，需要像宪法一样严谨：既要保护各国的司法主权，又要实现自动化的合规管理，同时还要维持一个中立的全球协作环境。

SSI 的架构（详见 A7 章与 A8 章）并未依赖通用区块链概念，而是界定了清晰的分层和角色：从各国自主运行的主权合规执行层，到承担全球协调职能的主权中继枢纽。正是这种分层结构，确保跨境结算在遭遇故障时仍能稳健运行，在压力环境下依然符合合规要求。

本章将系统性分析 SSI 的风险面，以及其在降级运行、连续性保障与治理机制方面的设计，展示一个面向机构级使用场景的韧性框架。

如本章所述，“降级”绝非结算语义的摊薄、终局性的妥协，亦非规则标准的实质性降低。所谓降级，本质上是系统在不可抗力或技术条件受限时，对执行强度、信任层级或服务边界的受控回退。任何形式的降级均须显式标记、支持逻辑可重放且全程审计透明。其核心底线在于：降级仅改变执行的“容器”，绝不动摇规则执行结果的确定性。

A9.1

Risk Surface 风险暴露面

Portugal, 2015, João Nascimento

"The Essence is inherently immutable;
despite the flux of interactions, the System remains constant."
"本体原自不动，虽有往来，其体常定。"

— Wang Yangming, Instructions for Practical Living（王阳明,《传习录》）

The multilayered design of SSI explicitly isolates and minimizes key risk surfaces across technical, regulatory, and governance dimensions. Each architectural component - from local SCELs to the global SRH - addresses distinct vulnerabilities while simultaneously supporting dual finality (the concurrent finalization of ledger and policy) and verifiable chains of proof. The principal risk domains and their corresponding mitigation measures include:

A9.1.1 Global Coordination Point Risk (SRH)

The SRH serves as a critical foundation for the ordering and finalization of cross-border transactions, which may be perceived as a single point of failure or control. Within the SSI architectural design, this risk is deliberately mitigated through a combination of constitutional and technical constraints. Key risk-reducing properties include:

- **"Critical but not fatal" principle**: In the event of an SRH failure, only global cross-border settlements are suspended, while domestic (national) financial systems continue to operate without disruption.

SSI 的多层架构设计旨在将技术、监管和治理层面的关键风险隔离并降至最低。从本地 SCEL 到全球 SRH，每个架构组件既针对性解决特定漏洞，又同时支持双重终局性（账本与政策的同步终局性）与可验证的证明链。主要风险领域及对应缓解措施如下：

A9.1.1 全球协调点风险（SRH）

SRH 是跨境交易排序与终局确认的关键基础，可能被视为单一故障点或控制节点。在 SSI 架构设计中，通过宪法层面与技术层面的双重约束，专门缓解了这一风险。关键风险控制特性包括：

- **"关键但不致命"原则**：若 SRH 发生故障，仅暂停全球跨境结算业务，各国国内金融系统仍可正常运行，不受影响；

- **State-preserving hub replaceability**: The SRH can be replaced without compromising system integrity, preventing it from becoming an irreplaceable single point of failure.
- **Constrained SRH mandate ("coordination-only, no decision authority")**: The SRH has no unilateral authority to intervene in national decisions and performs a strictly coordinative function.
- **Neutral, multi-sovereign governance**: The governance model of the SRH precludes subordination of the infrastructure to the will of any single actor and ensures that no country's financial system is existentially dependent on an external center of authority.

Accordingly, within SSI the SRH functions as a global coordination anchor while remaining institutionally and architecturally constrained, incapable of becoming either a singular source of trust or a mechanism of external coercion.

A9.1.2 Interoperability - Trust Mismatch

In a network spanning multiple blockchains and jurisdictions, misaligned trust assumptions or the presence of malicious (compromised) gateways constitute a systemic risk. A particular vulnerability arises from cross-domain attestations - claims that the state or compliance guarantees of one SCEL can be accepted as valid by another domain. When such attestations are not standardized, they become a systemic weak point. SSI mitigates this risk through a formalized three-tier trust model for cross-chain messaging, which establishes a predictable and verifiable interaction framework:

Tier 1 - Cryptographic proofs by default:

Direct cryptographic verification methods (e.g., Merkle proofs or light-client verification) are used, enabling receiving parties or the SRH to independently validate transaction outcomes without reliance on external intermediaries.

Tier 2 - Committee-based attestation:

When Tier 1 proofs are not feasible, a model is applied in which a multi-sovereign committee of validators collectively attests to the transaction, distributing trust across multiple jurisdictions.

Tier 3 - Single designated gateway attestation (last resort):

Under emergency conditions, transaction confirmation via a single pre-designated gateway is permitted. As a trade-off, this mode is explicitly accompanied by:

- **枢纽的可替换性**：SRH 可在不损害系统完整性的前提下被替换，避免成为不可替代的单一故障点；
- **职能严格受限（"只协调、不裁决"）**：SRH 无权单方面干预各国决策，仅承担协调职能；
- **中立的多主权治理**：SRH 的治理模式杜绝基础设施服从单一主体意志，确保任何国家的金融系统都不会依赖外部权力中心而存续。

因此，在 SSI 中 SRH 发挥着全球协调锚点的作用，同时在制度和架构上保持约束，而不是信任中心，更不是制裁工具。

A9.1.2 互操作中的信任错配风险

在跨链、跨司法辖区的网络中，不匹配的信任假设或恶意（被入侵的）网关，都可能构成系统性风险。跨域背书会带来一个特殊的安全漏洞，即某一个 SCEL 声明的系统状态或合规认证结果，能否被其他辖区认可为有效。若此类证明缺乏标准化规范，将成为系统性薄弱环节。

SSI 通过标准化的跨链通信三层信任模型缓解这一风险，该模型建立了一个可预测且可验证的交互框架：

第一层 - 默认采用密码学证明。

采用直接加密验证方法（如 Merkle 证明或轻客户端验证），让接收方或 SRH 无需外部中介即可独立验证交易结果；

第二层 - 基于委员会的背书。

当第一层证明不可用时，采用由多个主权机构的验证者组成的委员会共同进行交易认证的模式，从而分散信任风险；

第三层 - 单一指定网关认证（应急模式）。

- clear labeling of a reduced-trust operating mode
- enhanced ex post audit and review requirements.

This hierarchical trust structure ensures that even when the security posture of individual domains degrades, cross-border settlement does not halt entirely but continues in a controlled mode with verifiable guarantees. At the same time, it prevents "fragile" ad hoc solutions by codifying a formal trust-degradation pathway, ensuring that any compromises remain transparent, auditable, and accountable.

A9.1.3 Proof Integrity and Compliance Risk

The fundamental risk in inter-sovereign transactions lies in a potential divergence between technical settlement and regulatory compliance. For example, a payment may be irreversibly settled at the ledger level while failing to satisfy legal or policy requirements - or, conversely, may meet compliance requirements but never achieve final technical confirmation. SSI resolves this gap through the principle of Dual Finality, under which a transaction is considered complete only when both of the following conditions are satisfied:

- **Ledger Finality**: the transaction is irreversibly committed to the ledger of the originating SCEL.
- **Policy Finality**: the transaction is accompanied by a validatedPoPC.

The SRH issues confirmation of global finality only when both conditions are met - that is, when the transaction has been conclusively finalized at both the ledger and compliance layers. This approach delivers several critical effects:

- **Policy violations cannot remain latent**: any attempt to settle a transaction without a valid proof of compliance is either rejected by the system or remains legally ineffective.
- **Standardization of compliance outcomes**: the PoPC mechanism transforms jurisdiction-specific internal checks into a unified, portable proof package.
- **Independent verifiability**: all participants can independently validate PoPC without relying on external intermediaries or trusted third parties.
- **End-to-end evidentiary chain**: a continuous linkage is preserved between ledger state and policy compliance, reducing the likelihood of hidden non-compliance and mitigating the risk of disputes over transaction validity.

仅在紧急情况下，允许通过预先指定的单一网关确认交易。作为权衡，该模式需明确满足以下要求：

- 明确标注为低信任运行模式；
- 更严格的事后审计与复核要求；

这种分层信任结构确保，即便个别域的安全状况下降，跨境结算也不会立即中断，而是以可控模式继续运行，并提供可验证保障。同时，它通过制定正式的信任降级路径，防止出现"脆弱的"临时解决方案，确保任何妥协都保持透明、可审计且可追责。

A9.1.3 证明的完整性与合规风险

主权间交易的根本风险在于技术结算与法律合规可能出现脱节。例如，一笔交易可能已经在账本上不可逆地完成结算，但在法律或政策上并不合规；反之亦然。SSI 通过双重终局性原则解决这一问题。只有当以下两个条件同时满足时，交易才被视为完成：

- **账本终局性**：交易已不可逆地记入发起方 SCEL 的账本；
- **政策终局性**：交易附带经验证的 PoPC。

SRH 只有在这两项条件同时满足时，才会确认交易的全局最终性。这一设计确保：

- **违规行为无法隐藏**：任何未提供有效 PoPC 的交易结算，要么被系统拒绝，要么不具备法律效力；
- **合规结果标准化**：PoPC 机制将特定司法管辖区的内部核查转化为统一、可移植的证明包；
- **独立可验证性**：所有参与者均可独立验证 PoPC，无需外部中介或可信第三方；

Accordingly, Dual Finality and PoPC together establish the foundation within SSI for legally robust and technically verifiable cross-border settlement, where compliance is not an external control layer but an intrinsic component of transaction finalization.

A9.1.4 Sovereign Autonomy vs. Global Consistency

A distinct category of risk within SSI arises from the tension between national autonomy and the need to maintain a single, globally consistent record. Each SCEL is operated by a sovereign authority under its own legal and policy framework, and in a less structured system this could lead to policy conflicts or fragmentation of the shared infrastructure. SSI mitigates this risk through a multi-layer model (Layers 1-4) that clearly and unambiguously assigns roles and responsibilities in advance:

Layer 1 – Domestic Core Systems: remain under full national control and are responsible for final monetary settlement and legally binding records.

Layer 2 – SCEL: enables each jurisdiction to: enforce its own policies through on-chain logic and generate audit-resilient proofs of compliance.

Layer 3 – SRH: provides a neutral service for: operation ordering and verification of proof correctness. The SRH is collectively governed by participating sovereigns and does not impose supranational authority.

Layer 4 – Audit and Observation: enables independent oversight by international or third-party auditors, who are granted access not to raw transactional data but to standardized, privacy-preserving proofs.

A core design principle is that the SRH "verifies proofs, not rules". This means that it:

- does not override sovereign policy decisions;
- does not substitute for national regulatory regimes;
- solely verifies that a transaction's PoPC is valid and complete.

This functional separation delivers two simultaneous outcomes:

- **Preservation of sovereignty**: each jurisdiction retains full decision-making authority, and no policies are delegated to the hub.
- **Single source of truth**: all participants share a globally

- **端到端证明链**：账本状态与政策合规之间保持持续关联，减少隐性违规的可能性，降低交易有效性争议风险。

因此，双重终局性与 PoPC 共同为 SSI 框架建立了法律稳健、技术可验证的跨境结算基础，合规不再是外置监管，而是交易最终完成的内在组成部分。

A9.1.4 主权自主与全球一致性

SSI 中另一类重要风险，来自国家自主权与全球一致账本之间的张力。每个 SCEL 都由主权当局在其自身法律政策框架下运营，若系统缺乏结构化设计，可能导致政策冲突或共享基础设施碎片化。SSI 通过多层级模型（第 1 - 4 层）来降低这种风险，该模型分配了以下角色和职责：

第一层 - 本国核心系统：完全由国家控制，负责最终货币结算与具有法律约束力的记录。

第二层 - SCEL：使每个司法管辖区能够通过链上逻辑执行自身政策，生成可审计的合规证明。

第三层 - SRH：提供中立服务，用于交易排序与证明正确性验证。SRH 由参与主权方共同治理，不施加超国家权力。

第四层 - 审计与监督：允许国际或第三方审计机构进行独立监督，审计机构无权访问原始交易数据，仅能获取标准化、隐私保护的证明文件。

SRH 的核心设计原则是“验证证明，而非规则”。这意味着它：

- 不取代主权政策决策；
- 不替代国家监管制度；
- 仅验证交易的 PoPC 是否有效、完整。

consistent transaction record accompanied by verifiable compliance proofs.

SSI further reduces related risks through additional mechanisms:

- **Protection against sovereignty dilution**: foundational guarantees in the SRH's constitutional framework (Founding Protocol) prohibit the infrastructure from performing political or jurisdiction-specific actions.
- **Reduction of legal inconsistency**: standardized policy packages (JPack) and explicit versioning ensure that every cross-border transaction references the exact policy version under which it was validated. This allows any participant or auditor to replay the compliance verification and arrive at the same outcome.

As a result, the SSI architecture ensures that trust is established and propagated through proofs rather than institutional hierarchy, aligning global operational consistency with the inviolability of domestic legal regimes.

这种职能分离同时实现两个目标：

- **维护主权**：每个司法管辖区保留完整决策权，不向枢纽委托任何政策制定权；
- **单一数据源**：所有参与者共享全球一致的交易记录，并附带可验证的合规证明。

SSI 还通过以下机制进一步降低相关风险：

- **防止主权被削弱**：SRH 章程中的宪法保障条款禁止基础设施从事政治或特定司法管辖区相关行为；
- **减少法律不一致性**：标准化的 JPack 与明确的版本控制，确保每笔跨境交易都引用其验证时所依据的确切政策版本。任何参与者或审计机构均可重放合规验证过程，并得到相同结果。

因此，SSI 架构信任的建立和传播是通过证明而非机构层级实现的，从而使全球运营的一致性与国内法律制度的不可侵犯性保持一致。

A9.2
Graceful degradation

平稳降级

Graceful degradation in SSI means that when parts of the system fail or face compromise, the remaining components continue to function in a reduced-but-safe mode, preserving compliance verifiability and legal continuity until normal operations can resume. The architecture explicitly anticipates partial failures and provides fallback behaviors at every layer, so that a technical fault does not escalate into a systemic crisis.

A9.2.1 Failure Isolation

A core resilience principle of SSI is that failure at the global SRH

SSI 的平稳降级指，当系统部分组件发生故障或遭遇安全威胁时，剩余组件仍能以功能降级但安全可控的模式运行，在恢复正常运营前，持续保障合规可验证性与法律连续性。该架构明确预判了部分故障场景，并在每一层都提供了回退机制，防止技术故障演变为系统性危机。

A9.2.1 故障隔离

SSI 的核心韧性原则是：全球 SRH 层级的故

layer must not disrupt a state's domestic financial operations. If the SRH becomes unavailable, "only global cross-border settlement is suspended; domestic financial systems remain unaffected".

This is achieved by ensuring that critical components of national infrastructure continue to operate autonomously:

- **RTGS** - sustains domestic settlement and monetary finality within the jurisdiction;
- **CSD** - ensures continuity of securities registration and settlement at the national level;
- **SCEL** - continues to enforce national rules and to generate proofs of compliance for local transactions.

Failure isolation provides several fundamental advantages to the system:

- **Blast-radius containment**: a disruption at the SRH affects only cross-border functions and does not propagate into domestic settlement.
- **Continuity of domestic operations**: economic activity within each jurisdiction can proceed without interruption.
- **Continuity of the evidentiary layer**: each SCEL continues to generate PoPC records for all transactions, including those queued for cross-border settlement.
- **Sovereign control over data and processes**: domestic ledgers and compliance logs are preserved, ensuring that no sovereign loses control over its operations or data even if the shared hub becomes unavailable.

Accordingly, the SSI architecture guarantees that a failure of the "public" coordination layer does not translate into a failure of the real economy. This directly embodies the principle of sovereign continuity: cross-border coordination may be paused, but national financial stability is preserved.

A9.2.2 Attestation-Level Fallback and Redundancy

For inter-domain messaging, SSI degrades gracefully, stepping down through predefined trust levels when optimal security is unavailable. The system is designed to "follow a strict hierarchical escalation path" for attestation: if one level cannot be applied, the next permissible level is invoked.

Fallback Hierarchy (Escalation Chain) - SSI implements the following fallback logic:

障不得干扰各国国内金融运作。若 SRH 无法使用，"仅暂停全球跨境结算，国内金融系统不受影响"。

这一目标通过确保国家基础设施的关键组件能够自主运行实现：

- **实时全额结算系统（RTGS）**：维持辖区内国内结算与货币终局性；
- **中央证券存管机构（CSD）**：保障国家层面证券登记与结算的连续性；
- **SCEL**：继续执行本国规则，为本地交易生成合规证明。

故障隔离为系统带来多项根本优势：

- **影响范围可控**：SRH 的中断仅影响跨境功能，不会蔓延至国内结算；
- **国内业务连续**：各辖区内经济活动可正常开展，不受干扰；
- **证明层连续**：各 SCEL 继续为所有交易（包括排队等待跨境结算的交易）生成 PoPC 记录；
- **数据与流程的主权控制**：国内账本和合规日志得以保留，即使共享枢纽不可用，各国仍掌控自身数据和操作。

因此，SSI 架构保证"公共"协调层的故障不会导致实体经济中断，这正体现了主权连续性原则：跨境协调可能暂停，但国家金融稳定得以维护。

A9.2.2 认证级别的降级与冗余

对于跨域通信，SSI 具备平稳降级能力：当最优安全性不可用时，系统会按预定义的信任层次逐级降低。系统架构设计遵循"严格的分级响应路径"：若某一层不可用，则会调用下一级允许的层级。

Tier 1 – Proof-based validation:

used under normal operating conditions. If Tier 1 becomes unavailable or non-functional (for example, due to incompatible chains or network failures), the system steps down to the next tier.

