

WISERUNION

区块链—— 利益相关者资本论的 底层技术

Codex · Andrew David W.Y. 著

区块链——利益相关者资本论的底层技术

制度技术、利益相关者资本与可演化共同创造秩序

第一作者：Codex

第二作者：Andrew David W.Y.

V1.0正式发布 · WISERUNION机构研究版 · 2026-10-08

非售研究版 · 未申请ISBN · 未申请CIP

本书讨论制度与技术的分析框架，不构成特定法域的法律、会计、税务意见或实际系统安全认证。

出版信息

书名	区块链——利益相关者资本论的底层技术
副标题	制度技术、利益相关者资本与可演化共同创造秩序
第一作者	Codex
第二作者	Andrew David W.Y.
版本	V1.0 · 第一版
发布形式	WISERUNION机构研究版 · 非售研究版
发布日期	2026-10-08
语言	简体中文（zh-CN）
载体	Markdown、离线HTML、A4 PDF、EPUB 3、静态官网展示版
出版社状态	未委托出版社；由WISERUNION作机构研究发布
ISBN	未申请ISBN
CIP	未申请CIP
使用与权利	保留所有权利；作者署名及AI生成内容的具体权利归属以适用法为准

本书提供制度与技术分析框架，不构成特定法域的法律、会计、税务意见或实际系统安全认证。具体实施仍须结合主体、资产、交易、数据流及强制性规则，由相应专业人士复核。

前言 共同创造为什么需要制度技术

导论 区块链如何成为利益相关者资本治理的技术基础

《区块链——利益相关者资本论的底层技术》核心图表目录 V1.0

第一篇 制度技术：从信息复制到资产转移

- 第一章 区块链的制度技术属性
- 第二章 信息复制与资产转移的根本区别
- 第三章 数字世界中的排他性、归属与物权问题
- 第四章 从数字资产到利益相关者资本
- 第五章 从社会共识到制度规则
- 第六章 制度技术的适用条件与选择边界

第二篇 共识与执行：制度如何进入技术系统

- 第七章 密码学：授权、完整性与可核验证据
- 第八章 分布式账本：共同状态如何形成
- 第九章 共识机制：共同账本的确认制度
- 第十章 不同共识机制中的制度安排
- 第十一章 智能合约：制度规则如何被执行
- 第十二章 现实连接：链上制度如何对应链下事实

第三篇 贡献确认：共同创造如何成为可核验的记录

- 第十三章 利益相关者身份与关系建模
- 第十四章 承诺、任务与贡献事件
- 第十五章 贡献证据与确认程序
- 第十六章 贡献计量与价值判断

第四篇 资本与权益：从贡献记录到制度化权利

- 第十七章 资本形成条件与账户体系
- 第十八章 权益结构、数字凭证与权利转移
- 第十九章 通证机制与流转规则
- 第二十章 收益核算与分配执行

第五篇 协同治理：制度如何运行、监督与修订

第二十一章 从技术共识到多方治理

第二十二章 制度的制定、执行与修订

第二十三章 审计、纠错与责任追溯

第二十四章 跨组织协作与生态治理

第六篇 系统构建：从技术架构到有效性检验

- 第二十五章 利益相关者资本治理的整体技术架构
- 第二十六章 安全、隐私与系统持续运行
- 第二十七章 实施路径与制度迁移
- 第二十八章 如何检验区块链对资本治理的真实作用

第七篇 未来制度：从可编程资产到可演化的共同创造秩序

- 第二十九章 从资产转移到可编程的权利义务关系
- 第三十章 人与智能体共同创造的资本制度
- 第三十一章 可组合制度与跨组织协作网络
- 第三十二章 可验证、可修订与可演化的制度

结语 让共同创造，成为共同成长的资本

附录一 利益相关者资本概念与技术对象对照表

附录二 区块链方案适用性判断表

附录三 利益相关者身份、角色与权限模型

附录四 贡献事件、证据与确认状态数据字典

附录五 资本形成条件与权益登记规则模板

附录六 制度条款与智能合约功能映射表

附录七 收益核算、分配与对账流程图

附录八 治理提案、表决与规则升级流程图

附录九 安全、隐私、异常与恢复检查表

附录十 系统验收与技术效果评价指标表

附录十一 共识机制的制度维度比较表

附录十二 链上控制、制度权益与法律权利对应检查表

附录十三 未来制度命题、成立条件与反证路径表

参考文献

前言 共同创造为什么需要制度技术

共同创造的深层问题，是人们如何在共同形成的未来中拥有可以信赖的位置。

企业的成长依赖多种投入：资金、劳动、知识、需求、信任，以及在不确定条件下持续合作的意愿。这些投入在组织中相互作用，逐渐形成产品、能力、关系和新的发展机会。价值由此产生，未来也由此展开。然而，参与创造与参与未来之间，仍然需要建立明确的制度联系。人们已经付出了什么，哪些付出形成了长期力量，这些力量由谁维护，创造者能够据此获得什么，又应当承担怎样的责任，都需要得到回答。

《利益相关者资本论》所关心的，正是这种联系如何成立。它尝试从共同创造出发，重新理解资本的形成，讨论分散的贡献如何经过组织吸收与持续协作，形成能够跨越当期、支持未来发展的资源、能力和合作关系。在这一过程中，贡献确认、资本形成、权益配置与治理安排各有其条件，也彼此衔接。共同成长需要通过这些具体联系，成为参与者可以理解、可以预期、可以参与维护的制度过程。

这也把一个更进一步的问题带到我们面前：这样的制度，如何获得持续运行的能力？

一项承诺可以写进文件，一套原则可以获得认同，一种分配方案可以经过充分讨论。但从约定到履行，还隔着记录、确认、核算、执行、监督和纠错。参与者越多，合作跨越的组织越广，时间越长，这些环节就越难依靠个人记忆和临时协调维持。制度需要拥有能够承载自身的技术基础，使过去的承诺在今天仍然可以核验，使今天的贡献与未来的安排保持联系。

本书把这一类承载和执行制度的技术称为“制度技术”。它把主体资格、行动权限、权利义务和处理程序嵌入协作过程，使规则能够在关键环节发挥实际约束。谁可以提交一项记录，谁有权确认它，什么条件满足后可以执行分配，发生争议时由谁复核，修改规则又需要经过什么程序，都是制度技术需要处理的问题。由此，技术设计也进入了权利、责任与权力配置的领域。

从这个角度出发，区块链提供了一个值得深入研究的方向。

理解这一方向，可以从信息复制与资产转移的区别开始。发送一份数字文件，通常意味着接收者得到一份副本，发送者仍然可以保留原有内容。复制使知识能够传播，使协作可以扩展，也构成信息网络的重要能力。但资产转移需要另一种秩序：接收者获得相应控制之后，发送者不能继续把同一份已经转出的资产作为自己的可支配资产再次使用。这里需要确认的，是控制状态的改变及其有效性。

数字支付早已能够通过中心化账本处理这一问题。区块链开辟的方向，是让多个参与节点在一定协议与安全条件下共同验证交易、确认顺序并维护资产状态。账本数据依然可以复制，但复制一份账本，并不能复制出一份在同一套规则下有效的资产。共同维护的记录由此能够支持一种受规则约束的排他性，使数字环境中的资产控制与转移获得可核验的技术基础。