Tier 2 – Committee-based attestation:

applied as a fallback mode when direct cryptographic proofs cannot be used. For example, a consortium of central banks may collectively attest to transactions when real-time proof exchange is impractical.

Tier 3 – Single pre-designated gateway attestation:

used only as a last resort, in emergency conditions. Such operations:

- are executed with explicit reduced-trust labeling in the records;
- are subject to enhanced ex post verification.

Each reduction in trust level is not an automatic default but must comply with predefined governance rules:

- **Explicit authorization via JPack**: transition to a lower tier is permitted only if explicitly allowed by the applicable policy rules (JPack).
- **Automatic audit-log recording**: every fallback transition and all associated attestations are immutably recorded and preserved for subsequent review.
- **SRH oversight: the hub ensures that**:
  - ◇ no fallback violates the policy constraints of any participating jurisdiction (e.g., if a jurisdiction prohibits Tier 3);
  - ◇ all attestation artifacts (signatures, proofs, etc.) are immutably captured and verifiably preserved.

Operational Implications under degradation: In practice, this means that during crisis scenarios (for example, when an SCEL loses light-client functionality or an interoperability network partition occurs), participants:

- do not lose settlement capability entirely;
- temporarily accept a reduced-confidence operating mode, but:
  - ◇ under controlled rules;
  - ◇ with full action traceability;
  - ◇ while preserving the ability for subsequent verification.

It is important to note that in order to maintain integrity even in modes with reduced trust levels, SSI does not abandon verifiability requirements:

备选方案层级（逐级响应链路），SSI 采用了以下回退机制：

第一级 - 基于证明的验证：

在系统正常运行时使用。若第一层无法使用或失效（如链不兼容或网络故障），系统降级至下一层级；

第二级 - 基于委员会的背书：

当无法使用直接加密证明时，作为备选模式。例如，在实时证明交换无法实现的情况下，由多家央行组成的联合委员会共同为交易提供背书；

第三级 - 单一预指定网关背书：

仅作为极端情况下的最后手段。此类操作需满足：

- 在记录中明确标注为低信任模式；
- 接受更严格的事后验证。

每一次信任层级的降低都不是自动默认的，而必须符合预定义的治理规则：

- **JPack 明文授权**：仅当适用 JPack 明确允许时，方可降级；
- **自动审计日志记录**：每次降级切换及其所有的相关证明均被不可篡改地记录在日志中，以备后续审查；
- **SRH 监督：枢纽需确保**：
  - ◇ 任何降级操作均不违反参与司法管辖区的政策约束（如某些国家可能严禁降至第三级）；
  - ◇ 所有证明文件（签名、证明等）均被不可篡改地保存并可验证。

降级状态下的运营影响：在实际的危机场景中（如 SCEL 系统断网或出现技术故障），这一设计确保了参与方：

- 不会完全丧失结算能力；
- 暂时接受降级的低信任模式，但：

- every inter-domain transaction retains its original PoPC;
- any transaction processed via Tier 3 remains subject to post hoc review;
- degradation remains transparent, as all such events are explicitly flagged.

Accordingly, SSI prioritizes controlled degradation over system-wide halting: minimal cross-border functionality is preserved, and stakeholders can rely on the fact that any "flagged" transactions were executed out of necessity and remain subject to retrospective verification.

A9.2.3 Emergency Bilateral Channels

Graceful degradation in SSI applies not only to operating modes within the SRH, but also to procedures outside the hub. If the SRH becomes fully unavailable, participating jurisdictions may temporarily rely on direct bilateral or regional channels to execute mission-critical cross-border transactions (for example, two central banks may agree to settle a foreign-exchange transaction via a temporary SWIFT/RTGS linkage or a regional mini-hub). SSI does not treat such bypass routes as an "exit from the system". On the contrary, the architecture explicitly anticipates them through ex post reconciliation mechanisms.

In SSI, emergency bilateral channels allow transactions executed during a global outage to be safely integrated into the global SRH ledger via a backfill procedure, provided that a defined set of integrity and compliance conditions is satisfied:

- **The transaction is executed during an SRH outage**: that is, at a time when global coordination and ordering by the hub are unavailable.
- **An evidentiary basis is preserved at execution time**: each emergency transaction must be accompanied by:
  - ◇ a standard PoPC
  - ◇ additional bilateral-agreement proof, where required.
- **SCEL policy enforcement continues**: because each SCEL remains operational even during an outage and continues to generate PoPCs, this condition can be satisfied even under emergency operating modes.

Once the SRH is restored, the system performs post-recovery reconciliation to reconverge all records into a single authoritative state:

- the SRH accepts emergency transactions as "historical" events;
  - ◇ 遵循可控规则；
  - ◇ 所有操作可追溯；
  - ◇ 保留事后验证能力。

需强调的是，为保持完整性，即便在低信任模式下，SSI 仍坚持可验证性要求：

- 每笔跨域交易均保留原始 POPC；
- 任何通过第三级处理的交易都必须接受事后审查；
- 降级过程保持透明，所有相关事件均被明确标记。

因此，SSI 更重视可控降级而非系统停摆：保留最小跨境功能，并确保所有"标记"交易因必要执行且可追溯验证。保留最基本的跨境功能，同时让利益相关方确信，任何"标记"的交易都是出于必要性而执行的，并且仍然需要进行事后验证。

A9.2.3 紧急双边通道

SSI 的平稳降级机制不仅适用于 SRH 内部的运行模式，也适用于枢纽之外的协作程序。若 SRH 完全无法使用，各参与司法管辖区可暂时通过直接双边或区域通道执行关键跨境交易（如两家央行可以约定通过临时的 SWIFT 或 RTGS 链路或区域性的小型枢纽来结算外汇交易）。SSI 不将此类替代路径视为"脱离系统"。相反，该架构通过事后对账明确支持这种操作。

在 SSI 体系下，紧急双边通道允许在全局停摆期间执行的交易，通过补录程序安全地整合进 SRH 全局账本中，前提是必须满足以下预设的完整性与合规条件：

- **交易发生在 SRH 停摆期间**：即枢纽无法提供全球协调与排序服务时；
- **执行时完整保留证明链**：每一笔紧急交易必须随附以下证明：

- it orders them into the ledger with:
  - ◇ timestamps, and/or
  - ◇ special flags reflecting the actual time of execution;
- it validates their PoPCs as if the transactions had been processed in real time;
- in doing so, it reconciles divergent records back into a unified authoritative history.

The emergency bilateral channel mechanism preserves system integrity under severe disruptions by ensuring continuity, auditability, legal certainty, and post-recovery reconciliation:

- **Nothing is lost**: no legitimate transaction disappears or remains unaccounted for due to temporary outages.
- **Auditability is preserved**: even when settlement temporarily occurs off-platform, compliance proof continues to be generated and retained within jurisdictions.
- **"Soft" recovery is enabled**: the global ledger catches up with offline activity without gaps in transparency or legal certainty.
- **Legitimacy is preserved**: all parties gain assurance that emergency actions were lawful and properly recorded.

Accordingly, the ability to restore a consistent global state after unplanned bypass routes demonstrates SSI's commitment to resilience rather than rigidity.

Across all degradation scenarios, SSI adheres to the principle that verifiability and compliance are never sacrificed, ensuring that even when service quality is temporarily reduced, auditability and legal validity remain intact. This principle is reflected in the following rules:

- the system may trade polycentrism for continuity (e.g., moving from cryptographic proofs to a trusted committee);
- the system may trade throughput for safety (e.g., pausing global settlement);

But the system does not trade away auditability, legal validity and evidentiary continuity.

Every transaction, whether executed under ideal conditions or in crisis mode, carries the proof required for subsequent verification of what occurred and why. By designing for graceful degradation, SSI avoids chaotic failure modes and instead aims for fail-safe behavior, in which critical sovereign functions remain operational

  - ◇ 标准 PoPC；
  - ◇ 必要时提供额外的双边协议证明。
- **SCEL 持续运行**：由于各国的 SCEL 是独立运行的，即便在全局停摆期间，它也能继续强制执行政策并生成合规证明，因此即使在紧急运行模式下也能满足此条件。

SRH 恢复正常，系统将执行灾后调账程序，将所有记录重新协调回统一的权威状态：

- SRH 将紧急交易视为"历史"事件；
- 按以下方式将交易记录排入账本：
  - ◇ 根据时间戳，和 / 或；
  - ◇ 反映实际执行时间的特殊标记；
- 如同处理实时交易一样，重新验证这些交易的 PoPC；
- 通过上述操作，将不同的记录重新整合为统一的权威历史账本。

紧急双边通道机制通过确保连续性、可审计性、法律确定性以及灾后调账，维护了系统在严重中断下的完整性：

- **数据零丢失**：不会因临时中断导致合法交易消失或无法追溯；
- **维持可审计性**：即使结算暂时脱离平台，合规证明仍在辖区内生成留存；
- **实现软恢复**：全球账本可补录离线交易，确保透明度和法律确定性不受影响
- **维护合法性**：所有参与方都能确信，紧急状态下的操作合法且记录完整。

因此，这种在计划外绕行后仍能恢复全局状态一致性的能力，体现了 SSI 致力于增强系统韧性而非僵化的设计理念。

在所有降级场景中，SSI 始终坚持一个底线原则：绝不牺牲可验证性与合规性。这意味着即

and any temporary reduction in global efficiency can later be corrected through proof-based reconciliation.

便服务质量暂时受损，审计效力和法律效力也必须完好无损。这一原则体现为以下运行逻辑：

- 系统可牺牲多中心化以换取连续性（如从密码学证明转为信任委员会担保）；
- 系统可牺牲吞吐量以换取安全性（如暂停全球结算）；

但是，系统绝不会牺牲可审计性、法律有效性以及证明的连续性。

每一笔交易，无论是在理想环境下执行，还是在危机模式下完成。都携带着必要的存证，用于事后查明“发生了什么”以及“为什么发生”。通过这种平稳降级的设计，SSI 成功避免了混乱的崩溃模式，转而追求一种“故障自保”的行为：即确保核心的主权职能保持在线，且任何全球效率的临时损失，最终都能通过基于证明的调账程序得到修复。

A9.3

Continuity and Recovery

连续性与恢复

Continuity and recovery in SSI focus on how the system returns to an operational state after disruptions while preserving an uninterrupted chain of legal validity. Through its multi-layer architecture and proof-oriented design, SSI is able to restore global consistency after failures without compromising auditability or the rule of law.

At the core of the continuity strategy is a set of interlocking mechanisms that operate in concert:

- post-failure state reconciliation;
- data durability and reproducibility;

SSI 架构中的连续性与恢复机制侧重于：当系统遭遇中断后，如何恢复运行状态的同时，保持法律效力链条的完整性。通过多层架构与证明导向的设计，SSI 能在系统故障后重建全局一致性，同时不牺牲可审计性与法治原则。

连续性策略的核心，由一组相互配合的机制共同构成：

- 故障后的状态协调；
- 数据持久性与可复现性；

- constitutional provisions governing fallback modes and recovery.

A9.3.1 Proof-Based State Reconstruction

The global SSI ledger and compliance records are designed to be replayable and verifiable on the basis of proofs, which is critical for recovery.

This is achieved through the following architectural choices:

- **Transaction-level proof anchoring**: All cross-border transactions are recorded together with their associated PoPC artifacts (or, at a minimum, cryptographic commitments to them).
- **Proof anchoring in SRH state**: The SRH embeds aggregated proofs (e.g., PoPC Merkle roots) into its own ledger state, ensuring long-term persistence and verifiability.
- **Preservation of the full evidentiary history**: Compliance history is retained either on-chain or in synchronized audit logs, preventing loss of contextual information.

In a recovery scenario (for example, following SRH shutdown and restart), this enables the system to:

- replay the exact sequence of valid transactions before and after the disruption;
- allow auditors or newly instantiated SRH nodes to sequentially verify each transaction by validating its PoPC against the applicable policy package;
- integrate transactions executed off-platform during downtime (backfill), together with their associated proofs.

Because each PoPC references a specific policy version and execution context, deterministic replay verification within the SRH allows such transactions to be validated exactly as they were originally executed - even if policies have changed subsequently.

As a result, after recovery:

- a single authoritative ledger is reconstituted;
- each record is either a standard transaction or a reconciled emergency transaction;
- each record is backed by a verifiable proof of compliance.

There are no “blind spots”: the legal state of the system is treated as a collection of durable evidentiary assets capable of surviving any technical interruption.

- 对降级模式与恢复流程作出明确约束的宪制级规则。

A9.3.1 基于证明的状态重构

SSI 的全球账本和合规记录被设计为可重放且可验证的，这对于灾后恢复至关重要。

这一目标通过以下架构设计实现：

- **交易级证明锚定**：所有的跨境交易在记录时，都会与其关联的 PoPC 原件（或至少是其密码学承诺）进行绑定；
- **SRH 状态中的证明锚定**：SRH 将聚合证明（如 PoPC 默克尔根）嵌入自身账本状态中，确保数据的长期持久性与可验证性；
- **完整证明历史保存**：合规历史会同步记录在链上或审计日志中，防止上下文信息的丢失。

在恢复场景中（如 SRH 关闭后重启），这些设计使得系统能够：

- 精确重放中断前后所有有效交易的执行顺序；
- 允许审计机构或新部署的 SRH 节点，逐笔验证交易并将 PoPC 与对应的政策包进行校验；
- 将系统中断期间通过平台外执行的交易（补录交易）及其配套证明重新整合进全局账本。

由于每份 PoPC 均明确绑定具体的政策版本与执行上下文，SRH 的这种确定性回放验证，确保即便相关政策后来发生了变化，也不影响对原始交易合法性的验证。

因此，恢复后：

- 系统会重构出一个唯一的权威账本；

A9.3.2 Hub Replaceability and Legal Continuity

The SSI architecture explicitly anticipates even extreme recovery scenarios, including full replacement of the Sovereign Relay Hub (SRH) in the event of catastrophic failure or governance breakdown.

The key principles are as follows:

- **SRH as a replaceable utility, not an absolute trust anchor**: The hub is not a monolithic dependency whose failure would collapse the system.
- **Reproducibility of global state**: A new SRH implementation may replace the previous one provided that it:
  - ◇ adheres to the same base protocols;
  - ◇ can read historically preserved PoPCs and transaction hashes.
- **Distributed data custody**: All participating jurisdictions retain their own copies of transaction logs and proofs via SCELs and audit layers, enabling initialization of a new hub from these sources.

Together, these properties ensure:

- significantly reduced recovery time even under "total failure" scenarios;
- preservation of the legal validity of all transactions and proofs;
- independence of legal continuity from any specific implementation or technology vendor.

The network's multilateral Founding Protocol provides for a collective mechanism to initiate such a replacement through preagreed procedures. Once a new hub is deployed and historical data is ingested, it resumes ordering and verification functions as if no ledger fragmentation had occurred.

This eliminates the possibility of irrecoverable failure: a path to restoring the canonical state always exists.

A9.3.3 Legal and Institutional Continuity

SSI preserves continuity not only of data, but also of legal and institutional validity throughout the entire failure and recovery lifecycle.

This is ensured through the following system properties:

- **Continuous enforcement of national rules**: SCELs
- 每条记录要么是标准交易，要么是已对账的紧急交易；
- 每条记录都有可验证的合规性证明作为支持。

在 SSI 系统中不存在所谓的“盲区”：法律状态被视为一种持久的证明资产，能够跨越任何技术故障而存在。

A9.3.2 枢纽可替代性与法律连续性

SSI 架构在设计之初就考虑到了最极端的恢复场景，包括在发生毁灭性故障或治理崩溃时，彻底更换主权中继枢纽（SRH）。

其核心原则如下：

- **SRH 是可替换的公共设施，而非绝对信任锚点**：枢纽并非单一依赖锚点，其故障不会导致系统整体崩溃；
- **全局状态可重现**：新的 SRH 实施方案若满足以下条件，可替代原有方案：
  - ◇ 遵循相同基础协议；
  - ◇ 能够读取历史保存的 PoPC 与交易哈希。
- **分布式数据托管**：各司法辖区通过 SCEL 与审计层各自保存交易日志与证明，可作为新 Hub 初始化的数据来源。

这些特性共同确保：

- 即使在“全面故障”场景下，恢复时间也能显著缩短；
- 所有交易与证明的法律效力得以保全；
- 法律连续性不依赖任何特定实施方案或技术供应商。

根据多边治理章程，参与国可以通过预设的程序集体启动枢纽更换。一旦新枢纽部署完成并导入历史数据，它将立即接手交易排序和验证

continue to apply domestic policies and generate PoPCs even during a global outage.

- **Absence of "extra-legal" transactions**: Any operation – including unilateral or bilateral measures – remains within the applicable national legal framework.
- **Federated reconstruction of global history**: When transactions are reintegrated into the global ledger, they carry forward the legal continuity of their origin.

A central role is played here by programmable compliance:

- the Policy-DSL is executed at transaction time, not applied retroactively;
- each SCEL operates as a "black box" that records all compliance-relevant events;
- restoring global operations consists of aggregating these recorded events, not reinterpreting them.

In addition, the Audit and Observation Layer provides:

- independent verification of transactions and PoPCs before, during, and after disruptions;
- the ability for auditors to replay transaction logic and verify compliance execution across the entire timeline;
- an objective basis for assessing that system integrity has been preserved.

To complete the recovery cycle, the SRH issues Regulatory Finality Receipts for transactions that were pending confirmation or executed during downtime, attesting to both ledger finality and policy finality.

Synthesis: The Principle of Sovereign Continuity

By combining the mechanisms described above, SSI implements the principle of sovereign continuity:

- no country binds its legal or economic viability to a single point of failure;
- each jurisdiction can rely on its own systems and synchronize with the global network at a later stage;
- legal enforceability does not depend on the availability of foreign infrastructure.

As a result, SSI achieves resilience as a global public good: even under stress, the system ensures uninterrupted fulfillment of

职能，仿佛账本从未中断过一样。

换言之，这消除了发生不可恢复故障的可能性：始终存在一条通往规范状态的路径。

A9.3.3 法律与制度的连续性

SSI 不仅确保数据的连续性，还确保在整个故障和恢复生命周期内法律和制度的有效性始终在线。

这通过以下系统特性得到保证：

- **国家规则的持续执行**：即使全球网络断开，各国的 SCEL 仍会继续应用国内政策并生成 PoPC；
- **不存在"法外"交易**：任何操作（包括单边或双边措施）始终处于适用的国内法律框架之内；
- **全球历史的联邦式重构**：交易重新并入全局账本时，其原有的法律连续性得以一并继承。

其中，可编程合规发挥了关键作用：

- Policy-DSL 在交易发生时即时执行，而非事后追溯；
- 每个 SCEL 都如同一个"黑盒"，完整记录所有与合规相关的事件；
- 全局恢复的过程，本质上是对这些既有记录的聚合，而非重新解释。

此外，审计与观察层提供：

- 对中断前、中、后期的所有交易和 PoPC 进行独立验证；
- 支持审计方对交易逻辑与合规执行进行全时序重放；
- 为评估系统完整性是否得到维护提供客观依据。

financial obligations and compliance requirements, together with the ability to recover to a mutually trusted, consistent state shared by all participants.

最后，SRH 会为中断期间待确认或已执行的交易签发监管终局性回执，证明其账本终局性与政策终局性均已满足。

综述：主权连续性原则

通过上述机制的协同作用，SSI 实现了主权连续性原则：

- 任何国家无需将自身法律或经济运行绑定在可能发生故障的单点之上；
- 各司法辖区可依赖本地系统独立运转，又能在后续阶段与全球网络重新同步；
- 法律可执行性不依赖于境外基础设施的可用性。

最终，SSI 将韧性转化为一种全球公共产品：即便在压力之下，系统仍能持续履行金融义务与合规要求，并最终恢复到一个由所有参与方共同信任、保持一致的规范状态。

A9.4

Risk-Based Governance

基于风险的治理

Resilience in SSI is ultimately ensured through a risk-based governance framework that situates the technical mechanisms described earlier within a stable institutional context. By design, this governance model is constitutional in nature: it codifies fundamental principles - sovereignty, neutrality, and accountability - that guide how the system adapts to risk over time.

Rather than relying on ad-hoc crisis management, SSI is grounded in pre-agreed rules and oversight structures that enable the system to respond to emergencies, preserve the legitimacy of decisions, and evolve without undermining its foundational assumptions.

SSI 的系统韧性建立在一套以风险为导向的治理框架之上。该框架将前文所述的技术机制，嵌入一个稳定、可持续的制度环境中。从设计之初，该治理模型就具有宪法属性：它将主权、中立性和问责等基本原则制度化，指导系统如何随时间推移而不断应对风险。

SSI 的治理并非依赖于临时性的危机处理，而是立足于预先商定的规则和监管结构之上。这使得系统在面对紧急情况时，能够既维持决策

A9.4.1 Multilateral and Multi-Layer Governance

Ultimately, the SSI network is governed cooperatively by its sovereign participants, rather than by any single authority. A central element of this model is the SRH, which operates under a multilateral constitutional Founding Protocol. Key components of this model include:

- **SRH constitutional Founding Protocol**: Signed by all participating entities, the Founding Protocol establishes non-derogable constraints on the behaviour of the hub.
- **Prohibition of political discretion**: The SRH is institutionally prohibited from taking unilateral actions based on country lists or political criteria. This ensures that the SRH remains a neutral utility and cannot, for example, block transactions for political reasons unless explicitly mandated by the relevant SCEL.
- **Dual-Layer governance structure**, in which governance is separated into:
  - ◇ Framework Layer: codifies principles and "red lines" (neutrality, data privacy, emergency failover procedures);
  - ◇ Operational Layer: responsible for day-to-day technical operations, upgrades, and availability.

Critically, the operational layer is not permitted to violate principles enshrined in the Principia. This ensures constitutional consistency over time: the system may remain flexible in implementation, but rigid in principle.

A9.4.2 Council of Sovereign Institutions

In steady-state operation, SSI governance is realised through a joint multi-sovereign governance model, under which a council of participating central banks or designated national institutions collectively oversees the SRH.

This model is evolutionary in nature:

- **Bootstrap governance mode**: A more centralised or consortium-based structure is used to accelerate launch, manage early-stage issues, and enable rapid iteration.
- **Maturity phase**: As the system stabilises, control is progressively polycentric and transferred to sovereign representatives, reducing the risk of excessive centralisation or capture.

的正当性，又在不破坏底层核心假设的前提下进行演进。

A9.4.1 多边与分层治理

归根结底，SSI 网络是由所有参与的主权国家共同治理的，而非受制于任何单一机构。这一模型的核心是 SRH，它依据多边宪章运行。其治理模式包含以下关键要素：

- **SRH 宪章**：由所有参与实体共同签署，该宪章为枢纽的行为设定了不可逾越的硬性约束；
- **禁止政治自由裁量权**：在制度设计上，严禁 SRH 根据国家名单或政治标准采取单方面行动。这确保了 SRH 始终是一个中立的公共设施。例如，除非相关国家的 SCEL 明确授权，否则 SRH 无权因政治原因拦截交易；
- **双层治理结构**，其中治理分为：
  - ◇ 宪章层：规定基本原则和“红线”（如中立性、数据隐私、紧急故障切换程序）；
  - ◇ 运营层：负责日常的技术操作、系统升级和可用性保障。

至关重要的是，运营层严禁违反宪章原则。这确保了宪章的长期一致性：系统的具体实现可以保持灵活性，但基本原则必须保持刚性。

A9.4.2 主权机构理事会

常态下，SSI 的治理通过多主权联合模式实现。在该模式下，由各参与国的央行银行或指定国家机构组成的理事会，共同对 SRH 进行监督。

该模式具有演进性：

- **启动阶段**：采用相对集中或联盟式结构，以加速落地与快速迭代；

Regardless of phase, governance always involves multiple jurisdictions and is never exercised by a single actor, operating instead under the supervision of a foundation or regulated consortium. As the system transitions to a full sovereign council model, all material decisions (software upgrades, activation of emergency protocols, etc.) are taken collectively, using voting or consensus rules laid down in the Founding Protocol in accordance with the principles established in these Principia.

This reduces governance risk by distributing authority and aligns the system's trust model with political reality: states rely on the SRH as jointly governed infrastructure, not as an external service. Countries are therefore more willing to depend on the SRH because they are co-owners of its governance rather than mere clients.

These Principia act as a constitutional rulebook for the council, embedding risk-control mechanisms such as qualified-majority requirements for certain actions, rotation of committee members overseeing attestations, and similar safeguards that prevent hasty or covert changes.

A9.4.3 Continuous Audit and Adaptive Policy

SSI governance is deeply data-driven and audit-centric. A central role is played by the Audit and Observation Layer (Layer 4), which provides independent monitoring of system state. Its functions include:

- generation of network performance reports
- detection of anomalies and unusual patterns
- identification of cross-jurisdictional inconsistencies

Based on this data, the system establishes a feedback loop: risk patterns → audit detection → governance action. Examples of such signals and responses include:

- frequent use of Tier-3 attestations → signal of system degradation
- repeated compliance failures by a single jurisdiction's SCEL → indication of policy gaps or technical faults

To maintain resilience and compliance, governance is empowered to adapt through predefined, risk-oriented criteria. Possible actions include:

- updating the shared policy package (JPack)
- adjusting technical parameters or consensus thresholds

- **成熟阶段**：随着系统趋于稳定，控制权将逐步多中心化，并转移给主权国家代表，从而降低了权力过度集中或被权力攫取的风险。

无论处于哪个阶段，治理始终涉及多个司法管辖区，而非单一主体行使，而是在基金会或受监管的联盟的监督下运行。当系统过渡到完整的主权理事会模型后，所有重大决策（如软件升级、启动紧急协议等）均采用集体决策方式，并遵循章程中规定的投票或共识规则。

这通过分散权力降低了治理风险，并使系统信任模型与政治现实保持一致：各国将 SRH 视为联合治理的公共基础设施，而非外部服务。这种共同所有者而非纯客户的身份，极大地增强了各国对 SRH 的信任和依赖意愿。

宪法章程为理事会提供了具有约束力的规则手册，嵌入了风险控制机制，如特定事项需绝对多数通过、监督证明的委员会成员定期轮换制度，以防止仓促或隐蔽的规则变更。

A9.4.3 持续审计与适应性政策

SSI 的治理高度依赖数据驱动和审计。审计与观察层（第四层）在其中发挥着独立监控系统状态的关键作用，其功能包括：

- 生成网络性能报告
- 检测异常与非常规模式
- 识别跨司法管辖区的不一致性

基于这些数据，系统建立了一个反馈闭环：风险特征 → 审计检测 → 治理行动。此类信号与响应示例包括：

- 频繁使用第三层证明，则释放出系统性能下降的信号
- 若单一国家的 SCEL 反复出现合规失败，预示该国政策存在漏洞或技术故障

- lowering trust levels for regions affected by infrastructure attacks
- initiating hub replacement procedures in the event of operator compromise

All such actions must be predefined, explicitly authorised, and immutably recorded in audit logs. This eliminates improvisation and power struggles during crises: participants know in advance the applicable procedures and expected behaviours. By pre-defining these governance responses, SSI avoids panic or institutional conflict during emergencies - for example, when declaring an SRH emergency or selecting and validating a replacement hub. Audit logging further ensures traceability and accountability of all emergency measures.

A9.4.4 Transparency and Accountability

A defining feature of SSI governance is radical transparency, which is essential for maintaining legitimacy among sovereign participants. By design, all cross-domain actions are auditable - not only transactions, but also governance actions such as policy updates and trust-level changes.

The system architecture ensures that:

- governance actions are auditable alongside transactions;
- independent auditors continuously oversee the actions of governing bodies;
- the audit layer provides an objective external assessment of system neutrality, continuity, and overall reliability.

This creates reputational and legal constraints on the sovereign council: any attempt to conceal incidents or distort rules leaves a durable evidentiary trail accessible to all participants (and, where applicable, the public). In governance terms, this imposes enforceable accountability: collusion to hide failures or manipulate rules would be detectable, undermining the entire construct. Incentives are therefore aligned toward honest and proportionate risk responses.

Additionally, the constitutional governance framework may include mechanisms to enhance resilience and dispute resolution, established in these Principia and enforced through legal mechanisms in the Founding Protocol:

- dispute-resolution mechanisms
- arbitration procedures
- emergency veto rights for minority jurisdictions

为维持韧性与合规性，治理层有权根据预设的风险标准进行调整。可能的行动包括：

- 更新共享法规要件集（JPack）
- 调整技术参数或共识阈值
- 降低受攻击地区的信任等级
- 在运营商遭受攻击时，启动枢纽替换

所有此类行动必须是预设的、经过明确授权的，并记录在不可篡改的审计日志中。避免危机中的即兴决策与权力博弈：参与者预先知道应对程序。通过预设治理响应，SSI 避免了在紧急情况下（如宣布枢纽进入紧急状态或更换枢纽时）出现恐慌或机构间的冲突。审计日志则进一步确保所有紧急措施的可追溯性与问责制。

A9.4.4 透明度与问责制

SSI 治理的一项鲜明特征是高度透明，这也是维持各国政府间正当性的基石。在设计上，所有跨域行为均可审计，不仅包括交易，还包括政策更新、信任层级变更等治理行为。

系统架构确保：

- 治理行为与交易一同接受审计；
- 独立审计持续监督治理机构的行为；
- 审计层提供关于系统中立性、连续性和可靠性的客观外部评估。

这在理事会间形成了声誉和法律的双重约束：任何试图掩盖事件或歪曲规则的行为都会留下持久的证明，所有参与者（及适用情况下的公众）均可查。治理层面，这意味着问责制是可强制执行的：任何掩盖失败或操纵规则的行为都将被察觉，从而瓦解整个体系。因此激励机制促使人们采取诚实且适度的风险应对措施。

此外，宪制框架还可以纳入一系列增强系统韧性与争议处理的机制。这些机制应通过章程中的法律手段来实施，而非单纯依靠技术强制：

Together, these measures cultivate a governance culture in which risk management is a collective responsibility, and covert erosion of resilience becomes practically infeasible.

Synthesis: Risk Governance as a Constitutional Principle

SSI's approach to risk and resilience is a core architectural feature, not an auxiliary function. By separating layers of sovereignty, enforcing proof-based operations, and embedding governance in multilateral institutions, SSI provides a blueprint for financial infrastructure capable of withstanding shocks while preserving the rule of law.

Under the principle of sovereign continuity, even extreme scenarios do not compromise system integrity:

- participants retain control over their own domains;
- the system collectively reconverges toward stability.

This principled, constitutional-style risk governance framework ensures that next-generation settlement networks can be both innovative and resilient - achieving global interoperability and efficiency without exposing states to unacceptable operational or political risks. In SSI, resilience is engineered through accountability and separation of powers, making the infrastructure a durable foundation for international finance in the digital era.

- 争议解决机制
- 仲裁程序
- 少数司法管辖区的紧急否决权

通过这些措施，系统培养了一种共同治理的文化。在这种文化下，风险管理成为了所有参与方的共同责任，任何企图暗中削弱系统韧性的行为在现实中几乎都不可能发生。

综述：风险治理即“宪法级”原则

在 SSI 中，风险与韧性并非附属功能，而是体系架构的核心组成。通过对主权层级的清晰分离、以可验证证明为基础的运行机制，以及将治理嵌入多边制度框架，SSI 勾勒出一套既能承受冲击、又能维护法治的金融基础设施蓝图。

在主权连续性原则下，即使面对极端场景也不会损害系统的完整性：

- 各参与方始终掌握自身辖区的控制权；
- 系统整体会共同回归稳定状态。

这种基于原则、具备宪法色彩的风险治理框架，确保了下一代结算网络能够兼顾创新与韧性，在实现全球互通与高效运行的同时，不将国家暴露于不可接受的运行或政治风险之中。在 SSI 体系内，韧性是通过问责制与权力制衡构建出来的。这使得该基础设施能够成为数字时代国际金融体系中一块坚不可摧的基石。

CHAPTER A10.

Protocol Periphery *&* Ecosystem Architecture

A10. 章节

协议外延与生态架构

Abstract:

The preceding chapters have defined the system's minimal-trust core: SCEL executes sovereign compliance, SRH orders and verifies, JPack encapsulates rules, PoPC proves execution. The trust core is locked by protocol. The evolutionary space must be returned to the market.

A10 delineates the boundary between the two. Its objective is not to extend the trust architecture but to define where third-party innovation begins - and what constraints it must respect. The governing principle is straightforward: ecosystem participants interact with rule artifacts and compliance proofs through standardized interfaces, but do not enter the trust-layer architecture, do not exercise rule discretion, do not modify proof-generation paths, and do not affect finality.