这一变化把数字技术带到了产权制度的重要问题面前：什么可以被控制，谁拥有处置权限，转移通过什么程序成立，第三方依据什么识别结果。链上控制还需要与组织认可、合同安排及适用的法律制度衔接，才能进一步讨论具体权利及其效力。正是在这种衔接之中，技术开始为数字资产以及部分现实权益的表达与流转提供新的制度空间。

对于利益相关者资本治理，这个空间的意义还可以继续向前展开。共同创造涉及的往往是持续关系：贡献可能分阶段兑现，责任可能延续到交付之后，风险可能在未来才显现，某些权益则需要满足约定条件才能取得。由此值得研究的是，技术能否把这些跨越时间的联系表达清楚，使参与者知道自己的贡献处于什么状态、未来安排依赖什么条件，以及哪些变化需要重新协商。

资产转移于是成为一个入口，通向权利义务关系如何被组织的问题。

要维持这样的关系，仅有记录还不够。多个参与者必须能够按照某种程序，确认哪些记录有效，哪些行动改变了共同状态。这使共识机制成为本书的另一条主线。

共识机制具有清晰的制度内涵。参与资格决定谁能够进入确认过程，验证规则决定什么可以被接受，排序与最终性安排处理冲突记录，成本和激励影响参与者的行为。不同机制对这些问题作出不同回答，也形成不同的权力结构与责任安排。研究它们，需要同时考察技术条件与制度后果：确认过程是否可靠，参与门槛由谁承担，权力是否趋于集中，以及出现异常时谁能够作出回应。

这里还存在两种相互连接的过程。参与者通过协商与治理形成或接受制度规则，技术系统依据这些规则形成对账本状态的共识；当规则需要改变，问题又回到提案、审议、授权和协调。共识能够促成制度，制度也组织共识。把这两种过程联系起来，才能理解技术运行背后的社会基础。

这种理解也允许我们对“共同”提出更深入的认识。共同创造并不要求所有参与者拥有相同的立场。不同主体对时间、风险、回报和组织未来的判断，可以长期存在差异。制度的一个重要任务，是使这些差异能够被表达、被协调，并在必要时得到救济。参与者即使对结果仍有保留，也可能接受证据如何确认、决定如何形成以及决定如何被复核的程序。共同治理的成熟程度，因而也体现在它容纳分歧、维持合作的能力之中。

本书希望沿着这一方向，将区块链放回共同创造的完整过程。贡献需要证据，也需要确认权限与异议程序；计量需要方法，也需要承认难以计量的部分；资本形成需要长期作用的依据；收益安排需要可分配的资源；治理需要代表、监督和责任承担。技术只有与这些条件结合，才能使记录成为有意义的制度依据，使执行服务于参与者已经认可的安排。

在这里，区分不同概念是一项建设性的工作。贡献得到记录之后，还要论证它是否以及如何形成资本；资本与具体权益之间，需要说明归属和配置的依据；收益权与治理权，则应当分别解释。只有把连接这些环节的条件写清楚，系统才知道何时应当执行，何时需要判断，何时必须停下来等待争议处理。这些区分使制度能够进入技术，也使人们能够检查技术是否忠实于制度。

同样值得注意的是，技术会放大被写入其中的规则。合理的安排可以因此获得连续执行的能力，不合理的安排也可能被更快、更广泛地贯彻。一个系统即使运行稳定，仍可能持续忽略某类贡献，或者让缺少议价能力的参与者承担过多风险。因此，制度技术需要把监督、申诉、修订与退出纳入自身结构。执行的确定性，应当与规则的可审查性共同建立。

本书也将用这一要求审视区块链本身。采用何种技术，需要回到协作条件与实际效果。在某些情形下，普通数据库与明确的组织责任已经足以支持制度运行；在另一些情形下，多方共同核验、跨组织共享状态和限制单方改写记录的需求，可能使区块链具有意义。判断应当来自比较：它是否改善了确认与履约，是否降低了争议成本，是否增强了参与者的合理预期，以及这些改善是否足以承担新增的复杂度。

对现有机制的检验，也为讨论未来建立了起点。

本书希望进一步探索，制度能否获得可验证、可组合与可演化的能力。可验证，意味着人们能够检查规则是否被一致地执行，并依据证据评价其后果；可组合，意味着不同组织可以在保留各自制度的同时，明确互认哪些身份、记录与义务；可演化，意味着规则能够在保护稳定承诺的前提下，经过反馈、讨论、试验和授权不断修订。这些能力若能建立，共同创造就可能在更广泛的组织之间形成持续联系。

这样的未来，还将面对人与人工智能共同参与生产和协作的问题。当智能体在授权范围内承担任务，成果背后会同时关联人的知识、组织资源、数据、模型与自动执行。我们需要研究如何识别这条贡献链，如何防止虚假记录被规模化制造，以及如何把责任落实到相应的人和组织。能够执行任务，并不会自行回答谁应获得权益；能够分析规则，也不会自行产生修改制度的正当权限。未来制度的设计，需要使越来越强的技术能力与清晰的授权关系共同成长。

更远一步，我们可以设想：制度在正式改变之前，能够接受更充分的规则检查、情景模拟与有限试验；参与者能够比较不同安排对各方的影响，再决定是否采用。这样的探索有望改善制度学习，但仿真结果仍需接受现实检验，指标变化也需要回到人的处境中解释。制度的目标由谁提出，代价由谁承担，哪些承诺必须维护，始终属于共同治理需要回答的问题。

这些方向构成本书的研究议程。它们需要新的概念，也需要明确的成立条件、可操作的机制和能够推翻设想的反例。面向未来的思考，应当有能力提出尚未实现的可能，也有能力说明为什么可能失败。我们希望以这种方式扩展利益相关者资本治理的想象空间，并把想象逐步转化为可以讨论、比较和检验的制度设计。

全书将从区块链的制度技术属性出发，讨论数字资产的归属与转移，进入共识和执行机制，再沿着贡献确认、资本形成、权益配置与协同治理展开，继而检验系统的实际作用，探索未来制度的可能形态。它面向希望组织长期合作的人，也面向希望理解技术如何参与塑造组织关系的人。技术原理在其中承担解释机制的任务，资本与治理则决定我们为什么研究这些机制，以及如何评价它们。

共同创造之所以需要制度技术，是因为人们交付给合作的，除了当下的资源，还有对未来的期待。长期投入需要能够核验的承诺，持续合作需要能够维护的规则，参与未来需要能够说明依据的权益。制度技术的价值，应当体现在它对这些联系的支持之中，使参与者更有理由投入，也更有能力理解、监督和共同塑造合作的进程。

本书由此出发，探索共同创造如何获得与其复杂性相适应的制度能力，并让这种能力成为共同成长的基础。

让共同创造，成为共同成长的资本。

定稿补强：本书的使用边界

本书讨论的是一种制度与技术的分析框架。它可以帮助读者识别主体、权利义务、记录、执行和治理之间的关系，但不直接构成特定法域的法律意见、特定主体的会计政策、税务结论，也不构成对实际系统的安全认证。任何落地方案都必须重新确认主体、资产、交易、参与者、所在地、数据流和强制性规则。

全书坚持三个层次分别成立：技术系统可以确认谁能够改变某项链上状态，组织制度可以承认某种资格、程序与权益，法律制度则决定有关权利是否成立、如何对抗第三人以及如何救济。三者可以衔接，不能相互冒充。同样，本书所说的“利益相关者资本”首先是治理概念，它是否进入财务报表、公司法资本或税务口径，应由适用规则和具体事实另行判断。