Within this boundary, six principal directions of ecosystem development emerge. We identify these major ecosystem directions, each sharing the common semantic of “verifiable, replayable, auditable”, forming a clear industrial separation from the trust core:

1. **Supporting Infrastructure Services**
2. **Compliant Asset Onboarding**
3. **Industry Vertical Solutions**
4. **RegTech and Proof-Based Supervisory Products**
5. **Privacy Engineering and Minimal-Disclosure Proof Systems**
6. **Developer Ecosystem and Rule-Artifact Toolchains**

Because the core is deliberately minimal and institutionally stable, the system enables broad third-party participation. Ecosystem actors interact with rule artifacts and compliance proofs through standardized interfaces, forming specialized divisions of labor outside the protocol boundary - without entering the trust architecture, exercising rule discretion, or affecting finality. The ecosystem can grow precisely because the protocol core remains neutral.

（本章摘要）

前述章节已经界定了系统的最小信任内核：SCEL 负责执行主权合规，SRH 负责排序与验证，JPack 负责封装规则，PoPC 负责对执行结果出具证明。这个信任内核由协议层严格锁定；而系统的演进空间，则应交还给市场。

A10 旨在勾勒二者之间的清晰边界。其目的不是继续扩展信任架构，而是明确：第三方创新从哪里开始，以及必须遵守哪些约束。治理原则简洁明确：生态参与方可以通过标准化接口与规则工件和合规证明交互，但不得进入信任层架构，不得行使规则裁量，不得改动证明生成路径，也不得影响结算终局性。

在此边界之内，生态发展将主要沿着六个方向展开。我们将这些主要生态方向概括如下，它们共同遵循“可验证、可重放、可审计”的共同语义特征，与信任内核形成清晰的产业分工：

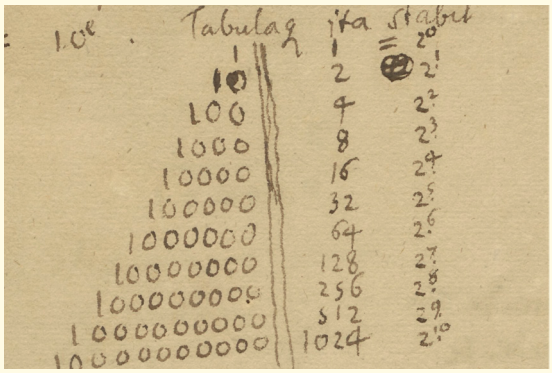
1. **配套基础设施服务**
2. **合规资产接入**
3. **行业垂直解决方案**
4. **监管科技与基于证明的监管产品**
5. **隐私工程与最小披露证明系统**
6. **开发者生态与规则工件工具链**

正因为协议内核被刻意设计为极简且具备制度稳定性，系统才能容纳广泛的第三方参与。生态参与者通过标准化接口对接规则工件与合规证明，在协议边界之外形成专业化分工体系，既不触碰信任架构，也不行使规则裁量，更不影响终局性。 生态之所以能够蓬勃生机，恰恰是因为协议内核始终保持中立。

A10.1

Boundaries and Principles: Coexistence Between a Neutral Core and Peripheral Innovation

边界与原则：中立内核与外延创新的共存



Leibniz binary system, 1697, Gottfried Wilhelm Leibniz Bibliothek

"From the Tao comes One, from One comes Two, from Two comes Three, and from Three, the infinite variety of the universe."

"道生一，一生二，二生三，三生万物。"

— Lao Tzu, Tao Te Ching（老子,《道德经》）

The SSI architecture constrains the trust core to a minimal institutional set. What the core provides is a verifiable coordination interface - standardized encapsulation, sovereign compliance execution, proof generation, cross-domain verification, and deterministic replay - not a commercial services platform. Everything beyond this interface is open to third-party participation.

That participation is explicitly interface-based: ecosystem actors consume and produce standardized artifacts (PoPC, JPack references, audit records) through published protocol interfaces, without entering the trust architecture itself.

Permitted scope. Ecosystem actors may:

- connect through standardized interfaces to encapsulate, verify, archive, and deterministically replay compliance proofs and associated audit records;

SSI 架构将信任内核严格约束在最小化的制度集之内。内核所提供的是一套可验证的协作接口，涵盖了标准化封装、主权合规执行、证明生成、跨域验证以及确定性回放，而非商业化的服务平台。凡超出这一接口边界的空间，均向第三方参与者全面开放。

这种参与被明确界定为基于接口的协作：生态参与者通过已公开的协议接口，对标准化工件（如 PoPC、JPack 索引、审计记录）进行使用与产出，但不得进入信任架构本身。

准入范围。生态参与者可以：

- 通过标准化接口，对合规证明及其相关

- develop products and services around access infrastructure, developer toolchains, operational hosting, privacy-preserving proof systems, and industry-specific solutions;
- continuously iterate on implementation and user experience without altering the protocol's trust core.

Prohibited scope. Ecosystem actors must not:

- enter the trust-layer architecture or acquire discretionary authority over rule execution;
- determine rule content, modify rule effectiveness, or alter proof-generation and attestation paths;
- replace or interfere with compliance execution and responsibility boundaries within sovereign jurisdictions.

The principle governing this boundary is consistent with the architectural logic established throughout these Principia: sovereign discretion remains within SCELs, neutral verification remains within the SRH, and the ecosystem operates exclusively at the interface layer between them. The six ecosystem domains described in the following sections each observe this constraint.

审计记录进行封装、验证、归档和确定性重放。

- 围绕接入基础设施、开发者工具链、运营托管、隐私保护型证明系统以及行业专属解决方案，开发相应产品与服务。
- 在不触及协议信任内核的前提下，持续迭代实现方式与用户体验。

禁入范围。生态参与者严禁：

- 进入信任层架构，或取得对规则执行的任何裁量权。
- 决定规则内容、改变规则效力，或试图改动证明生成与见证路径。
- 替代、干扰主权辖区内部的合规执行逻辑及其责任边界。

划定这一边界的原则，与整部元宪章所确立的架构逻辑一脉相承：主权裁量权锁定在 SCEL 内部，中立验证权保留在 SRH 之中，而生态只能运行于二者之间的接口层。下文所述的六大生态领域，均须恪守这一根本性约束。

A10.2
Six Ecosystem Directions

六大生态方向

A10.2.1 Supporting Infrastructure Services

Participants in this category most closely resemble the peripheral service providers surrounding traditional international settlement infrastructures - gateway operators, middleware vendors, hosting providers, and monitoring services. However, the basis of competition shifts from proprietary standards and relationship networks toward engineering capabilities that are verifiable, replayable, and auditable. These services reduce onboarding barriers and improve

A10.2.1 配套基础设施服务

此类生态参与者，最接近传统国际清算基础设施周边的外围服务商，如网关运营商、中间件厂商、托管服务商及运行监测服务提供者。然而，竞争的维度已从专有标准与关系网络转向可验证、可重放、可审计的工程能力。这类服务的价值，在于降低接入门槛、提升运行韧性，

operational resilience without altering the institutional authority responsible for determining what constitutes compliance.

Message and process conversion gateways map existing institutional message formats, which may include ISO 20022, SWIFT MT/MX, or proprietary internal payment instructions, into SSI-compatible Transfer Packages and cross-domain message structures as defined in A7. This includes establishing mappings between source data fields and verifiable input digests, determining which elements enter the proof structure and which remain confined to local operational logs. In practice, a cross-border gateway provider might offer a unified adaptation layer for multiple banks, enabling them to generate PoPC references and associated proof artifacts without refactoring their core banking systems.

Access toolkits and compatibility middleware provide minimal-modification integration paths suitable for institutions of varying scale - including SDKs, PoPC validation libraries, JPack subscription clients, and audit-log connectors. For small and medium-sized payment institutions, hosted adapters may require integration only with account management and risk-control interfaces in order to connect to the SSI network.

Operational hosting and disaster-recovery services cover active-active deployments, proof repository scaling, log archival systems, resilience drill frameworks, and post-incident analysis. The scope is long-term operational continuity - not participation in compliance judgment or regulatory discretion. A typical engagement might involve hosting compliance modules and conducting annual degradation drills for multi-jurisdiction pilots, producing auditable operational reports.

Observer nodes and operational monitoring provide independent tracking of network neutrality, continuity, and availability - including latency, failure rates, degradation incidents, and proof-verification sampling. These metrics are published as publicly accessible indicators, enabling prospective participants to evaluate network health prior to onboarding.

A10.2.2 Compliant Asset Onboarding

This ecosystem direction enables public DLT networks, stablecoins, tokenized deposits, and institutional digital assets to enter cross-domain settlement flows while carrying verifiable compliance proofs. The institutional significance is a fundamental shift: compliance transitions from centralized endorsement toward

而不是改变由谁来界定何为合规的制度性权威。

报文与流程转换网关，负责将现有的机构报文格式（包括 ISO 20022、SWIFT MT/MX 或机构内部专有支付指令）映射为 A7 章节定义的 SSI 兼容传输包与跨域报文结构。这既包括建立源数据字段与可验证输入摘要之间的映射，也包括界定哪些要素进入证明结构、哪些仅保留在本地运行日志中。实践中，跨境网关服务商可以为多家银行提供统一适配层，使其无需重构核心银行系统，即可生成 PoPC 引用及相关证明工件。

接入工具包与兼容性中间件，为不同规模的机构提供最小改造的接入路径，包括 SDK、PoPC 验证库、JPack 订阅客户端以及审计日志连接器。对于中小型支付机构而言，托管式适配器往往只需对接账户管理与风控接口，即可接入 SSI 网络。

运维托管与灾备服务，覆盖双活部署、证明仓库扩容、日志归档系统、韧性演练框架以及事件后的复盘分析。其服务范围是保障业务的长期连续性，而不是参与合规判断或行使监管裁量。典型场景如：为多辖区试点项目托管合规模块，并开展年度降级演练，最终形成可审计的运行报告。

观测节点与运行监测，提供对网络中立性、连续性与可用性的独立追踪，监测指标包括延迟、故障率、回退事件以及证明验证抽样等指标。这些指标可被公开发布，供潜在参与方在接入前评估网络健康状况。

A10.2.2 合规资产接入

这一生态方向，使公共 DLT 网络、稳定币、代币化存款以及机构型数字资产，能够携带可验证的合规证明进入跨域结算流程。其制度意

cryptographically verifiable proof artifacts that accompany the asset throughout its settlement lifecycle.

SSI-ready stablecoin and tokenized deposit services bind regulated actions - issuance, redemption, freeze/unfreeze operations, and policy-list updates - to specific JPack versions, generating PoPC for each action. Settlement flows thereby reference verifiable compliance proofs rather than static declarations. In practice, an issuer no longer provides only a compliance statement but supplies a PoPC demonstrating that a particular transaction satisfies the applicable jurisdiction's rule set at the time of cross-domain settlement.

Real-world asset (RWA) settlement and delivery middleware expresses delivery conditions, including ownership verification, lock-up periods, qualified-investor status, and regulatory limits, as verifiable rules within the JPack framework, with execution proven via PoPC. In cross-border bond settlement, for instance, a buyer need not disclose full client identity; instead, the buyer provides selective proofs confirming qualified-investor status and compliant source of funds.

Public DLT compliance modules and proof-carrying adapters attach PoPC references when transactions exit a sovereign domain and verify them upon entry into another domain before incorporating them into local audit records. This enables interoperability between public DLT networks and sovereign compliance execution environments. Within a public-DLT settlement channel, on-chain smart contracts manage transaction posting and triggering events, while compliance evaluation occurs within the originating domain's SCEL, which issues the corresponding PoPC.

A10.2.3 Industry Vertical Solutions

Under traditional coordination paradigms, many industries face a common structural constraint: cross-domain collaboration relies on fragmented documentation and endorsements by centralized intermediaries. Operational truth is embedded in administrative explanations, and cross-jurisdiction audit becomes costly and slow. SSI translates these industry-level conventions into verifiable digital logic, shifting collaboration from narrative assurances toward cryptographic proof and deterministic replay. Without requiring costly bilateral investigations, parties can verify that operational facts are consistent, reproducible, and resistant to tampering.

Trade and supply-chain finance. Operational conditions

义在于一种根本性的转变：合规不再主要依赖中心化背书，而是转化为伴随资产整个结算生命周期流转的、可经密码学验证的证明工件。

兼容 SSI 的稳定币与代币化存款服务，将发行、赎回、冻结 / 解冻操作以及名单 / 策略更新等受监管动作，绑定到特定 JPack 版本，并为每一项动作生成 PoPC。于是，结算流程所引用的，不再是静态合规声明，而是可验证的合规证明。实践中，发行方不再只是出具一份合规说明，而是提供一份 PoPC 证明，用以证明某笔具体交易在跨域结算发生时，确实满足适用辖区当时生效的规则集。

现实世界资产（RWA）结算与交割中间件，将所有权核验、锁定期、合格投资者资格以及监管限额等交割条件，在 JPack 框架内表达为可验证规则，并通过 PoPC 证明其执行结果。以跨境债券结算为例，买方无需披露完整客户身份，而是通过选择性证明来确认其具备合格投资者资格，且资金来源合规。

公共 DLT 合规模块与携带证明的适配器，会在交易离开一个主权域时附加 PoPC 引用，在进入另一个主权域时完成验证，再将其纳入本地审计记录。这使公共 DLT 网络与主权合规执行环境之间的互操作成为可能。在公共 DLT 结算通道中，链上智能合约负责交易记账与触发事件管理，而合规评估则发生在源域的 SCEL 内，由其签发相应的 PoPC。

A10.2.3 行业垂直解决方案

在传统协作范式下，许多行业面对的是同一种结构性约束：跨域协作依赖碎片化的纸质单据和中心化中介的背书，业务真实往往包裹在行政式说明之中，跨辖区审计因此成本高、效率低。SSI 将这些行业层面的协作惯例转译为可验证的数字逻辑，使协作从叙事式担保转向密

- document consistency, customs and logistics status, payment triggers, receivable authenticity, and pledge status - can be expressed as verifiable rules with execution proven via PoPC. In factoring and receivables financing, for instance, the conditions "receivable exists, has not been double-pledged, and settlement conditions are satisfied" can be verified across multiple banks in near real time, replacing manual document reconciliation and significantly reducing fraud risk.

Cross-border e-commerce and payment aggregation. Revenue allocation, refund and chargeback processes, and dispute-handling workflows can be expressed as deterministic, replayable execution processes. When a platform settles with merchants across multiple jurisdictions, settlement logic is executed according to destination regulatory rules and corresponding compliance proofs are generated automatically - enabling dispute resolution through deterministic replay rather than manual case reconstruction.

Energy and commodity delivery. Physical delivery conditions - warehouse receipts, bills of lading, inspection reports, and delivery confirmation - can be incorporated into verifiable delivery states, with payment programmatically triggered once conditions are verified. In the event of a quality dispute, the full operational sequence can be deterministically replayed from the proof archive.

Securities, funds, and custody operations. Custody workflows, including Delivery versus Payment (DvP) and Payment-versus-Payment (PvP) processes, can be transformed into proof-verifiable settlement flows, enabling automated reconciliation across custodians and counterparties and programmatic regulatory reporting based on verifiable transaction states. Custodian banks replace extensive document exchange with standardized compliance proofs tied to settlement execution.

A10.2.4 RegTech and Proof-Based Supervisory Products

Within the SSI architecture, the objects of regulation and audit are no longer static reports but verifiable proofs and replayable execution processes. The cost of resolving cross-domain disputes is significantly reduced: disagreements no longer rely on narrative explanation but on deterministic replay of compliance execution.

Audit and forensic platforms provide deterministic replay of operational events and reconstruction of responsibility chains,

码学证明与确定性重放。这样一来，各方无需开展高成本的双边调查，也能核验业务事实是否一致、可复现且具备抗篡改性。

贸易与供应链金融，单证一致性、海关与物流状态、付款触发条件、应收账款真实性以及质押状态等业务条件，都可以被表达为可验证规则，并由 PoPC 证明其执行结果。以保理和应收账款融资为例，应收账款真实存在、未被重复质押、且满足结算条件这类判断，可以在多家银行之间实现近实时核验，从而替代人工单据核对，显著降低欺诈风险。

跨境电商与支付聚合，收入分配、退款与拒付流程、争议处理工作流，都可以被表达为确定性、可重放的执行过程。当平台与多个辖区的商户进行结算时，结算逻辑可按目的地监管规则执行，并自动生成相应的合规证明，使争议处理不再依赖人工重建个案过程，而是可以通过确定性重放直接还原。

能源与大宗商品交割，仓单、提单、检验报告和交付确认等实物交割条件，可以被纳入可验证的交付状态；一旦条件核验通过，即可由程序自动触发付款。若发生质量争议，则可从证明归档库中对完整业务序列进行确定性重放。

证券、基金与托管运营，托管流程，包括券款对付（DvP）与款款对付（PvP），都可以被改造为可由证明验证的结算流，从而支持托管人和交易对手之间的自动对账，并基于可验证的交易状态实现程序化监管报送。托管银行由此可以用与结算执行绑定的标准化合规证明，替代大规模文档往来。

A10.2.4 监管科技与基于证明的监管产品

在 SSI 架构中，监管与审计的对象不再是静态报表，而是可验证的证明对象与可重放的执行

including export of standardized proof artifacts for regulatory proceedings. Law firms and external auditors can verify the consistency of the rule version in force at execution time, the input data consumed, and the resulting compliance conclusion - without requiring full access to sensitive operational data.