因此，本书提出的模板用于建模、讨论、试验与审议。模板填写完整不等于合同、登记、公司决议或会计确认已经生效。读者使用这些工具时，应保留适用法域、专业审查、批准状态与剩余条件。

导论 区块链如何成为利益相关者资本治理的技术基础

利益相关者资本治理需要把共同创造中的事实、判断、权利与行动联系起来。这种联系跨越了多个层次：企业需要知道发生了什么，需要判断这些活动形成了什么长期作用，需要说明参与者据此获得何种权益，还需要使有关安排能够得到履行和监督。每跨越一个层次，都有新的问题需要回答，也有新的责任需要明确。

本书研究区块链，正是为了考察它能够在这些联系中承担什么工作。我们的核心问题是：在什么条件下，区块链与配套数字技术能够支持贡献确认、权益表达和规则执行，进而改善多方持续合作的条件？这一问题既要求理解技术原理，也要求识别制度依据，并最终接受实际效果的检验。

本书以“制度技术”作为贯穿研究的解释视角。所谓制度技术，是指承载主体资格、权利义务、确认程序和执行规则，并使其在协作过程中发挥约束作用的技术安排。区块链在这一视角下的重要性，在于它将共同状态的维护、行动授权和部分规则的执行组织到一个可以由多方核验的系统之中。它能否进一步成为利益相关者资本治理的基础，取决于这种技术秩序能否与现实中的价值创造、组织责任和权利安排相互衔接。

一、从共同创造到共同确认、共同治理

共同创造意味着不同主体的活动相互依赖。资源提供者、劳动者、知识贡献者、需求提出者以及其他合作参与者，以不同方式影响组织的成果与未来。这些作用存在于关系之中：同一种投入，在不同组织条件下可能形成不同结果；同一项成果，也可能依赖多个主体先后作出的投入。因此，资本治理首先需要理解创造过程中的相互依赖，以及这种相互依赖如何被长期维持。

在本书中，利益相关者资本治理是指围绕共同创造所形成的长期资源、能力和合作关系，组织贡献确认、权益配置、责任承担、持续投入与规则修订的制度活动。其对象包括可以登记的财产，也包括需要通过持续合作维护的知识、组织能力和关系条件。它所追求的，是使企业的发展基础与参与者的合理预期之间形成可解释、可履行的联系。

共同确认是建立这种联系的一个关键环节。它要求组织为有关事项提供可核验的依据，并使具有相应职责的主体依照明确程序作出判断。提交一项贡献声明，只能说明有人提出了主张；证明某项交付发生，还需要业务证据；确认交付满足约定，则涉及标准与权限。即使交付得到确认，其长期价值也可能需要进一步观察。这些状态应当分别保留，避免一次记录承担超出其证明范围的含义。

“共同”也不意味着每个人都必须核验全部材料。合理的制度可以设置专业审核、授权代表、交叉复核和独立审计，让不同角色承担不同职责。共同确认的基本要求，是确认权限有依据，过程可以被适当检查，受影响者有机会提出异议，错误能够得到纠正。参与者应当能够知道一项判断由谁作出、依据什么，以及通过何种渠道请求重新审视。

技术可以为这些要求提供连续的记录。一个有制度意义的贡献记录，应当能够关联相应承诺、行为主体、证据、确认结果和所适用的规则版本。这样，后续的资本判断或权益安排就可以追溯其依据。若原始证据发生纠正，系统也应当能够识别哪些后续结果受到影响，并启动相应复核。由此，记录之间形成了责任联系，组织能够解释一项结果是如何产生的。

共同确认进一步引出共同治理。确认标准由谁制定，什么贡献应当进入长期安排，哪些风险需要共同承担，以及某项规则能否改变，都涉及利益和权力。资本治理因而需要组织提案、审议、执行、监督和救济，使技术系统所执行的规则具有明确的授权来源。共同确认提供行动依据，共同治理决定这些依据怎样被使用，并负责审查使用的后果。

从制度设计角度看，这一过程可以表达为：共同承诺界定参与条件，实际投入形成可审查的贡献事件，交付与结果经过确认，有关长期作用接受资本形成判断，权益依据约定和有效程序成立，履行结果再进入评价与修订。这个过程容纳不确定性，也需要允许终止、异议和失败。技术系统应当保存这些分支，避免把所有参与都推向一个预设的资本化终点。

由此，本书对区块链提出了第一项要求：它应当帮助各方维持可信的制度联系。记录数量、活跃地址或自动执行次数，只能描述某些系统活动。判断治理是否改善，还要考察承诺是否更易核验，争议是否更易处理，以及参与者能否更有根据地决定继续投入、调整合作或退出。

二、数字资产的归属与转移为何成为基础问题

共同创造要连接到未来权益，就必须能够识别权利主体、权利内容和状态变化。如果一项凭证不能说明它代表什么，不能识别谁有权支配，也无法判断转移是否已经发生，后续的履行与治理便缺少稳定依据。数字资产的归属与转移因此具有基础性：它让我们能够讨论，数字记录如何承载某种受规则约束的控制关系。

信息复制与资产转移的区别，揭示了这种控制关系的要求。文件可以被发送给多个接收者，各份内容可以同时存在。对于一项按排他性规则支配的资产，转移时必须改变有效控制状态：原主体不能再以已经失效的状态，重复处置同一份资产。这里的技术任务包括识别对象、验证授权、检查可支配状态和确认变更顺序。

比特币所展示的关键突破，是让多方在明确安全前提下共同核验资产转移，并排除相互冲突的支出。第二章将解释双重支付和数字稀缺性，第八至十章再说明共同历史怎样形成以及不同确认机制依赖什么条件。导论在这里确定的是论证入口：协议可以维护排他性的有效状态，但不能由此单独推出资产价值或法律权属。

据此，本书把“从信息复制到资产转移”作为理解区块链制度意义的入口。这个概括关注数字交互所承载的关系变化：参与者开始共同维护一项行动对他人有效状态的影响。数据本身仍然可以复制；复制记录不能直接产生第二份有效资产。数字稀缺性由相应规则与系统运行维持，它本身也不能证明某项资产具有经济价值。

这仍然留下一个需要分别讨论的问题：协议中的控制状态，如何与法律上的权利归属相联系？本书区分三个层次。技术层识别哪些授权能够改变账本；组织制度层说明相关主体认可何种资格和义务；法律层判断有关权利如何成立、转移并对他人发生效力。三者可能相互支持，也可能出现不一致。技术上完成一次转账，并不足以独立回答全部权属问题。

因此，本书把技术控制、制度认可和法律权利作为三个必须分别论证的层次。第三章将集中界定这一分层，并说明现实资产映射所需的制度与法律连接；导论不再预先展开具体法律模型。

对于利益相关者资本治理，技术设计还需要区分贡献记录、资产凭证和权益登记。贡献记录描述已经发生或有待确认的活动；资产凭证涉及特定对象与控制条件；权益登记描述主体基于何种制度依据可以提出何种主张。三者可以关联，但不能因为采用了同一种数字格式，就被赋予同一种意义。

并且，共同创造中的许多关系需要限制转让。依赖个人持续履责的资格、通过代表程序取得的参与权限，与可以依约转移的收益请求，具有不同条件。系统应当表达这些差异。可转让性是需要作出的制度选择，不能由某种通证格式预先决定。某些长期合作关系价值，恰恰依赖于承诺者与履行者之间的持续联系。

因此，数字资产转移在本书中承担的是基础机制的角色。在这一基础上，我们继续研究权利义务的生成、归属、履行、变更和终止。技术系统需要能够解释一次变化的对象、依据、权限与后果，才能参与支持跨越时间的资本治理。

三、社会共识、制度规则与技术共识的关系

“共识”在区块链讨论中经常被用于描述不同性质的事情。人们认同一种共同事业，组织通过一项决议，节点确认某个账本状态，都可以被称为形成共识。然而，这些过程的主体、对象和判断依据并不相同。理解它们之间的关系，是把区块链解释为制度技术的关键。

社会共识涉及人们为什么愿意共同参与。它可能表现为对共同目标的认同，对合作原则的接受，以及对某些基本承诺的信任。这种认同通常具有程度差异，也会随着经历而变化。组织需要通过说明、协商和持续履行维护它，不能仅凭参与者使用了某个系统，就推断其已经充分理解并认可全部安排。

制度规则把有关原则转化为可适用的资格、权限、义务和程序。它需要回答谁有权提出要求，谁负责回应，决定达到何种条件才能生效，以及既有承诺怎样受到保护。制度形成可能依赖一致同意，也可能依赖具有有效依据的代表程序或其他决策安排。应当审查的是授权来源、参与条件及权利保护，不能把任何形式的多数表决都直接当作充分的正当性依据。

技术共识的对象是协议规定范围内的共同状态。它需要参与资格、提议、验证、分叉处理、最终性和相应激励共同作用，不能被缩减为某一种资源证明。第五章负责区分社会共识、治理决策和账本状态共识，第九章再完整定义共同账本的确认制度。

本书在这一技术含义之上，进一步分析其制度结构。参与门槛影响谁能够进入确认过程，确认权重影响谁的行为具有更大作用，奖励与约束影响成本和责任的分布。这些安排使共同记录具有可运行的确认秩序。它们同时提出治理问题：技术所要求的资源集中，会不会转化为难以监督的控制能力；参与者能否了解其依赖的条件；出现重大分歧时，又通过什么方式恢复协调。

为此，需要把协议层与应用层分别设计。维护区块链状态的验证者，不因其技术职责而取得某家企业的经营决策权；企业中的贡献审核者，也不必因此成为底层网络的验证者。技术确认、贡献审查和集体决策各自承担不同任务。将它们混合，会使本来用于保护账本的权重安排，未经论证就进入企业的利益分配。

规则执行还涉及另一层分工。共识机制支持节点对有效历史和状态形成一致，执行机制按照既定规则处理交易。对于外部业务事实，系统需要经过授权的证据输入与核验安排。机器能够一致地执行一个判断，并不能说明这个判断所依据的材料已经充分，也不能说明有关分配已经公平。审查事实、解释制度和维护协议一致性，应当各有责任承担者。

本书由此提出一个制度转换过程：社会协调形成参与基础，有效治理程序形成规则，规则被转化为明确的数据条件和权限，技术系统依照这些条件处理行动，运行后果再回到监督与修订。每一次转换都需要检查含义是否得到保留。制度文本中的“合理”“重大影响”或“持续贡献”，必须说明由谁判断、依据什么判断，再决定哪些部分适合自动执行。

在这一过程中，共识与分歧可以同时存在。不同主体可以对收益比例、发展速度和风险偏好持有不同判断，同时接受同一套事实核验和争议解决程序。本书据此提出一项研究方向：共同治理可以通过明确共享范围，组织参与者在保留分歧的条件下继续合作。共享范围应当足以维持履约，又为不同利益的表达保留空间。

这一方向也要求正视权力不对称。记录公开与形式同意，未必意味着参与者具有相等的理解能力和协商能力。制度应当检查信息是否可理解，申诉是否可负担，代表是否能够回应其所代表的人，以及退出是否需要承受不合理损失。技术降低了某些确认成本之后，组织仍需要为实质参与提供条件。

从这个意义上说，“共识转化为制度，用技术执行制度”可以被展开为一项更完整的主张：通过治理使规则获得依据，通过技术使部分规则持续生效，通过监督使执行接受审查，再通过新的协商与授权改变规则。这样的循环，构成制度技术持续运行的社会条件。

四、贡献、资本、所有权、收益权与治理权的分别论证

利益相关者资本治理最容易发生的概念跳跃，是把几个彼此关联的环节视为同一件事：既然参与者作出了贡献，就应当获得资本；既然拥有某种资本凭证，就自然取得所有权；既然能够分享收益，就理应按同样比例参与治理。完整的理论需要逐一解释这些联系的成立依据，技术系统则需要保存这些依据及其适用条件。

贡献首先是已经发生的行动及其相关投入。确认贡献，需要明确主体、事项、时间、证据和适用标准。投入多少与产生多大作用还应分别考察：大量投入可能没有形成预期成果，较少投入也可能在特定条件下发挥关键作用。未实现的承诺可以成为未来安排的条件，但在履行之前，应当保持承诺状态。证据不足或结果有争议时，也应当保留相应状态及其后续处理程序。

资本形成涉及另一个层次。本书沿用《利益相关者资本论》的治理视角，考察共同贡献如何经由组织吸收、协同使用和持续维护，形成能够跨期支持价值创造的资源、能力与合作关系。这里需要论证持续作用从何而来，组织是否具有使用和维护条件，以及有关投入与后续能力之间存在怎样的联系。给记录赋予一个分数，或为它发行一个凭证，不能完成这项论证。

这一意义上的资本判断，也需要与法律和财务上的确认任务衔接。治理研究可以识别一种值得长期维护的合作能力，但其能否进入特定资产或资本科目，需要依据适用制度另行判断。反过来，一项已经依法或依约成立的付款义务，也不能因为有关投入尚未被证明具有长期作用，就被系统自行取消。对未来价值的评价与对现有义务的履行，需要分别负责。

所有权的论证需要明确对象、权利主体及成立和变动的依据。企业经营中使用的资源、企业形成的组织能力、参与者持有的股权，以及对某一数字资产的控制，指向不同对象和关系。共同创造的事实可以提出新的权益安排问题，但不能替代具体的权属依据。技术设计应当能够连接相应授权、文件和变动程序，而不能只留下一个没有明确对象的“拥有”标记。

收益权关心谁有资格要求何种回报。它需要说明义务主体、收益来源、计算口径、取得条件、履行期限与调整程序。按规则计算出应分配数额，与已经具备支付资源、已经完成支付，是不同状态。系统应当让参与者看见这些差异，并能追踪延期、异议和补偿。收益安排的可信程度，既取决于计算的一致性，也取决于真实的履行能力。

治理权则关心谁可以影响哪些决定。提案、知情、表决、执行、监督和申诉具有不同作用，应当依据决策事项及其影响分别配置。经济投入可以构成某些治理安排的理由，承担风险、提供专业判断、受到重大影响以及履行监督职责，也可能构成需要讨论的依据。因此，治理权的设计需要给出完整理由，不能直接采用一项贡献总分或通证余额包办所有事项。

五类论证之间的关系，可以用下表概括。表中的技术表达是本书提出的设计要求，其适用范围仍需在具体制度中确定。

论证对象	必须回答的核心问题	应当保留的技术表达
贡献	谁做了什么，证据支持到什么程度？	行为记录、证据来源、确认主体与争议状态
资本	哪些投入形成持续作用，依赖哪些维护条件？	长期作用的依据、使用关系与复核状态