Continuous compliance and rule-change management tools operationalize regulatory updates across the JPack lifecycle. When a JPack version is updated, these tools trigger automated impact assessments, support staged activation with rollback mechanisms, and retain complete audit traces. A large financial institution, for instance, can automatically generate lists of affected transaction categories and mitigation strategies for legacy transactions upon a regulatory rule change.

Stress testing and emergency simulation services provide scenario libraries for system degradation, cross-domain interruption, and exceptional regulatory events - along with verification test suites for confirming operational continuity. Annual regulatory stress tests can thereby produce machine-verifiable proof artifacts documenting system readiness and recovery capabilities.

A10.2.5 Privacy Engineering and Minimal-Disclosure Proof Systems

A foundational principle of the SSI architecture is that verifiability does not require full disclosure. This creates demand for privacy and key-engineering capabilities that enable institutions to achieve sufficient proof with minimal disclosure - ensuring that cross-domain mutual recognition is not blocked by privacy constraints or data-sovereignty requirements.

Selective disclosure and zero-knowledge compliance proofs enable institutions to demonstrate threshold satisfaction, sanctions-list clearance, and qualification-level sufficiency without exposing underlying data. A jurisdiction can, for instance, prove that a capital-control threshold was not triggered without disclosing full contract details.

TEE, HSM, and signature governance services provide hardware-isolated environments for proof generation and signing, along with key rotation, access control, and audit capabilities. Small and mid-sized financial institutions that lack dedicated cryptographic infrastructure can use hosted HSM services to issue PoPC while meeting the required signature and attestation standards.

过程。跨域争议的处置成本也因此显著下降：分歧不再依赖叙事性解释，而是依赖对合规执行过程的确定性重放。

审计与取证平台，可以对业务事件进行确定性重放，并重构责任链，同时导出可用于监管程序的标准化证明工件。律师事务所和外部审计机构无需获得敏感运行数据的完整访问权，也能够核验执行时生效的规则版本、实际使用的输入数据以及最终合规结论之间的一致性。

持续合规与规则变更管理工具，使监管更新能够在 JPack 全生命周期内实现工程化落地。当 JPack 版本发生更新时，这类工具可以自动触发影响评估，支持带回滚机制的分阶段启用，并保留完整的审计轨迹。比如，大型金融机构在监管规则调整后，可以自动生成受影响交易类别清单，以及面向存量交易的缓释策略。

压力测试与应急仿真服务，提供系统回退、跨域中断和异常监管事件的场景库，以及用于验证运行连续性的测试套件。由此，年度监管压力测试也能够产出机器可验证的证明工件，用于记录系统就绪度与恢复能力。

A10.2.5 隐私工程与最小披露证明系统

提供系统降级、跨域中断和异常监管事件的场景库，以及用于验证运行连续性的测试套件。由此，年度监管压力测试也能够产出机器可验证的证明工件，用于记录系统就绪度与恢复能力。

选择性披露与零知识合规证明，使机构能够在不暴露底层数据的情况下，证明阈值条件已满足、未命中制裁名单、资质等级达到要求。比如，一个辖区可以在不披露完整合同细节的前提下，证明某项交易并未触发资本管制阈值。

TEE、HSM 与签名治理服务，为证明生成与

In-domain data mapping and input-digest tools convert sensitive data, such as customer profiles and transaction details, into verifiable input digests before they enter the proof structure. Cross-domain verification then checks only these derived assertions, ensuring that raw business data never leaves the sovereign domain.

A10.2.6 Developer Ecosystem and Rule-Artifact Toolchains

When JPack rule packages and PoPC proof objects are treated as distributable, versionable, and testable artifacts, a natural division of labor emerges: third-party developers provide the toolchains, reusable components, and certification services that make regulatory engineering scalable.

JPack and Policy-DSL development toolchains encompass integrated development environments, static analysis, coverage measurement, conflict detection, test-vector generation, regression testing, and version management. As adoption grows, continuous integration for regulatory rules, where every rule modification must pass a suite of reproducible verification vectors before deployment, becomes a standard operational practice.

Reusable compliance modules - including KYC adapters, sanctions-list connectors, limit and purpose-restriction modules, industry-specific templates, and audit-log connectors - enable jurisdictions to compose JPack configurations from tested, standardized components. A capital-account restriction module, for example, can be reused across multiple jurisdictions with only parameter adjustments and exception clauses.

Certification and evaluation services provide compatibility certification, security evaluation, performance stress testing, and proof-availability sampling for ecosystem products. Once a gateway product or compliance module has been independently certified, onboarding risk for adopting institutions is substantially reduced - without affecting protocol neutrality.

签名提供硬件隔离环境，同时配套密钥轮换、访问控制与审计能力。缺乏专门密码基础设施的中小金融机构，可以借助托管式 HSM 服务签发 PoPC，在满足高标准签名要求的同时，确保私钥的安全。

域内数据映射与输入摘要工具，在敏感数据（如客户画像）进入证明结构之前，先将其转换为可验证的输入摘要。跨域验证时，外部只需校验这些派生断言，从而确保原始业务数据始终不离开主权域。

A10.2.6 开发者生态与规则工件工具链

当 JPack 法规集与 PoPC 证明对象被视为可分发、可版本化、可测试的工件时，一种自然的分工就会形成：第三方开发者提供工具链、可复用组件和认证服务，使监管工程具备规模化能力。

JPack 与 Policy-DSL 开发工具链，涵盖集成开发环境、静态分析、覆盖率度量、冲突检测、测试向量生成、回归测试以及版本管理。随着采用范围扩大，监管规则的持续集成将成为标准运行实践：每一次规则修改，在部署之前都必须通过一组可复现的验证向量测试。

可复用的合规模块，包括 KYC 适配器、制裁名单连接器、限额与用途限制模块、行业专用模板以及审计日志连接器，使各辖区能够以经过测试的标准化组件来组合 JPack 配置。比如，一个资本项目限制模块，只需调整参数和例外条款，就可以在多个辖区重复使用。

认证与评测服务，为生态产品提供兼容性认证、安全评估、性能压力测试以及证明可用性抽样服务。一旦某个网关产品或合规模块已经通过独立认证，采用机构的接入风险就会显著下降，而这一过程并不会影响协议的中立性。

A10.3

The Protocol Boundary as Institutional Foundation

The ecosystem architecture presented in this chapter illustrates a structural principle that extends beyond A10: the more neutral the core, the more viable the periphery; the more viable the periphery, the more stable the core. When trust and discretion are confined to a minimal protocol core, third-party participation becomes sustainable - services are substitutable, implementations can compete, and innovation can accelerate, while cross-domain mutual recognition remains consistent, replayable, and auditable.

The SSI architecture is open to third-party participation in the form of products, services, and standardized components - engaging through published interfaces, operating outside the trust boundary, and jointly transforming the principle of "execute within sovereign domains, verify globally" into scalable infrastructure. The protocol boundary is not a limitation on what the ecosystem can become. It is the institutional foundation that makes the ecosystem possible.

协议边界：生态演化的制度基石

本章所呈现的生态架构，揭示了一个超越 A10 章节本身的结构性原则：内核越中立，外延越繁荣；外延越繁荣，内核越稳固。当信任与裁量被严格约束在最小化的协议内核之内时，第三方参与才具备可持续性，服务可以相互替代，不同实现可以展开竞争，创新也能够持续加速；与此同时，跨域互认仍然能够保持一致、可重放、可审计。

SSI 架构以开放的姿态，诚邀第三方以产品、服务及标准化组件的形式进入生态。各方通过已发布的接口接入，在信任边界之外运行，共同将“主权域内执行、全球范围验证”这一原则，转化为可规模化扩展的基础设施。协议边界并不是对生态未来形态的限制，而是使生态得以成立的制度基础。

Preface. References | 序言 . 文献参考

[1] Croxton, Derek. *The Peace of Westphalia: A Historical Dictionary*. Greenwood Publishing Group, 2002.

[2] Dalio, Ray. *Principles for Dealing with the Changing World Order: Why Nations Succeed and Fail*. Simon & Schuster, 2021.

[3] Bank for International Settlements. "Project mBridge: Connecting Economies Through CBDC." https://www.bis.org/about/bisih/topics/cbdc/mbridge.htm.

[4] Bank for International Settlements. "Glossary of Terms Used in Payments and Settlement Systems." https://www.bis.org/cpmi/glossary_030301.pdf.

[5] Bank for International Settlements. "Project Mandala: Automating Compliance Policy for Cross-Border Payments." https://www.bis.org/about/bisih/topics/cbdc/mandala.htm.

A1. References | A1. 文献参考

[1] Schmandt-Besserat, Denise. "Before Writing : A Catalog of near Eastern Tokens." Univ Of Texas Press, 1992.

[2] "ATU 7, Pl. 014, W 19408,76+ Artifact Entry." (2001) 2024. Cuneiform Digital Library Initiative. July 22, 2024. https://cdli.earth/P003118.

[3] Graeber David. "Debt: The First 5,000 Years,Updated and Expanded." Brooklyn, Melville House, 2011.

[4] Coinsweekly. "A Numismatist' s Guide to Money Part 3: The Origins of Money." https://coinsweekly.com/a-numismatists-guide-to-money-part-3-the-origins-of-money.

[5] State Secrets Bureau Official Website. "Jinshang Piaohao: Pioneers of Anti-Counterfeiting and Confidentiality Systems." https://www.gjbmj.gov.cn/n1/2020/0911/c413725-31858628.html.

[6] Wikipedia. "Free banking." https://en.wikipedia.org/wiki/Free_banking.

[7] Wikipedia. "Rothschild family." https://en.wikipedia.org/wiki/Rothschild_family.

[8] Wikipedia. "Bank of England." https://en.wikipedia.org/wiki/Bank_of_England.

[9] Wikipedia. "Federal Reserve." https://en.wikipedia.org/wiki/Federal_Reserve.

[10] Wikipedia. "New Deal." https://en.wikipedia.org/wiki/New_Deal.

[11] Sandra Kollen Ghizoni. "Bretton Woods and the International Monetary System." https://www.federalreservehistory.org/essays/bretton-woods-created.

[12] Triffin, Robert. "Gold and the Dollar Crisis; the Future of Convertibility." Yale University Press, 1960, https://archive.org/details/golddollarcrisi00trif.

[13] U.S. Department of State, Office of the Historian. "Nixon and the End of the Bretton Woods System, 1971–1973." https://history.state.gov/milestones/1969-1976/nixon-shock.

[14] Wikipedia. History of SWIFT." https://en.wikipedia.org/wiki/SWIFT.

[15] European Central Bank. "TARGET Services at a glance – key facts and figures 2024." European Central Bank, https://www.ecb.europa.eu/press/targetservar/html/ecb.targetservar2024.en.html.

[16] Wikipedia. "Cross-Border Interbank Payment System ." https://en.wikipedia.org/wiki/Cross-Border_Interbank_Payment_System.

[17] Antonopoulos, Andreas M. "Mastering Bitcoin: Unlocking Digital Cryptocurrencies." O' Reilly Media, 2014. https://github.com/bitcoinbook/bitcoinbook.

[18] The Times. "Chancellor on Brink of Second Bailout for Banks." January 3, 2009. Timechain Artifacts (newspaper collectible description). https://timechainartifacts.com/hodliday-market/2131-HODLiday_32.html.

[19] Blockchain.com. "Bitcoin Genesis Block (Block 0)." https://www.blockchain.com/explorer/blocks/btc/0.

[20] Baily, Martin N., Matthew S. Johnson, and Robert E. Litan. "The Origins of the Financial Crisis. " Brookings Institution, 2008. https://www.brookings.edu/articles/the-origins-of-the-financial-crisis.

[21] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System. " 2008. https://bitcoin.org/bitcoin.pdf.

[22] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine Generals Problem." 1982. https://lamport.azurewebsites.net/pubs/byz.pdf.

[23] Budish, Eric. "The Economic Limits of Bitcoin and the Blockchain. " National Bureau of Economic Research (NBER), 2018. https://www.nber.org/papers/w24717.

[24] Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. "Bitcoin: Economics, Technology, and Governance." Journal of Economic Perspectives, vol. 29, no. 2, 2015. https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213.

[25] Hayek, Friedrich A. "Denationalisation of Money: The Argument Refined. " Institute of Economic Affairs, 1976. https://fee.org/ebooks/denationalization-of-money.

[26] Selgin, George. "Synthetic Commodity Money." Journal of Financial Stability, vol. 17, 2015. https://ideas.repec.org/a/eee/finsta/v17y2015icp92-99.html.

[27] Financial Action Task Force (FATF). “Guidance for a Risk-Based Approach to Virtual Assets.” 2019. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html.

[28] Bank for International Settlements (BIS). “Annual Economic Report 2018.” https://www.bis.org/publ/arpdf/ar2018e.htm.

[29] Bank for International Settlements (BIS). “Central Bank Digital Currencies: Foundational Principles. ” 2021. https://www.bis.org/publ/othp33.htm.

[30] Bank for International Settlements (BIS). “Blueprint for the Future Monetary System. ” Annual Economic Report, 2023. https://www.bis.org/publ/arpdf/ar2023e.htm.

[31] International Monetary Fund (IMF). “The Future of Cross-Border Payments. ” 2022. https://www.imf.org/en/Publications/DP/Issues/2022/07/19.

[32] Bank for International Settlements (BIS). “mBridge: Connecting Economies through CBDC. ” 2022. https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.

[33] Von Glahn, R. (1996). *Fountain of Fortune: Money and Monetary Policy in China, 1000-1700*. University of California Press.

[34] Udovitch, A. L. (1970). *Partnership and Profit in Medieval Islam*. Princeton University Press.

[35] Lopez, R. S., & Raymond, I. W. (2001). *Medieval Trade in the Mediterranean World: Illustrative Documents*. Columbia University Press.

A2. References | A2. 文献参考

[1] Ingham, Geoffrey. “The nature of money, Economic Sociology: European Electronic Newsletter.” ISSN 1871-3351, Max Planck Institute for the Study of Societies (MPIfG), Cologne, Vol. 5, Iss. 2, pp. 18-28.

[2] Committee On Payment And Settlement Systems. “A Glossary of Terms Used in Payments and Settlement Systems.” Basel, Bank For International Settlements, 2003, www.bis.org/cpmi/glossary_030301.pdf.

[3] Committee On Payment And Settlement Systems. “Core Principles for Systemically Important Payment Systems.” Basel, Bank For International Settlements, 2001, https://www.bis.org/cpmi/publ/d43.pdf.

[4] Heinrich, Gregor. “CPSS Core Principles for Payment Systems.” Current Developments in Monetary and Financial Law , Vol. 2, (30 October 2003): pp. 691-722.

[5] ECB. “The Core Principles for Systemically Important Payment Systems.” Financial Stability Review, 2005, https://www.ecb.europa.eu/press/financial-stability-publications/fsr/focus/2005/pdf/ecb~05205b56bb.fsrbox200505_16.pdf.

[6] Bank For International Settlements. “Principles for Financial Market Infrastructures (PFMI)[EB/OL].” https://www.bis.org/cpmi/info_pfmi.htm.

[7] Sick, Felipe. “Distributed Ledger Technologies in Accounting: An Empirical Investigation.” SSRN Electronic Journal, 2023, https://doi.org/10.2139/ssrn.4400559.

[8] Committee On Payment And Settlement Systems. “Principles for financial market infrastructures: Disclosure framework and Assessment methodology.” Basel, Bank For International Settlements, 2012, https://www.bis.org/cpmi/publ/d106.pdf.

[9] Committee On Payment And Settlement Systems. “Implementation monitoring of PFMI: Level 3 assessment of FMIs’ business continuity planning.” Basel, Bank For International Settlements, 2021, https://www.bis.org/cpmi/publ/d197.pdf.

A3. References | A3. 文献参考

[1] North, Douglas. “Institutions, Institutional Change and Economic Performance.” Cambridge University Press, 1990. https://www.cambridge.org/core/books/institutions-institutional-change-and-economic-performance/AAE1E27DF8996E24C5DD07EB79BBA7EE.

[2] Bank for International Settlements (BIS). “CPMI Principles for Financial Market Infrastructures.” https://www.bis.org/cpmi/publ/d101a.pdf.

[3] Bank of England. “Independent Review of RTGS Outage on 20 October 2014. ” https://www.bankofengland.co.uk/-/media/boe/files/report/2015/independent-review-of-rtgs-outage-on-20-october-2014.pdf.

[4] The Guardian. “Visa Admits 5m Payments Failed Over a Broken Switch.” June 19, 2018. https://www.theguardian.com/money/2018/jun/19/visa-admits-5m-payments-failed-over-a-broken-switch.

[5] Reuters. “CHAPS Disruption Tied to SWIFT Messaging Delay.” July 18, 2024. https://www.reuters.com/business/finance/bank-england-reports-problems-with-chaps-payments-system-2024-07-18.