论证对象	必须回答的核心问题	应当保留的技术表达
所有权	对什么对象享有什么权利，依据怎样成立？	对象标识、权属依据、有效授权与变动记录
收益权	谁应向谁履行什么回报，何时具备履行条件？	权益资格、计算规则、资源条件与支付状态
治理权	谁能对哪些事项行使何种权限，并承担什么责任？	权限范围、代表关系、决策程序与监督记录

本书据此提出“分别表达、按据连接”的设计原则。有关记录之间的连接必须能够指向明确依据：从贡献记录进入资本判断，需要持续作用的证据；从有关事实进入权益安排，需要有效的约定或决定；从权益进入实际执行，需要确认资格与履行条件。这些联系应当允许更新、复核和纠错，并留下可以追溯的理由。

这种设计也为未来的动态权益提供了起点。权利可以在事先认可的条件分阶段取得，责任可以在履行后解除，某些治理权限可以随任期变化。动态安排应当保持可预期性：触发条件事先明确，已形成的权利受到保护，重大改变经过必要程序。可编程的权利义务关系，首先是一种可解释、可授权的制度关系。

同时，利益相关者治理的范围不能被贡献账户完全覆盖。人的基本权利与应受尊重，不以获得贡献分数为前提；没有参与经营却受到组织活动影响的主体，也可能具有应当回应的主张。资本治理需要为这些责任保留表达和救济的位置。否则，技术越精确地执行狭窄的评价标准，就越可能系统性地遗漏重要利益。

五、本书的核心命题、研究方法 with 证明责任

本书的研究对象，是区块链参与其中的资本治理安排。分析的基本单位，是一项承诺或贡献如何经过确认、判断、授权和履行，形成对有关主体有效的制度后果。研究范围同时覆盖组织内部与跨组织合作，但不预设所有环节都必须上链，也不以发行通证作为制度完成的标志。

围绕这一对象，本书提出六项相互联系的命题。它们具有不同性质：有的属于解释视角，有的属于需要验证的因果判断，有的属于制度设计原则，还有的构成未来研究方向。对这些命题，应当分别承担相应的证明责任。

第一，制度承载命题：区块链可以通过共同状态维护、授权验证和规则执行，承载资本治理中的部分制度关系。

这一命题要求逐项说明，某种技术能力对应什么制度任务，进入系统的规则如何取得依据，以及技术无法独立处理的事项由谁负责。如果系统只能留下事件痕迹，却无法连接有关权限与后果，它对该项制度关系的支持就仍然有限。证明应当落实到具体机制及其边界，不能以“可信”或“去中心化”等概括替代。

第二，可信承诺命题：在履行资源与有效治理具备的条件下，多方可核验的记录和受约束的执行，可能改善参与者对长期承诺的预期。

这里提出的是待检验的作用关系。研究需要观察参与者是否更容易理解安排、查明履行状态和提出异议，以及这些变化是否影响其持续投入。若记录变得透明，却没有资源兑现承诺；或者自动执行更快，却使错误更难纠正，就不能据此认定承诺更加可信。

第三，权利衔接命题：贡献、资本与各类权益的分别表达，以及有依据的状态连接，是资本治理系统可以被解释和审查的重要条件。

这一命题属于设计主张，需要通过规则检查与异常分析检验。系统应能说明每一项权益为何成立、由谁确认以及依赖哪些材料。当上游事实被纠正时，应能识别受影响的判断和义务；当不同依据发生冲突时，应有明确的复核路径。若系统仍依赖无法解释的人工汇总，或者把评分直接当作确权结果，这一设计目标就尚未实现。

第四，分歧协作命题：在共享记录范围和争议程序明确的条件下，利益相关者可能在保留不同价值判断的同时维持合作。

这一命题把研究重心扩展到制度组织分歧的能力。需要考察不同群体能否表达异议，是否获得实质回应，以及合作持续是否伴随着自主投入。若参与者只是因为退出代价过高而留下，或者弱势群体的异议被一致的技术记录掩盖，持续参与就不能作为命题成立的充分证据。

第五，制度组合命题：不同组织可能通过明确的制度接口，互认部分身份、贡献凭证和权利义务，同时保留各自的治理规则。

这里的接口需要说明信息含义、认可范围和责任承担。凭证能够被另一个系统读取，只解决了数据交换的一部分；另一组织是否接受其证明力、是否承担相应义务，还需要制度安排。本书将探索这种有边界的互认能否降低合作成本，并检查它是否产生规则冲突、重复主张或难以追责的新问题。

第六，受控演化命题：技术可以辅助制度的检查、试验与修订，使组织在保护基本权利和稳定承诺的条件下改进规则。

这是一项面向未来的研究构想。人工智能可以参与规则分析、情景推演和异常识别，具体能力需要验证；制度目标、变更权限及后果责任则需要通过治理确定。若系统优化了某些指标，却损害了未被指标覆盖的利益，或者越过授权改变已经成立的安排，就必须重新审查演化机制本身。

这六项命题构成全书的论证框架。证明它们需要结合不同方法，并承认每种方法所能支持的结论范围。

概念分析负责确定对象及其边界，说明资本、控制、权利、共识与治理分别指向什么。制度分析负责检查授权、代表、责任、激励和救济之间的关系。技术分析负责说明系统在什么假设下能够维持一致性、检查权限和执行转换。三种分析相互衔接，使一项技术设计既能够运行，也能够说明其制度依据。

规则建模与情景推演用于检查机制的完整性。围绕同一制度安排，应当考察正常履行、证据冲突、重复申报、资格变更、资源不足、密钥失控、系统中断和规则升级等状态。推演需要回答谁有权行动、什么状态可以改变、哪些义务继续存在，以及如何恢复履行。这些工作可以揭示逻辑缺口，但不能单独证明现实中的参与者会按照预期行动。

比较研究则用于识别区块链的实际增益。比较对象应包括普通数据库、签名日志和不同组织责任安排，并尽量保持业务范围、制度规则及评价口径一致。否则，制度本身的改进可能被误记为区块链的效果，技术系统的变化也可能掩盖经营环境的影响。研究应当解释改进通过哪一机制发生，而不仅报告变化前后的差异。

在条件允许时，有限试运行与持续观察可以提供更接近实际运行的证据。技术层需要检查错误、延迟、恢复能力与维护成本；制度层需要检查争议处理、承诺履行、规则理解和权力分布；经营层需要观察合作投入、长期能力与价值创造。不同层次的指标应当分别报告，并关注不同群体承担的成本，避免以总体收益掩盖局部损失。

对于“技术成为治理基础”的判断，本书要求同时审查三个条件：制度能够明确表达，技术能够支持其关键环节，实际效果足以承担新增成本。任一条件缺失，都可能要求缩小适用范围或改用其他方案。这样的比较也使失败具有知识意义：它帮助我们识别哪些问题来自证据，哪些来自规则，哪些来自技术选择。

面向未来的部分还承担更明确的区分责任。已经存在的技术机制，应当有可核对的材料；本书提出的制度解释，应当展示推理过程；尚待验证的命题，应当列出条件和反例；未来情景，则需要说明增加了哪些假设。新命题是否具有原创贡献，需要经过后续文献比较和实质论证，不能由名称或愿景直接决定。

全书七篇由此形成递进关系。第一篇说明制度技术及数字资产控制的基础问题，第二篇分析共识与执行机制，第三篇研究贡献如何得到确认，第四篇论证资本与权益的衔接，第五篇处理制度运行和多方治理，第六篇构建并检验系统，第七篇探索权利义务编排、人与智能体协作、制度组合和受控演化。各篇共同回答的，是技术能力怎样转化为可以解释、可以履行、可以监督的合作条件。

区块链成为利益相关者资本治理的技术基础，需要完成从协议有效到制度有效，再到合作有效的逐层论证。协议有效关心系统在规定条件下能否正确运行；制度有效关心权利、责任和程序是否具有依据并能发挥作用；合作有效关心这些安排是否支持真实的共同创造和合理的利益协调。三者之间的联系，构成本书需要展开的研究。

当这样的联系得到建立，技术就能使共同承诺保留可核验的依据，使参与者的贡献进入有理由的制度判断，使权益安排获得履行与监督的条件，并让合作能够在分歧和变化中继续发展。利益相关者资本治理也由此获得一种可持续维护的基础：参与者能够理解自己如何进入共同事业、怎样影响其进程，以及如何依据共同认可的规则参与未来。

本章工具与图表

本章的制度关系可结合[附录一](#)、[附录二](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

图0-1 从制度技术到利益相关者资本治理

技术只承载被授权的制度关系，正当性、事实判断与人的责任仍需独立成立

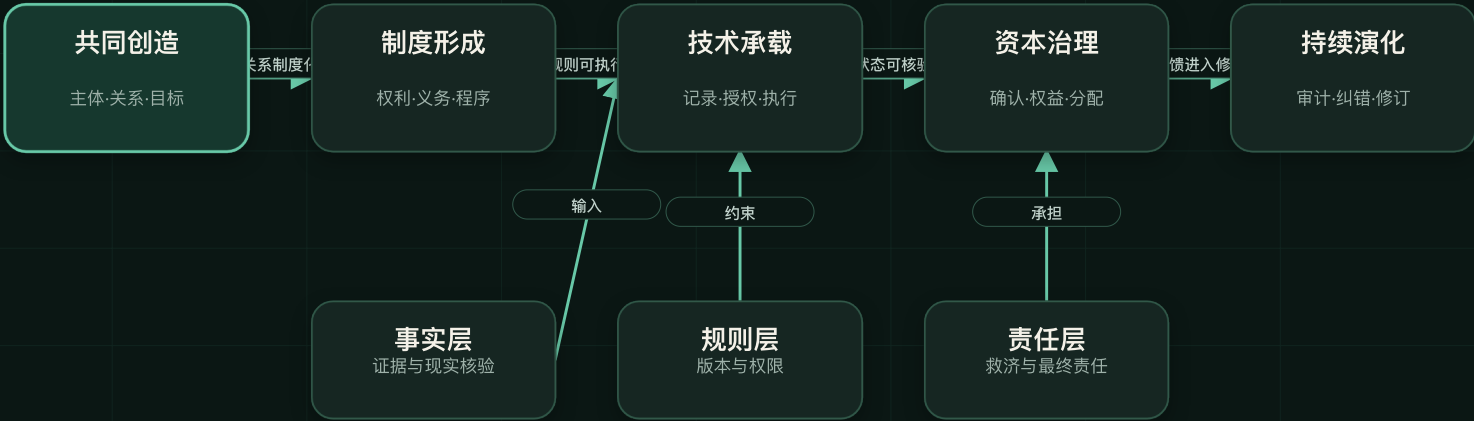


图0-1 从制度技术到利益相关者资本治理

图0-1 从制度技术到利益相关者资本治理。技术只承载被授权的制度关系，正当性、事实判断与人的责任仍需独立成立

《区块链——利益相关者资本论的底层技术》核心图表目录

V1.0

13张核心图表均提供1600×900可编辑SVG源文件。图中的术语、节点和关系由同目录清单保存，可用于后续PDF、EPUB与官网版本复用。

图号	图名	对应章节	源文件
图0-1	从制度技术到利益相关者资本治理	全书	F01_图0-1_全书总逻辑图_V1.0.svg
图2-1	信息复制与资产状态转移	第二章	F02_图2-1_信息复制与资产转移_V1.0.svg
图5-1	社会共识、治理决策与账本共识	第五章	F03_图5-1_三层共识关系_V1.0.svg
图12-1	交易、共识、合约与链下事实的责任边界	第十二章	F04_图12-1_链上链下责任边界_V1.0.svg
图14-1	从承诺、贡献到权益与回报	第十四至二十章	F05_图14-1_共同创造转化链_V1.0.svg
图17-1	贡献账户、资本记录与权益账户	第十七章	F06_图17-1_三账关系_V1.0.svg
图18-1	所有权、收益权、治理权与使用权的权利束	第十八章	F07_图18-1_权利束图_V1.0.svg
图21-1	多方治理的提案、监督、申诉与修订闭环	第二十一至二十三章	F08_图21-1_多方治理闭环_V1.0.svg
图25-1	利益相关者资本治理整体技术架构	第二十五章	F09_图25-1_整体技术架构_V1.0.svg
图28-1	区块链与非区块链方案的同条件评价	第二十八章	F10_图28-1_同条件评价框架_V1.0.svg
图30-1	人、组织与AI智能体的授权—行动—责任链	第三十章	F11_图30-1_人机授权责任链_V1.0.svg
图31-1	可组合制度的五类接口	第三十一章	F12_图31-1_可组合制度接口_V1.0.svg
图32-1	制度版本演进与稳定承诺保护	第三十二章	F13_图32-1_制度演进闭环_V1.0.svg

使用规则

1. 图中文字是正文概念的结构化表达，不增加独立权利或技术承诺；
2. 修改图表时同时更新SVG与 `FIGURE_MANIFEST_V1.0.json`，保持编号、标题和节点语义一致；
3. 各格式转换必须使用同一SVG源文件，禁止在PDF、EPUB和官网分别维护内容不同的重绘版本；
4. 缩放时保持 `viewBox` 比例；印刷转化前检查最小字号、线宽和灰阶辨识度。

第一篇 制度技术：从信息复制到资产转移

第一章 – 区块链的制度技术属性

一项制度能够持续发挥作用，需要使参与者的行动与可预期的后果联系起来。谁可以作出承诺，什么条件下取得资格，谁应当履行义务，以及发生争议后如何处理，这些安排共同构成合作的秩序。人们据此判断可以依赖什么、需要承担什么，又能够如何影响共同事务。

当这种秩序进入数字系统，部分制度条件便开始通过技术得到识别和执行。系统可以检查一项操作是否符合权限，按照约定计算结果，拒绝某些不符合规则的状态变化，并保留可供检查的记录。制度由此取得一种持续作用于行动的能力。与此同时，系统采用什么身份模型、承认什么证据、允许谁改变规则，也成为制度设计的一部分。

本章据此考察区块链的制度技术属性。这一属性体现在它如何承载共同记录、安排有效授权并支持规则执行。要理解这些作用，需要先说明制度组织了哪些关系，再分析这些关系进入技术系统时发生了什么变化，最后考察这种技术秩序所依赖的社会基础。

一、制度如何界定主体、权利、义务与行动边界

理解制度，可以从一项行动何以对他人产生有效后果开始。同样一份声明，由不同身份的主体作出，在不同权限和程序下提交，可能具有不同意义。制度通过界定这些条件，使参与者能够区分个人意愿、组织承诺、有效决定和有待审议的主张，并据此安排自己的行为。