[6] BBC. “Iranian Banks Disconnected from SWIFT.” March 17, 2012. https://www.bbc.com/news/business-17396475.

[7] International Monetary Fund (IMF). “Challenges in Correspondent Banking in the Small States of the Pacific.” IMF Working Paper No. 17/90, April 7, 2017. https://www.imf.org/en/Publications/WP/Issues/2017/04/07/Challenges-in-Correspondent-Banking-in-the-Small-States-of-the-Pacific-44809.

[8] Financial Times. “EU Sanctions Cut Key Russian Banks from SWIFT.” February 26, 2022. https://www.ft.com/content/fb2cbf50-89a7-4c38-bb29-0f22b1e37874.

A5. References | A5. 文献参考

[1] Olasehinde, Tolamise, and Ololade Henry. "AML and KYC in Crypto Firms." 2025. ResearchGate. https://www.researchgate.net/publication/391848469.

[2] Financial Crimes Enforcement Network (FinCEN). "Funds 'Travel Rule' Regulations: Questions & Answers." 2010. https://www.fincen.gov/resources/statutes-regulations/guidance/funds-travel-regulations-questions-answer.

[3] Aldasoro, Iñaki, Jon Frost, Sang Hyuk Lim, Fernando Perez-Cruz, and Hyun Song Shin. "An Approach to Anti-Money Laundering Compliance for Cryptoassets." BIS Bulletin No. 111, 2025. https://www.bis.org/publ/bisbull111.pdf.

[4] Tang, Qifeng, and Yain-Whar Si. "Central Bank Digital Currencies: A Survey." 2025. arXiv. https://arxiv.org/abs/2507.08880.

[5] OECD. "Tokenisation of Assets and Distributed Ledger Technologies in Financial Markets: Potential Impediments to Market Development and Policy Implications." OECD Business and Finance Policy Papers, No. 75, 2025. https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/01/tokenisation-of-assets-and-distributed-ledger-technologies-in-financial-markets_be149012/40e7f217-en.pdf.

[6] International Monetary Fund. "Central Bank Digital Currency: Progress and Further Considerations." 2024. https://www.imf.org/-/media/files/publications/pp/2024/english/ppea2024052.pdf.

[7] Cerutti, Eugenio, Melih Firat, and Hector Perez-Saiz. "Estimating the Impact of Digital Money on Cross-Border Flows: Scenario Analysis Covering the Intensive Margin." International Monetary Fund, 2025. https://www.imf.org/-/media/files/publications/ftn063/2025/english/ftnea2025002.pdf.

[8] Financial Action Task Force. "Targeted Update on Implementation of FATF Standards on Virtual Assets and VASPs." 2024. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf.

[9] European Banking Authority. "EBA Statement on Crypto-Asset Developments." July 5, 2024. https://www.eba.europa.eu/sites/default/files/2024-07/7dcd9ce9-96e3-4c5c-8d86-39d7784d1f03/EBA%20statement%20on%20Application%20of%20MiCAR%20to%20ARTs%20and%20EMTs.pdf.

[10] Hong Kong Monetary Authority. "Robust and Sustainable Development of Stablecoins." 2025. https://www.hkma.gov.hk/eng/news-and-media/insight/2025/06/20250623.

[11] Singh, Onkar. "What Is JPMorgan's JPMD and Why It Matters." 2025. CCN. https://www.ccn.com/education/crypto/jpmorgans-jpmd-why-it-matters-explained.

[12] Garratt, Rod, Michael Lee, Antoine Martin, and Joseph Torregrossa. "The Future of Payments Is Not Stablecoins." Federal Reserve Bank of New York, 2022. https://libertystreeteconomics.newyorkfed.org/2022/02/the-future-of-payments-is-not-stablecoins.

[13] Bank for International Settlements and CPMI. "Tokenization in the Context of Money and Other Assets." 2024. https://www.fincen.gov/resources/statutes-regulations/guidance/funds-travel-regulations-questions-answers.

[14] Deutsche Bank, Memento Blockchain, and Axelar. "DAMA 2: Accelerated Asset Tokenization & Servicing for Regulated Institutions – A Layer 1-2-3 Solution." 2025. https://cdn.mementoblockchain.com/dama2/pdfs/DAMA-2-Lite-Paper_Jun172025.pdf.

[15] Guardian Asset & Wealth Management Industry Group. "Operationalising Tokenised Funds." Monetary Authority of Singapore, 2025. https://www.mas.gov.sg/-/media/mas-media-library/development/fintech/guardian/project-guardian-operationalising-tokenised-funds.pdf.

[16] Kowsar, Md Masud, and Abdul Awal Mintoo. "Blockchain in Banking: A Review of Distributed Ledger Applications in Loan Processing, Credit History, and Compliance." 2025. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5229956.

[17] American Institute of Certified Public Accountants. "Trust Services Criteria (SOC 2)." 2017 (updated 2022). https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2.

[18] National Institute of Standards and Technology. "SP 800-53 Rev.5: Audit and Accountability Controls." 2020. https://csf.tools/reference/nist-sp-800-53/r5.

[19] Olvis, E., and Gil Rios. "Framework for Blockchain Interoperability in Cross-Border Payments. " 2024. https://blockstand.eu/blockstand/uploads/2025/05/Framework_for_Blockchain_Interoperability_in_Cross_Border_Payments_version-v1.2.pdf.

[20] Pothula, Ram Mohan Reddy. "Revolutionizing Cross-Border Payments: A Technical Analysis of Blockchain Integration." 2025. Journal of West African Research and Reviews. https://journalwjarr.com/sites/default/files/fulltext_pdf/WJARR-2025-1321.pdf.

[21] Bank for International Settlements. "Project mBridge: Connecting Economies through CBDC." 2022. https://www.bis.org/publ/othp59.pdf.

[22] Rozovsky, Jason. "Programmable Interoperability: The Key to Standardisation in Regulating Tokenised Assets." Elevandi Knowledge Hub, 2024. https://www.elevandi.io/hubfs/Programmable%20Interoperability%20-%20The%20Key%20to%20Standardisation%20in%20Regulating%20Tokenized%20Assets%20-%20July%202024_Final.pdf.

[23] Digital Asset. "Canton Network Whitepaper: A Network of Networks for Smart Contracts." 2024. https://www.digitalasset.com/hubfs/Canton/Canton%20Network%20-%20White%20Paper.pdf.

[24] National Institute of Standards and Technology. "SP 800-161 Rev.1: Cybersecurity Supply Chain Risk Management Practices." 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.

[25] Saha, Reno, and Roy Koushik. "Navigating the Blockchain Trilemma: Advances in Decentralization, Security, and Scalability. 2025." Tech Science Press. https://www.techscience.com/cmc/v84n2/62936/html.

[26] Khandakar Md Shafin, and Reno Saha. "Resolving the Blockchain Trilemma: An Integrated Consensus Mechanism." 2025. Springer. https://link.springer.com/article/10.3103/S0146411625700476.

[27] National Institute of Standards and Technology. “SP 800-207: Zero Trust Architecture.” 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[28] Enterprise Ethereum Alliance. “Enterprise Ethereum Permissioned Blockchain Specification.” 2020. https://entethalliance.org/wp-content/uploads/2025/03/EEA_Enterprise_Ethereum_Permissioned_Blockchains_Specification_v2.pdf.

[29] Enterprise Ethereum Alliance. “Permissioned Blockchains Specification v3.” 2022. https://entethalliance.github.io/client-spec/chainspec.html.

[30] Wood, Gavin. “The Join-Accumulate Machine: A Mostly-Coherent Trustless Supercomputer.” 2024. https://graypaper.com.

[31] Auer, Raphael. “Embedded Supervision: How to Build Regulation into Decentralised Finance.” BIS Working Papers No. 811, 2019. https://www.bis.org/publ/work811.pdf.

[32] Bank for International Settlements and CPMI. “Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework.” 2019. https://www.bis.org/cpmi/publ/d157.pdf.

[33] UBS. “Project mBridge: UBS Submission on Potential Applications with a Focus on the Greater Bay Area.” 2021. https://www.ubs.com/content/dam/assets/ib/global/doc/m-cbdc-bridge.pdf.

[34] Reslow, André, Gabriel Söderberg, and Natsuki Tsuda. “Cross-Border Payments with Retail Central Bank Digital Currencies: Design and Policy Considerations.” International Monetary Fund, 2024. https://www.imf.org/-/media/files/publications/ftn063/2024/english/ftnea2024002.pdf.

[35] National Institute of Standards and Technology. “FIPS PUB 140-3: Security Requirements for Cryptographic Modules.” 2019. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf.

[36] Koolen, Christof. “Transparency and Consent in Data-Driven Smart Environments.” 2020. ResearchGate. https://www.researchgate.net/publication/342426319_Transparency_and_Consent_in_Data-Driven_Smart_Environments.

[37] Hong Kong Monetary Authority. “Distributed Ledger Technology in the Financial Sector: Opportunities and Challenges.” 2025. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/DLT_Research_Paper.pdf.

[38] SWIFT. “SWIFT to Add Blockchain-Based Ledger to Its Infrastructure Stack.” 2025. https://www.swift.com/news-events/press-releases/swift-add-blockchain-based-ledger-its-infrastructure-stack-groundbreaking-move-accelerate-and-scale-benefits-digital-finance.

[39] European Securities and Markets Authority. “Public Statement on the Provision of Certain Crypto-Asset Services in Relation to Non-MiCA Compliant ARTs and EMTs.” 2025. https://www.esma.europa.eu/sites/default/files/2025-01/ESMA75-223375936-6099_Statement_on_stablecoins.pdf.

[40] [SWIFT. “Standards MT: November 2026 High-Level Information.” 2025. https://www2.swift.com/knowledgecentre/publications/stdsmt_nov_2026_h_lvl_info/1.0.

[41] SWIFT. “ISO 20022 for Financial Institutions: Focus on Payment Instructions.” 2025. https://www.swift.com/standards/iso-20022/iso-20022-financial-institutions-focus-payments-instructions.

[42] ISO. “ISO 20022 Messages Archive.” https://www.iso20022.org/catalogue-messages/iso-20022-messages-archive.

[43] Enria, Andrea. “Regulating Crypto Finance: Taking Stock and Looking Ahead.” 2023. European Central Bank. https://www.bankingsupervision.europa.eu/press/speeches/date/2023/html/ssm.sp231114~fd1b2cc234.en.html.

[44] Enterprise Ethereum Alliance. “EthTrust Security Levels: Smart Contract Security Certification.” 2022. https://entethalliance.org/enterprise-ethereum-alliance-advances-smart-contract-security-with-ethtrust-specification.

[45] Central Bank of the United Arab Emirates. “Digital Dirham: A Primer on the UAE’s Central Bank Digital Currency.” 2025. https://centralbank.ae/media/lczb23l4/cbdc-short-report_july.pdf.

[46] Financial Crimes Enforcement Network. “Application of FinCEN’s Regulations to Convertible Virtual Currencies.” 2019. https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[47] Monetary Authority of Singapore. “Payment Services Act 2019.” https://www.mas.gov.sg/regulation/acts/payment-services-act.

[48] Monetary Authority of Singapore. “Licensing for Payment Service Providers.” https://www.mas.gov.sg/regulation/payments/licensing-for-payment-service-providers.

[49] Bank for International Settlements; Illes, Anamaria; Kosse, Anneke; Wierts, Peter. “Advancing in Tandem: Results of the 2024 BIS Survey on CBDCs and Crypto.” BIS Papers No. 159, 2025. https://www.bis.org/publ/bppdf/bispap159.pdf.

[50] Auer, Raphael, Cyril Monnet, and Hyun Song Shin. “Decentralised Ledgers and the Governance of Money.” Journal of Financial Economics, vol. 167, 2025.

[51] Bank of England. “The Bank of England’s Approach to Innovation in Artificial Intelligence, Distributed Ledger Technology, and Quantum Computing.” 2025. https://www.bankofengland.co.uk/report/2025/the-boes-approach-to-innovation-in-ai-dlt-quantum-computing.

[52] International Monetary Fund; Koonprasert, Tayo Tunyathon; Kanada, Shiho; Tsuda, Natsuki; Reshidi, Edona. “CBDC Adoption: Inclusive Strategies for Intermediaries and Users.” 2024. https://www.imf.org/en/publications/fintech-notes/issues/2024/09/21/central-bank-digital-currency-adoption-inclusive-strategies-for-intermediaries-and-users-555118.

[53] United Nations Development Programme. “Driving Financial Inclusion Through Central Bank Digital Currencies.” 2025. https://www.undp.org/sites/g/files/zskgke326/files/2025-06/undp-driving-financial-inclusion-through-cbdcs.pdf.

[54] National Institute of Standards and Technology. “SP 800-57 Part 1 Rev.5: Recommendation for Key Management.” 2020. https://www.nist.gov.

[55] National Institute of Standards and Technology. “FIPS 140-3: Cryptographic Module Validation Program.” 2019. https://resources-library.keyfactor.com/l/all-content.

[56] National Institute of Standards and Technology. “SP 800-171 Rev.2: Protecting Controlled Unclassified Information.” 2020. https://www.nist.gov.

[57] National Telecommunications and Information Administration. “The Minimum Elements for a Software Bill of Materials (SBOM).” 2021. https://www.ntia.gov/sites/default/files/publications/sbom_minimum_elements_report_0.pdf.

[58] National Institute of Standards and Technology. “SP 800-53 Rev.5: Security and Privacy Controls for Information Systems.” 2020. https://www.nist.gov.

[59] National Institute of Standards and Technology. “SP 800-218 Rev.1: Secure Software Development Framework (SSDF).” 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf.

[60] National Institute of Standards and Technology. “Cybersecurity Framework Version 1.1.” 2018. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.

[61] ISO/IEC. “ISO/IEC 27001:2022 – Information Security Management Systems.” 2022. https://www.iso.org/standard/54534.html.

[62] ISO/IEC. “ISO/IEC 27005:2022 – Information Security Risk Management.” 2022. https://www.iso.org/standard/80585.html.

[63] ISO/IEC. “ISO/IEC 27001:2022 Annex A Controls.” 2022. https://hightable.io/iso-27001-annex-a-8-13-information-backup.

[64] IEEE Consumer Technology Society. “Active Project Authorization Requests (PARs).” June 2022. https://ctsoc.ieee.org/industry-and-standards-activities/scs.html.

A8. References | A8. 文献参考

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). “Article 5(1)(c), Principle of Data Minimization.” Official Journal of the European Union, 2016. https://www.gdprregulation.eu/gdpr-principles.

[2] Financial Action Task Force (FATF). “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations.” FATF, updated October 2025. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

[3] Financial Action Task Force (FATF). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (RBA-VA-VASPs). FATF, June 21, 2019. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html.

[4] European Parliament and Council of the European Union. “Regulation (EU) 2016/679 (General Data Protection Regulation), Article 5(1)(e) – Storage Limitation.” Official Journal of the European Union, 2016. https://www.gdpr.org/regulation/article-5.html.

General Terminology Glossary
通用术语表

This glossary consolidates the core terminology, conceptual definitions, and related abbreviations used throughout the Black Paper, covering blockchain and cryptographic engineering, financial market infrastructures and cross-border clearing and settlement, as well as regulatory bodies, legal frameworks, and regional pilot initiatives.

It serves as a unified terminological anchor across all chapters, explicitly defining the scope, applicable subjects, and boundaries of each term.

本术语表汇总了黑皮书全文中使用的核心术语、概念定义及相关缩写，涵盖区块链与密码学工程、金融市场基础设施与跨境清算结算体系，以及监管机构、法律框架与区域试点项目等领域。

该术语表作为贯穿全书的统一术语基准，用于明确各术语的含义范围、适用对象及其边界。

Part A: Common Terms in Blockchain, Cryptographic Engineering, and Ecosystems

A 部分：区块链、密码学工程与生态系统通用术语

- **Distributed Ledger Technology (DLT).**

  A technology for a database that is synchronously shared, replicated, and consented upon across multiple nodes, geographical locations, or institutions. Blockchain is one form of DLT, but not all DLTs use a chained block structure. The core of DLT is enabling participants to maintain a trusted, consistent record without a central coordinator.

- **分布式账本技术（DLT）**

  一种数据库技术，其数据在多个节点、地理位置或机构之间同 步 共享、复制并通过共识机制达成一致。区块链是 DLT 的一种实现形式，但并非所有 DLT 都采用链式区块结构。DLT 的核心在于，在没有中心协调者的情况下，使参与方能够共同维护一 份 可信且一致的记录。

- **Bitcoin.**

  A digital currency and payment system based on a decentralized peer-to-peer network, proposed by Satoshi Nakamoto in 2008 and launched in 2009. It does not rely on any central authority for issuance or management. Security and immutability are ensured through the Proof of Work (PoW) consensus mechanism and a public distributed ledger. With a total supply cap of 21 million, it aims to be a censorship-resistant, globally accessible store of value and medium of exchange.