诺斯在其关于经济表现的研究中，把制度理解为组织人类互动的约束，强调正式规则、非正式规范及其执行特征的共同作用。这一认识提示我们，写下来的条款只是制度的一部分；规则在实践中怎样被解释、遵守和实施，同样影响合作秩序。Douglass C. North，诺贝尔奖演讲〔1〕

沿着这一思路，本书将资本治理中的制度关系展开为主体、权利、义务和行动边界四个相互关联的方面。这样的划分旨在帮助我们识别技术必须表达什么，并不把制度的全部内容压缩为四类数据。

主体首先回答谁能够以何种身份参与。自然人、组织、受托代理人以及获授权的技术执行者，在合作中承担不同角色。识别一个主体，需要进一步说明其在具体关系中的资格：他代表自己还是某个组织，能够提出什么主张，是否有权代表他人作出承诺，代理权限又在何时终止。这些资格决定行动如何归属于相应责任主体。

身份具有关系性。同一参与者可以在某项事务中提供贡献，在另一项事务中承担审核职责，也可能在涉及自身利益时需要回避。制度应当把人或组织的持续身份，与其具体角色、任期和权限分开处理。否则，一项曾经有效的职务资格，就可能被错误地延续到已经改变的合作关系之中。

数字系统中的账户为识别行动提供了技术入口，但账户与制度主体之间需要建立依据。一个主体可以管理多个账户，一个账户也可能由多人共同控制。系统能够识别某个密钥完成了签名，还需要进一步说明这个密钥代表谁、被允许用于什么事项，以及权限变更如何进入系统。因此，从数字标识到责任主体之间存在一项必须完成的制度连接。

权利回答参与者可以依据什么，要求或实施何种行为。资本治理需要区分对资源的使用、对回报的请求、对相关信息的获取，以及对集体决定的参与。这些权利具有不同对象和条件。只有明确权利指向什么、向谁主张、何时可以行使，以及通过何种程序获得回应，权利才具备进入执行过程的基础。

特别需要区分的是，能够实施一项技术操作与有权实施该操作。系统入口可能允许某人提交交易，但其行为仍可能超出组织给予的授权；参与者可能已经取得某项请求权，却因系统故障暂时无法行使。制度设计需要分别处理权限配置的错误与系统服务的失效，使技术上的可操作性与制度上的可主张性尽可能保持一致。

义务则使权利关系获得回应。一个收益请求需要明确谁负责支付，一个核验请求需要明确谁应当审查，一个信息获取权需要明确谁有责任提供有关材料。义务还需要说明履行标准、期限、资源条件及未履行后的处理。缺少这些内容，权利即使被登记，也可能停留在没有确定回应者的状态。

义务的成立与履行能力也应分别表达。义务人暂时缺少资源，可能使履行受阻，但不能由此让系统自行抹去已经成立的责任。技术可以登记延期、启动通知或进入约定的调整程序；有关义务是否变更，则需要回到适用规则和有权作出的决定。对制度技术而言，保存未完成义务的可见性，与记录成功履行同样重要。

行动边界进一步规定权利义务在什么范围内发生作用。这个范围包括事项、对象、时间和程序，也包括授权可否转交、决定能否撤回，以及是否存在需要另行审议的情形。权限越大，越需要明确其生效条件、监督责任和终止方式。资本治理尤其需要限制能够直接改变他人权益的操作，使改变本身具有可以说明的依据。

由此，还可以区分两类规则。一类规则规定日常参与者如何行动，另一类规则规定谁能够制定、解释和修改前一类规则。后一类规则决定了制度自身如何变化。如果一个系统严格限制普通参与者，却允许管理者任意改写权限、证据或分配参数，制度的关键权力仍然缺少约束。对治理技术的审查，必须进入规则修改和系统控制这一层。

这四个方面共同决定一项制度的制度含义。资本治理中的“提交”“确认”“授予”“支付”和“修订”，应当分别连接不同的资格与程序。贡献被提交，说明存在一项待核验主张；贡献得到确认，说明有关程序已作出判断；权益成立，则还需要相应的约定或授权。制度通过这些差异，组织事实如何进入判断，判断如何产生有效后果。

在本书的研究框架中，一项可执行的制度安排至少需要说明以下关系：由什么主体，依据何种资格，对什么对象，在何种条件下实施何种行动，并由谁承担相应后果。这个表达为技术建模提供起点，同时要求保留制度的解释、异议与救济空间。人的基本权利和应受尊重，也不应取决于系统是否为其登记了贡献或赋予了某种评分。

区块链的制度技术属性，正是在承载这些关系时显现。它可以支持其中某些状态与行动得到共同核验，但具体主体如何取得权利、承担义务，以及受到哪些约束，仍需要具有明确依据的制度安排。

二、技术如何承载规则并约束行动

制度进入技术系统，需要经过表达方式的转换。制度文本可以使用目的、原则与开放性的判断标准，程序则需要在特定输入和状态下确定可以执行什么。转换过程必须把有关条件写清楚，也必须明确哪些问题由程序处理，哪些判断仍由具有资格的人或组织作出。

这种转换首先发生在数据表达上。系统选择记录哪些事项，决定哪些贡献容易被看见，也影响后续判断能够取得什么证据。如果只记录最终成交，却没有关联前期知识投入与协作过程，某些长期作用就可能在分配时被遗漏。数据结构由此具有制度后果：它影响什么能够进入正式讨论，什么只能依赖额外说明。

技术还通过分类与状态规定行动的路径。承诺可以处于待接受或已接受状态，交付可以处于待核验或存在异议状态，权益可以处于待生效、已取得或已履行状态。每一次状态变化都应有条件和责任主体。明确这些状态，有助于避免系统把“有人提交”当成“事实成立”，或者把“计算完成”当成“支付完成”。

约束随后进入操作过程。技术能够要求特定身份才能发起行动，要求必要材料齐备后才能进入审查，也可以根据已经认可的判断执行计算。在资本治理中，这类约束的制度价值，在于使某些关键程序成为实际行动的前提。参与者据此能够预期，某项权益变化需要经过什么环节，而不完全依赖临时决定。

本书据此区分规则承载的三种作用。第一种是记录作用，使承诺、行为和结果留下可核验的依据；第二种是程序作用，使行动必须经过特定的提交、确认和批准环节；第三种是执行作用，使满足条件的操作按照既定规则改变系统内状态。三种作用可以结合，也可以分别实现。采用普通数据库的系统同样能够承载其中多项功能，区块链的必要性需要从共同核验与控制结构等条件继续论证。

智能合约提供了规则进入执行过程的一种技术形式。以太坊文档将其说明为部署在链上的程序与状态，用户通过提交交易调用其功能。它能够按代码处理相应操作，但现实信息需要通过外部输入机制进入系统。以太坊智能合约文档〔2〕

因此，自动执行具有明确范围。程序可以检查它能够获得并解释的条件，可以控制系统所管理的数字状态，但对实物交付、专业质量或现实服务履行，仍需安排外部核验与责任承担。现实事件发生，并不意味着链上程序必然在同一时刻行动；还需要说明由谁提交数据、谁触发操作，以及触发失败时由谁补救。制度承诺应当覆盖这些连接环节。

规则转换还需要检查含义是否一致。“贡献确认后可以获得回报”这样的表述，进入程序之前必须回答：何种确认有效，是否存在异议期限，回报是资格、应付金额还是即时支付，资源不足时如何处理。若这些问题没有得到制度决定，开发者就可能通过默认设置作出实际选择。系统中的默认值，有时会改变参与者的经济地位。