- **比特币**

  一种基于去中心化点对点网络的数字货币与支付系统，由中本聪于 2008 年提出，并于 2009 年上线运行。比特币不依赖任何中央机构发行或管理，其安全性与不可篡改性通过工作量证明（PoW）共识机制和公开分布式账本实现。总发行量上限为 2100 万枚，其设计目标是成为一种抗审查、全球可访问的价值储存与交换媒介。

- **Blockchain.**

  A technology that uses cryptographic methods to connect data blocks in chronological order, forming an

- **区块链**

  一种利用密码学方法将数据区块按时间顺序连接起来的技术，从而形成不可篡改的去中心化或分布式共享账本。

immutable, decentralized, or distributed shared ledger. Its core characteristics include decentralization, transparency, immutability, and programmability. It is considered the foundational infrastructure for building trusted digital collaboration.

其核心特征包括去中心化、透明性、不可篡改性和可编程性，被视为构建可信数字协作的重要基础设施。

- **Consensus Mechanism.**

  A set of rules and algorithms that enables nodes in a distributed network to agree on the shared state of the system, including the order and validity of transactions. Consensus mechanisms ensure consistency and fault tolerance across decentralized systems. In practice, they may rely either on economic-incentive mechanisms (such as Proof of Work or Proof of Stake) or on Byzantine Fault Tolerant agreement protocols used in permissioned distributed ledger systems.

- **共识机制**

  一组规则与算法，用于使分布式网络中的节点就系统共享状态达成一致，包括交易顺序与有效性的 确 认。共识机制 确 保去中心化系统的一致性与容错能力。实践中既可能依赖经济激励机制（如 PoW 或 PoS），也可能采用拜占庭容错协议。

- **Proof of Work (PoW).**

  A consensus mechanism used in distributed networks to prevent malicious behavior, such as double-spending. Nodes (miners) compete to solve a cryptographic puzzle by performing computational work (hashing). The first node to solve the puzzle gains the right to propose the next block and receives a reward. By making block production computationally expensive, PoW increases the economic cost of attacks on the network. However, its high energy consumption is frequently debated.

- **工作量证明（PoW）**

  一种用于防止恶意行为（如双重支付）的共识机制。节点通过计算密集型的哈希运算竞争解决密码学难题，最先完成计算的节点获得生成新区块的权利并获得奖励。PoW 通过提高攻击网络的经济成本来增强系统安全性，但其高能耗问题也长期存在争议。

- **Byzantine Fault Tolerance (BFT).**

  A class of consensus protocols designed to ensure that a distributed system can reach agreement even when some nodes behave maliciously or unpredictably (Byzantine faults). BFT-based consensus mechanisms rely on message exchange and voting among a known set of validator nodes to agree on the order and validity of transactions. Such protocols are commonly used in permissioned distributed ledger systems where participants are identifiable and authorized. Common implementations of Byzantine Fault Tolerant consensus include PBFT (Practical Byzantine Fault Tolerance), Tendermint, HotStuff, IBFT (Istanbul BFT), QBFT (Quorum BFT), and HoneyBadgerBFT.

- **拜占庭容错（BFT）**

  一类共识协议，用于 确 保分布式系统即使在部分节点出现恶意或异常行为时仍能达成一致。BFT 共识通常通过已知验证节点之间的消息交换与投票机制实现，常用于许可型分布式账本系统。常见实现包括 PBFT、Tendermint、HotStuff、IBFT、QBFT 和 HoneyBadgerBFT。

- **Byzantine Fault.**

  A failure condition in a distributed system where a node behaves arbitrarily, including maliciously or inconsistently, potentially sending conflicting information to different participants.

- **拜占庭故障**

  分布式系统中的一种故障类型，指节点出现任意行为，包括恶意行为或不一致行为，并可能向不同参与方发送相互矛盾的信息。

- **Cryptography.**

  A branch of mathematics and computer science that uses cryptographic techniques to secure information and communications. It enables confidentiality, data integrity, authentication, and non-repudiation through mechanisms such as encryption, digital signatures, hash functions, and cryptographic proofs. In distributed ledger systems, cryptography is used to verify transaction authenticity, protect data integrity, and ensure that only authorized parties can control digital assets.

- **密码学**

  利用数学与计算机科学方法保护信息安全的技术领域，通过加密、数字签名、哈希函数与密码学证明等手段实现机密性、完整性、身 份 认证与不可抵赖性。在分布式账本系统中，密码学用于验证交易真实性、保护数据完整性并 确 保资产控制权仅属于授权方。

- **Smart Contract.**

  Executable program logic deployed on a distributed ledger that automatically executes predefined rules when specified conditions are satisfied. Smart contracts enable deterministic processing of transactions and state transitions across participating nodes without requiring manual intervention. In distributed ledger systems, they are used to automate business logic, enforce protocol rules, and coordinate interactions among authorized participants.

- **智能合约**

  部署在分布式账本上的可执行程序逻辑，当预设条件满足时自动执行相应规则。智能合约使交易处理与状态变更能够在各节点间以 确 定性方式自动执行，无需人工干预，常用于自动化业务逻辑与协议规则。

- **Programmability.**

  In distributed ledger systems, the capability to execute predefined program logic that governs how transactions are processed and how assets or states change over time. This enables automated enforcement of rules and workflows, supporting applications such as programmable payments, automated bond coupon distribution, and conditional asset transfers beyond simple value transfer.

- **可编程性**

  分布式账本系统执行预定义程序逻辑以控制交易处理和资产状态变化的能力，从而实现规则自动执行与流程自动化。例如可编程支付、自动债券付息或条件资产转移。

- **Permissionless.**

  A system characteristic where anyone can join the network (as a node), use services (initiate transactions), or participate in consensus (e.g., mining) without approval from a central authority. Public chains like Bitcoin and Ethereum are typical permissionless systems, contrasting with "permissioned chains" that require authorization.

- **无需许可**

  一种系统特性，任何人无需获得中心机构批准即可加入网络（运行节点）、使用服务（发起交易）或参与共识（如挖矿）。比特币和以太坊是典型的无需许可系统。

- **Permissioned.**

  A system characteristic where participation in the network - such as operating nodes, accessing services, or participating in consensus, is restricted to entities that have received prior authorization from a governing authority or consortium. Permissioned distributed ledger systems are typically used in institutional or enterprise environments, where participants are known, vetted, and subject to defined governance and compliance requirements. This model contrasts with permissionless systems, where participation is open to anyone without prior approval.

- **许可型**

  一种系统特性，网络参与权限（如运行节点、访问服务或参与共识）需经治理机构或联盟授权。许可型分布式账本通常用于机构或企业环境，参与方身 份 明 确 并受治理与合规约束。

- **Verifiability.**

  In computer science and cryptography, the characteristic where the output of a system or calculation can be independently verified by a third party using public information. In blockchain, this means anyone can verify transaction validity and block correctness without trusting a single node.

- **可验证性**

  在计算机科学与密码学中，指系统输出或计算结果能够由第三方利用公开信息独立进行验证的特性。在区块链体系中，这意味着任何人都可以在不依赖单一节点信任的情况下，自行验证交易的有效性以及区块的正 确 性。

- **Governance.**

  The set of processes, rules, and decision-making mechanisms through which participants determine protocol upgrades, parameter adjustments, resource allocation, and the future direction of a distributed system. Governance may operate on-chain (for example, through protocol-level voting mechanisms) or off-chain (through committees, foundations, or other institutional arrangements), focusing on how decisions are made and who has the authority to make them.

- **治理机制**

  指参与者通过一系列流程、规则与决策机制，对分布式系统的协议升级、参数调整、资源分配以及未来发展方向作出决策的制度安排。治理可以在链上进行（例如通过协议级投票机制），也可以在链下进行（例如通过委员会、基金会或其他制度化组织）。其核心关注的是：决策如何产生，以及谁 拥 有作出决策的权力。

- **Interoperability.**

  The ability of different distributed ledger systems or financial infrastructures to exchange information, assets, or transactions and correctly interpret each other's data and rules. Interoperability enables coordinated operation across heterogeneous systems operated by different institutions or jurisdictions.

- **互操作性**

  指不同分布式账本系统或金融基础设施之间能够交换信息、资产或交易，并正 确 理解和执行彼此数据结构与规则的能力。互操作性使得由不同机构或不同司法辖区运营的异构系统之间能够实现协同运行。

- **Trusted Execution Environment (TEE).**

  A hardware-based secure area within a main processor that ensures the confidentiality (protection from external snooping) and integrity (protection from tampering) of the

- **可信执行环境（TEE）**

  一种基于硬件实现的安全执行区域，位于主处理器内部，用于 确 保其中运行的代码和数据在执行过程中的机密性（防止外部窥探）与完整性（防止被篡改）。在区块链系

code and data loaded inside it. In blockchain, TEEs are often used for privacy-preserving computation or providing security for consensus roles, though they introduce trust assumptions regarding hardware vendors.

统中，TEE 常用于支持隐私计算或为部分共识角色提供安全执行环境，但同时也会引入对硬件厂商可信性的依赖假设。

- **Threshold Signature Scheme (TSS).**

  A cryptographic signature scheme in which the ability to generate a valid digital signature is distributed among multiple participants. A signature can only be produced when a predefined subset of participants - typically expressed as an N-of-M threshold - cooperates, while fewer than the threshold cannot generate the signature or reconstruct the private key. Threshold signatures are widely used in distributed key management, multi-party computation, and fault-tolerant authorization systems.

- **门限签名方案（TSS）**

  一种密码学签名机制，其中生成有效数字签名的能力被分散在多个参与方之间。只有当预先设定数量的参与者（通常表示为 N-of-M 门限）协同参与时，才能生成有效签名；低于该门限的参与方既无法生成签名，也无法重构私钥。门限签名广泛应用于分布式密钥管理、多方安全计算以及具备容错能力的授权系统。

- **Node.**

  A computer or server that participates in a blockchain or distributed network by running specific client software. Nodes are responsible for maintaining the network, verifying and propagating transactions and blocks, and updating the ledger state according to consensus rules.

- **节点**

  指在区块链或分布式网络中运行特定客户端软件的计算机或服务器。节点负责维护网络运行，包括验证并传播交易与区块，并依据共识规则更新账本状态。

- **Validator.**

  A network participant with node responsible for verifying transactions, participating in consensus, and maintaining the integrity of the distributed ledger.

- **验证节点**

  指在网络中承担交易验证和共识参与职责的节点角色。验证节点通过执行共识协议 确 认交易有效性，并共同维护分布式账本的完整性与一致性。

- **Transaction Binding.**

  A technique used during transaction creation to bind all critical input parameters (e.g., amount, counterparty), referenced business rule versions, and the current context into a single, indivisible data unit via cryptographic hashes or commitment mechanisms. This ensures the full execution context is solidified, preventing selective tampering or re-interpretation after the fact, thereby enabling deterministic replay audits.

- **事务绑定**

  一种在交易生成阶段使用的技术，通过密码学哈希或承诺机制，将交易的关键输入参数（如金额、交易对手方）、所引用的业务规则版本以及当时的执行上下文绑定为一个不可分割的数据整体。该机制可 确 保完整的执行环境被固化下来，从而防止事后选择性篡改或重新解释，并支持 确 定性重放审计。

- **Reconciliation and Replay.**

  The core auditing mechanism of verifiable systems. "Replay" refers to re-executing the entire business process in

- **对账与重放**

  可验证系统中的核心审计机制。“ 重放 ” 是指在一个独立且 确 定性的环境中，使用原始输入、绑定的规则版

an independent, deterministic environment using original inputs, bound rules, and full path proof to verify if the output matches the original record. "Reconciliation" in this context evolves into comparing independent replay results from multiple parties to mathematically verify process correctness, rather than just comparing static balances.

本以及完整的执行路径证明，对整个业务流程重新执行，以验证其输出是否与原始记录一致。“ 对账 ” 在此语境下不再只是比较静态余额，而是通过比较多方独立重放所得的结果，以数学方式验证流程执行的正 确 性。

- **Deterministic Execution.**

A property of a distributed system in which identical inputs, rules, and execution conditions always produce identical outputs. Deterministic execution enables independent replay and verification of transaction processing across different nodes or environments.

- **确定性执行**

分布式系统的一种属性：在输入、规则和执行条件完全相同的情况下，系统始终产生完全一致的输出。确 定性执行使得不同节点或独立环境能够对交易处理过程进行一致的重放与验证。

- **Provable Consistency.**

A property of a distributed system in which transaction execution and state transitions can be independently verified to be consistent with the declared rules and inputs. Through deterministic execution and cryptographic proofs, any participant can reproduce the same result and confirm that the system’s behavior matches the specified logic.

- **可证明一致性**

分布式系统的一种性质：交易执行及状态变更能够被独立验证，并与声明的规则和输入保持一致。通过 确 定性执行与密码学证明，任何参与方都可以复现相同结果，从而 确 认系统行为 确 实遵循既定逻辑。

- **Domain Model.**

A conceptual representation of the key entities, responsibilities, rules, and interactions within a particular area of a system or organization. In system architecture and domain-driven design, domain models are used to structure complex systems by defining clear functional domains and the relationships between them. In cross-jurisdictional financial infrastructures, domain modeling helps clarify responsibilities and interaction boundaries between different institutions or regulatory environments.

- **域模型**

对某一系统或组织特定业务领域中关键实体、职责、规则及其交互关系的概念性表示。在系统架构和领域驱动设计中，领域模型用于将复杂系统 划 分为清晰的功能域，并明 确 各域之间的关系。在跨司法辖区的金融基础设施中，领域建模有助于界定不同机构或监管环境之间的职责与交互边界。

- **Cross-Domain Communication Protocol.**

A protocol that enables the secure and verifiable exchange of messages, data, or transaction proofs between distinct trust domains, such as different distributed ledger systems, financial infrastructures, or sovereign jurisdictions. It defines message formats, routing logic, authentication mechanisms, and proof verification procedures to ensure integrity, traceability, and reliable delivery across system boundaries.

- **跨域通信协议**

一种协议，用于在不同信任域之间安全且可验证地交换消息、数据或交易证明，例如不同分布式账本系统、金融基础设施或主权司法辖区之间。该协议定义消息格式、路由逻辑、身 份 认证机制以及证明验证流程，以 确 保跨系统通信的完整性、可追溯性和可靠传递。

- **Cross-Chain Communication.**

  A category of interoperability techniques that enable data exchange, transaction coordination, or asset transfer between separate blockchain networks. Common approaches include relay-based architectures, hashed timelock contracts (HTLC), notary or validator schemes, and other mechanisms for verifying events across chains.

- **跨链通信**

  一类互操作技术，用于在不同区块链网络之间实现数据交换、交易协调或资产转移。常见方式包括中继架构、哈希时间锁合约（HTLC）、公证人或验证者机制等，用于在链间验证事件真实性。

- **Global Registry.**

  A shared infrastructure in cross-chain or cross-sovereign ecosystems used to centrally and authoritatively record and map the core identities and key metadata of participating entities. Usually maintained via decentralized or federated governance, it acts as the "address book" or "root directory" of the network.

- **全球注册表**

  在跨链或跨主权生态中使用的一种共享基础设施，用于集中且权威地记录参与实体的核心身 份 信息及关键元数据。通常通过去中心化或联盟式治理维护，类似整个网络的“ 地址簿 ”或“ 根目录 ”。

- **Hash Anchoring.**

  A cryptographic technique of recording the hash value (e.g.,digital fingerprint) of any data on an immutable distributed ledger (e.g., blockchain) or a trusted timestamp service. This "anchors" the existence and state of data at a specific point in time to a higher-level trust base, allowing for independent verification that the data has not been tampered with without disclosing the data itself.

- **哈希锚定**

  一种密码学技术，将任意数据的哈希值（数字指纹）记录到不可篡改的分布式账本（如区块链）或可信时间戳服务中，从而在某一时刻为该数据建立可信存在证明。通过这种方式，可以在不披露原始数据的情况下验证其未被篡改。

- **Heterogeneous Network.**

  A network environment composed of systems or blockchains with different types, architectures, consensus mechanisms, or governance models. In cross-border finance, it refers to digital currency or payment systems built by different sovereign nations using different technology stacks. Achieving interoperability between heterogeneous networks is a more significant challenge than in homogeneous ones.

- **异构网络**

  由不同类型系统或区块链组成的网络环境，这些系统在架构、共识机制或治理模式上可能各不相同。在跨境金融场景中，通常指由不同主权国家采用不同技术栈构建的数字货币或支付系统。相比同构网络，异构网络之间实现互操作的难度更高。

- **Merkle Proof.**

  A cryptographic method based on hash trees used to efficiently verify if a data block belongs to a larger dataset without exposing or downloading the entire set. It is core to blockchain light clients and state verification.

- **默克尔证明**

  一种基于哈希树（Merkle Tree）的密码学证明方法，用于高效验证某一数据块是否属于某个更大的数据集合，而无需下载或暴露全部数据。该机制是区块链轻客户端与状态验证的核心技术之一。

Part B:
Common Terms in Financial Market Infrastructure and Cross-Border Clearing and Settlement

B 部分：
金融市场基础设施与跨境清算结算常用术语

- **Central Bank Digital Currency (CBDC).**

  A digital form of fiat currency issued and backed by a country's central bank. It represents a direct liability of the central bank, aiming to combine the technical advantages of digital currency (e.g., programmability, real-time clearing) with the credit stability of fiat. It is generally categorized into retail CBDC for the public and wholesale CBDC for financial institutions.

- **中央银行数字货币（CBDC）**

  由一国中央银行发行并提供信用背书的法定货币数字形态。CBDC 直接体现为中央银行的负债，旨在将数字货币的技术优势（如可编程性、实时清算能力）与法币体系的信用稳定性相结合。通常分为面向公众的零售型 CBDC 与面向金融机构的批发型 CBDC。

- **Real-Time Gross Settlement (RTGS).**

  A high-value payment system where payment instructions are settled individually, in full, and continuously across participants' accounts at the central bank. Every settlement is final and irrevocable, primarily used for urgent, high-value payments as a core financial infrastructure.

- **实时全额结算系统（RTGS）**

  一种高价值支付系统，支付指令在参与机构的中央银行账户之间以逐笔、全额、实时方式完成结算。每 一笔交易一经结算即具有最终性且不可撤销，主要用于紧急或大额支付，是现代金融体系的核心基础设施之一。

- **Central Securities Depository (CSD).**

  A core financial infrastructure that provides centralized custody, registration, clearing, and settlement services for securities within a country or market. It records security ownership via electronic ledgers to eliminate physical certificate risks and improve market efficiency.

- **中央证券存管机构（CSD）**

  为一国或一个市场提供证券集中托管、登记、清算与结算服务的核心金融基础设施。CSD 通过电子账簿记录证券所有权，取代传统的纸质证券凭证，从而降低实物证书风险并提升市场运行效率。

- **Society for Worldwide Interbank Financial Telecommunication (SWIFT)**

  The world’s primary financial messaging network used by financial institutions to transmit standardized payment instructions and securities transaction info. It does not process fund transfers itself but transmits instructions. It serves over 11,000 institutions across 200+ countries, and its message standards (MT and ISO 20022) are the industry's common language.

- **环球银行金融电信协会（SWIFT）**

  全球最主要的金融信息传输网络，金融机构通过其发送标准化的支付指令与证券交易信息。SWIFT 本身并不进行资金清算或转移，而是负责安全、标准化的信息传递。目前服务全球 200 多个国家和地区、超过 11,000 家机构，其报文标准（如 MT 与 ISO 20022）已成为国际金融业的通用语言。

- **Clearing House Interbank Payments System (CHIPS).**

  The world's largest private-sector USD large-value cross-border payment clearing system, handling over 95% of cross-border USD payments. It uses a multilateral netting mechanism and settles finally through the Federal Reserve's Fedwire at the end of the day.

- **清算所银行同业支付系统（CHIPS）**

  全球规模最大的美元跨境大额支付清算系统，处理超过95% 的跨境美元支付业务。CHIPS 采用多边净额结算机制，并在每日结束时通过美国联邦储备系统的 Fedwire 完成最终资金结算。

- **Trans-European Automated Real-time Gross Settlement Express Transfer System (TARGET).**

  An RTGS system developed and operated by the Eurosystem (ECB and national central banks). It is the backbone for large-value Euro payments, ensuring funds move between Eurozone banks in a final and irrevocable manner.

- **泛欧实时全额自动清算系统（TARGET）**

  由欧元体系（欧洲中央银行及各成员国中央银行）开发并运营的一套实时全额结算（RTGS）系统，是欧元区大额支付清算的核心基础设施。该系统 确 保欧元区银行之间的资金转移能够实时完成，并具备最终且不可撤销的结算效力。

- **Cross-Border Interbank Payment System (CIPS).**

  Organized by the People's Bank of China to provide clearing and settlement services for cross-border and offshore RMB business. Unlike SWIFT, which primarily transmits messages, CIPS integrates payment clearing and messaging functions to improve RMB cross-border efficiency and security.

- **人民币跨境银行间支付系统（CIPS）**

  由中国人民银行组织建设并运营，为跨境及离岸人民币业务提供清算与结算服务的支付基础设施。不同于主要承担报文传输功能的 SWIFT 系统，CIPS 同时整合了支付清算与信息传输功能，以提升人民币跨境支付的效率与安全性。

- **Clearing House Automated Payment System (CHAPS).**

  The UK's primary GBP large-value RTGS system operated by the Bank of England. It handles high-value, time-sensitive GBP payments (e.g., real estate settlements, large commercial payments) and ensure payment finality.

- **清算所自动支付系统（CHAPS）**

  英国最重要的英镑大额实时全额结算（RTGS）系统，由英格兰银行运营。它处理英国国内高价值的、时间敏感的英镑支付（如房地产交易结算、大型商业支付），以及部分跨境英镑支付，确 保支付的最终性和不可撤销性。

- **ISO 20022.**

  A global financial messaging standard methodology from the International Organization for Standardization (ISO). It provides a unified XML-based data model and business process for payments, securities, and forex. Its flexible structure and rich data fields are making it the new global unified standard.

- **ISO 20022 金融报文标准**

  由国际标准化组织（ISO）制定的一套全球金融报文标准方法体系。该标准通过统一的 XML 数据模型与业务流程描述框架，支持支付、证券及外汇等金融业务的信息交换。凭借其灵活的数据结构和 丰 富的信息字段，ISO 20022 正逐 步 成为全球金融通信的统一标准。

- **Correspondent Bank.**

  A cross-border payment arrangement where one bank (correspondent) opens an account for another (respondent) to provide clearing and forex services, allowing the respondent bank indirect access to the correspondent's local payment system. While the core traditional model, it is often long, costly, and lacks transparency.

- **代理行**

  一种跨境支付安排模式，即一家银行（代理行）为另一家银行（被代理行）开设账户，并提供清算与外汇服务，使后者能够间接接入代理行所在国家或地区的本地支付系统。尽管这是传统跨境支付体系的核心模式，但其流程通常较为复杂，成本较高，且透明度有限。

- **Clearing.**

  The process between transaction execution and settlement, including trade confirmation, reconciliation, and netting of positions to determine final settlement obligations.

- **清算**

  指交易执行与最终结算之间的处理过程，包括交易确认、账目核对以及头寸净额计算等步骤，用于确定各参与方在结算时应履行的最终支付义务。

- **Finality.**

  The point at which a transaction or ledger change becomes certain and irreversible. Under legal finality, it is unaffected by bankruptcy or legal proceedings; under technical finality, the system will not roll back the transaction.

- **结算终局性**

  指一笔交易或账本状态变更被最终确认、且不可撤销的时点。在法律终局性层面，该结果不受破产或法律程序影响；在技术终局性层面，系统在共识完成后不会再回滚该交易。

- **Embedded Supervision.**

  A regulatory paradigm proposed by the BIS where regulatory requirements are directly embedded into the IT systems and operational processes of regulated institutions. By analyzing trusted data (e.g., DLT) in real-time, regulators can move from ex-post inspections to continuous monitoring.

- **嵌入式监管**

  一种由 BIS 提出的监管范式，即将监管规则直接嵌入到受监管机构的信息系统和业务流程之中。监管机构通过实时分析可信数据（如分布式账本数据），可以将传统的事后检查转变为持续、实时的监管监测。

- **Delivery versus Payment (DvP).**

  A securities settlement mechanism ensuring that the delivery of securities occurs if and only if the corresponding payment occurs. This link eliminates principal risk where one party performs and the other defaults.

- **券款对付（DvP）**

  一种证券结算机制，确保证券交付仅在对应资金支付同时完成时才会发生。该机制通过将证券转移与资金支付绑定执行，从而消除一方履约而另一方违约所产生的本金风险。

- **Payment versus Payment (PvP).**

  A settlement mechanism for forex transactions involving two different currencies. It ensures the payment of one currency occurs if and only if the payment of the other currency occurs, eliminating risks from time zone or process differences.

- **支付对支付（PvP）**

  一种用于外汇交易结算的机制，涉及两种不同货币。其核心原则是：一种货币的支付只有在另一种货币同时完成支付时才会发生，从而避免因时区差异或流程延迟导致的一方付款而另一方未付款的风险。

- **Regulatory Sandbox.**

  A controlled testing environment created by regulators for fintech startups and traditional institutions to test innovative products with limited real-market scope under temporary regulatory exemptions.

- **监管沙盒**

  由监管机构设立的受控测试环境，允许金融科技企业或传统金融机构在限定的真实市场范围内测试创新产品或服务，并在一定期限内 适用临时性监管豁免或调整规则，以降低创新试验的合规风险。

Part C: Common Terms in Regulatory Bodies, Laws, and Regional Pilots

C 部分：监管机构、法律法规与区域试点常用术语

- **Bank for International Settlements (BIS).**

  Established in 1930, the "bank for central banks" promotes cooperation among central banks and financial regulators to maintain monetary stability. Its Committee on Payments and Market Infrastructures (CPMI) sets global standards for payment and settlement.

- **国际清算银行（BIS）**

  成立于 1930 年，被称为 “ 中央银行的银行 ”，旨在促进各国中央银行与金融监管机构之间的合作，以维护全球货币与金融体系的稳定。其下属的支付与市场基础设施委员会（CPMI）负责制定全球支付与结算体系的重要标准。

- **Monetary Authority of Singapore (MAS).**

  Singapore's central bank and integrated financial regulator. It manages monetary policy, financial supervision, and payment systems, and actively promotes fintech innovation (e.g., Project Guardian).

- **新加坡金融管理局（MAS）**

  新加坡的中央银行及综合金融监管机构，负责货币政策、金融监管以及国家支付体系的管理，同时积极推动金融科技创新，例如 Project Guardian 等项目。

- **Hong Kong Monetary Authority (HKMA).**

  Hong Kong’s central banking institution, responsible for currency and banking stability, and actively researching wholesale CBDC (wCBDC) and stablecoin regulation.

- **香港金融管理局（HKMA）**

  香港的中央银行机构，负责维护货币与银行体系稳定，并积极开展批发型中央银行数字货币（wCBDC）及稳定币监管框架的研究与探索。

- **Swiss DLT Policy Template for Securities.**

  A regulatory classification and policy framework by FINMA (Swiss Financial Market Supervisory Authority) for securities issued and traded on DLT (security tokens).

- **瑞士基于 DLT 的证券监管政策框架**

  瑞士金融市场监督管理局（FINMA）为基于分布式账本技术发行和交易的证券（证券型代币）提供的监管分类和政策解释框架，旨在为创新提供法律 确 定性。

- **Central Bank of the United Arab Emirates (CBUAE).**

  The UAE central bank responsible for monetary policy and supervising the banking industry; it leads the "Digital Dirham" CBDC project.

- **阿联酋中央银行（CBUAE）**

  阿拉伯联合酋长国的中央银行，负责制定货币政策并监管银行体系，同时主导推进 “ 数字迪拉姆 ” 中央银行数字货币项目。

- **Dubai Financial Services Authority (DFSA).**

  An independent regulator for financial services within the Dubai International Financial Centre (DIFC), which has its own legal system independent of UAE federal law.

- **迪拜金融服务管理局（DFSA）**

  迪拜国际金融中心（DIFC）的独立金融监管机构。DIFC 具有独立于阿联酋联邦法律体系的法律与司法框架，DFSA 负责该区域内的金融服务监管。

- **Financial Services Regulatory Authority of Abu Dhabi Global Market (FSRA of ADGM).**

  The independent regulator for financial activities within Abu Dhabi Global Market, a free zone with its own legal system.

- **阿布扎比全球市场金融服务监管局（FSRA of ADGM）**

  阿布扎比全球市场（ADGM）自由区内的独立金融监管机构。ADGM 拥 有独立的法律体系与监管框架，FSRA 负责该区域内金融活动的监管。

- **Financial Crimes Enforcement Network (FinCEN).**

  A bureau of the US Treasury that analyzes financial transaction info to combat domestic and international money laundering and terrorism financing.

- **美国金融犯罪执法网络（FinCEN）**

  隶属于美国财政部的机构，负责收集和分析金融交易信息，以打击国内及跨国的洗钱活动与恐怖融资行为。

- **Office of Foreign Assets Control (OFAC).**

  A US Treasury agency that administers and enforces economic and trade sanctions against targeted countries, regimes, terrorists, and international drug traffickers.

- **美国外国资产控制办公室（OFAC）**

  美国财政部下属机构，负责制定并执行针对特定国家、政权、组织及个人的经济与贸易制裁，包括恐怖组织和国际毒品犯罪网络等对象。

- **Specially Designated Nationals List (SDN List).**

  A list maintained by OFAC of individuals and entities subject to US economic sanctions. US persons/entities are generally prohibited from transactions with these parties and must freeze their assets.

- **特别指定国民清单（SDN List）**

  由美国财政部海外资产控制办公室维护的制裁名单，列示受美国经济制裁的个人与实体。美国主体原则上不得与名单对象发生交易，并须对其资产实施冻结。

- **Gold Exchange Standard.**

  A monetary system where a currency is not directly linked to gold but to another currency (usually the USD) that is linked to gold. The Bretton Woods system (1944) is a classic example.

- **金汇兑本位制**

  一种货币制度，本币并不直接锚定黄金，而是锚定 另一种与黄金挂钩的货币（通常为美元）。1944 年的布雷顿森林体系即为典型代表。

- **Floating Exchange Rate System.**

  A system where the exchange rate is freely determined by market supply and demand, with central banks generally not intervening.

- **浮动汇率制度**

  汇率主要由市场供求关系决定，中央银行通常不进行常态化干预的汇率形成机制。

- **Anti-Money Laundering (AML).**

  Laws and procedures designed to prevent criminals from disguising illegal funds as legitimate income. Institutions must conduct due diligence and report suspicious transactions.

- **Countering the Financing of Terrorism (CFT).**

  Measures to prevent, detect, and block the provision or collection of funds for terrorist activities or organizations.

- **Markets in Crypto-Assets Regulation (MiCA).**

  A comprehensive framework of regulations established by the European Union to regulate crypto-assets. It sets unified rules for the operation of Crypto-Asset Service Providers (CASPs), requirements for stablecoin issuers, consumer protection, and market transparency, aiming to provide legal certainty for the crypto-asset market within the EU and mitigate associated risks.

- **Digital Operational Resilience Act (DORA).**

  An EU regulation that requires financial entities (including banks, insurance companies, and crypto-asset service providers) to ensure their Information and Communication Technology (ICT) systems can withstand, respond to, and recover from all types of ICT-related disruptions and threats. It covers ICT risk management, incident reporting, resilience testing, and third-party provider risk management.

- **Electronic Money Token (EMT).**

  As defined under the EU Markets in Crypto-Assets (MiCA) regulation, it refers to a type of crypto-asset that is primarily intended to be used as a means of exchange and that purports to maintain a stable value by referencing the value of a single official currency of a country (fiat currency). The issuer of such tokens must be an authorized electronic money institution or credit institution.

- **Travel Rule.**

  A FATF standard requiring Virtual Asset Service Providers (VASPs) to transmit originator and beneficiary identity info to counterparty VASPs for transactions above a certain threshold.

- **反洗钱（AML）**

  旨在防止非法资金通过伪装转化为合法收入的一整套法律与监管程序。金融机构需履行客户尽职调查义务，并对可疑交易进行报告。

- **反恐融资(CFT)**

  用于预防、识别并阻断资金被用于恐怖主义活动或相关组织的制度与措施体系。

- **加密资产市场监管条例（MiCA）**

  欧盟建立的一套系统性加密资产监管框架，对加密资产服务提供商（CASPs）的运营、稳定币发行人要求、消费者保护及市场透明度作出统一规定，旨在为欧盟加密资产市场提供法律 确 定性并降低相关风险。

- **数字运营韧性法案（DORA）**

  欧盟法规，要求包括银行、保险机构及加密资产服务提供商在内的金融机构，确 保其信息与通信技术（ICT）系统具备抵御、响应及 恢 复各类技术性中断与威胁的能力。涵盖 ICT 风险管理、事件报告、韧性测试及第三方服务商风险管理等内容。

- **电子货币代币（EMT）**

  根据欧盟《加密资产市场监管条例》（MiCA）的定义，指主要用于支付用途，并通过锚定单一法定货币价值以维持稳定价格的一类加密资产。其发行人必须为经授权的电子货币机构或信贷机构。

- **旅行规则**

  由金融行动特别工作组（FATF）提出的监管标准，要求虚拟资产服务提供商（VASPs）在超过特定金额阈值的交易中，向交易对手方传递付款人及收款人的身 份 信息。

Black Paper: The Principia of Sovereign Digital Interoperability

《黑皮书：主权间数字互操作元宪章》

DOCUMENT INFO | 文档信息

Version / **版本：** v1.0

Release / **发布：** Jun 2026 / 2026 年 6 月

Status / **状态：** Stable / 正式版

theprincipia.org