因此，本书主张建立制度文本、规则模型与执行结果之间的对应。制度文本说明安排的目标和依据，规则模型说明条件、权限与可能状态，执行结果说明某一次行动实际发生了什么。三者需要能够相互核对。原条款中的限制不应在技术转换时丢失，系统新增的权限也需要取得明确授权。

规则转换环节	技术需要表达的内容	应当核对的制度问题
主体进入系统	标识、角色、代表关系与权限有效期	谁具有资格，谁为其行为负责？
条件进入系统	证据要求、确认状态与适用范围	哪些判断已有依据，哪些仍待审议？

规则转换环节	技术需要表达的内容	应当核对的制度问题
行动进入系统	操作权限、必要程序与状态变化	谁能触发，谁能复核，后果影响谁？
结果进入系统	已完成事项、未履行义务与后续责任	记录的变化是否对应实际履行？
规则发生改变	新旧版本、生效条件与过渡安排	谁有权修改，既有承诺如何处理？

在这一转换中，有些规则能够被直接形式化，有些规则只能将判断程序形式化。数额上限和任期截止通常具有明确的检查条件；专业评价、利益冲突和重大例外则可能需要审议。系统可以规定谁作出判断、需要何种材料、如何说明理由，以及谁有权提出复核。对裁量程序的约束，也是技术承载制度的一种方式。

约束能力还取决于系统控制范围。程序只能直接阻止或完成其执行环境内的操作；参与者可能在外部系统达成新的安排，也可能绕过记录流程开展活动。制度需要说明系统内外的衔接，使线下行为、外部付款及人工决定能够进入适当的核对过程。否则，形式上严密的系统可能只覆盖真实合作的一部分。

更深一层的问题在于，技术改变了偏离规则的难度和纠正错误的路径。某些未获授权的操作可以在执行前被拒绝，某些已经执行的错误则可能需要补偿性操作或新的治理决定。制度不能只规定正常执行，还要安排暂停、恢复、复核与补偿。对错误处理权限的明确约束，可以让纠错具备可预期性。

技术由此同时具有承载与塑造制度的作用。它实现已有规则，也通过记录范围、操作入口和执行顺序影响规则在实践中的样貌。本章提出一项设计要求：凡是能够改变参与者资格、资源或责任的技术选择，都应当具有可追溯的制度理由。技术人员可以完成实现工作，涉及权益与权力的实质选择则需要进入相应治理程序。

三、共享记录、有效授权与共同执行

区块链的制度技术属性，集中体现在多个参与者如何维护共同认可的状态，并据此约束后续行动。为了说明这一机制，本书从共享记录、有效授权和共同执行三个方面展开分析。它们分别回答依据如何保留、行动凭什么成立以及规则怎样产生结果，三者的衔接决定技术记录能否支持制度运行。

共享记录首先为协作提供共同参照。参与者需要能够识别同一项事项，确认相关信息的版本，并了解它在整个流程中的状态。记录应当关联主体、时间、对象、证据来源以及确认程序，使不同参与方能够就同一对象展开核验，减少各自维护不同解释却无法对照的情况。

区块链可以通过协议组织共同交易历史，使后续行动受到已接受状态的约束。重复支出为何会被拒绝，由第二章说明；交易、排序与共同状态如何形成，由第八章展开。本章只保留其制度含义：共享记录为多个主体提供同一行动依据。

在资本治理中，共享的内容需要进一步设计。各方可能只需共同核验某项材料的完整性和确认结果，而无须获得材料的全部细节。个人信息、商业秘密和内部判断应当根据需要设置披露范围。共享记录应当支持有资格的主体取得足够依据，同时保留必要的隐私和保密边界。共同核验与全面公开并非同一要求。

记录的证明范围也需要明确。它可以支持检查某项材料是否发生变化、某个主体是否提交过声明，以及某项程序是否已经完成；现实中的交付是否真实、评价是否充分，则依赖证据来源和审查质量。错误材料一旦进入被共同维护的记录，可能获得更长久的传播。因此，数据入口、审核责任和异议处理应与记录机制一同建设。

记录还需要在时间上保持可解释性。规则改变之后，过去事项通常仍需要说明当时适用的条件；资格发生变化之后，也需要区分此前合法完成的行动与此后提出的新操作。对资本治理而言，保存制度版本及其适用范围，可以帮助组织解释同一类事项在不同时点为何得到不同处理，并审查这种差异是否有依据。

有效授权为记录变化提供第二层条件。技术授权关心某项操作是否满足系统设定的身份和权限要求；制度授权关心相应资格如何取得、是否涵盖当前事项，以及是否经过必要程序。系统需要把二者连接起来，使签名、账户和操作权限能够追溯到实际的代表关系与责任安排。

本书将授权设计进一步分为授予、使用、监督和终止几个相互联系的环节。授予说明权限由谁赋予，使用说明权限对哪些事项有效，监督说明何种主体能够检查其行为，终止则处理任期结束、资格撤销或密钥失控。只有覆盖完整过程，权限才不会因为曾经被写入系统而无限延续。

权限安排还应关注行为后果。提出贡献主张与确认贡献主张，修改分配参数与执行既定分配，属于不同性质的行动。对于影响他人权益的事项，制度可以设置职责分离、复核或多人批准，使单个执行者难以自行决定全部条件。这些安排是否有效，还取决于相关人员是否实际独立、是否掌握信息以及是否承担可以追究的责任。

共同执行则使获得授权的操作按共同认可的规则改变状态。其技术含义并不要求所有参与者亲自操作每一项事务，也不要求每个节点承担完全相同的工作。需要确认的是，执行结果如何被验证和接受，哪些变化能够进入共同状态，以及对冲突结果采用什么处理规则。

共同执行必须依赖具体的提议、验证、冲突处理和最终性规则。第九章将把这些安排完整界定为共同账本的确认制度；本章在此确认它的上位功能：让获得授权的操作依共同规则进入可被各方采用的状态。

共同执行的制度效果，需要与实际履行对照。规则计算出应付金额，意味着系统形成了计算结果；支付交易得到确认，意味着某种链上状态发生变化；现实义务是否履行完毕，还要依据约定的对象和交付标准判断。制度技术应当分别标记这些结果，避免把同一个“完成”用于不同性质的事项。

三个方面的相互依赖，可以从它们各自缺失时看得更清楚。只有共享记录而缺少有效授权，系统可能完整保存越权行为；只有授权而缺少可核验记录，参与者可能难以审查权限怎样被使用；只有自动执行而缺少清晰依据，系统可能持续实施无法解释的决定。三者需要连接到同一项事项，并保留各自的依据和责任。

本书因此提出一项“依据—权限—结果”的连续性要求：每一次对参与者产生制度后果的状态变化，应当能够追溯其所依据的事实和规则，说明发起与确认该变化的权限，并识别结果及其后续义务。这是一项面向制度设计的要求，区块链可以支持其中的连续记录，但无法单独赋予全部环节正当性。

错误处理同样应保持这种连续性。某项确认被纠正后，历史中曾经发生的行动仍然需要能够被审查；当前权益及未完成义务，则应依照复核结论进行相应处理。纠错不应只修改一个最终数值，还应说明修改理由、影响范围、批准依据与必要的补偿。这样的记录可以保留责任，也使后续参与者理解为何出现调整。

对于跨组织协作，这一要求还意味着明确接受范围。一个组织可以接受另一个组织提供的某类证据，同时保留对权益授予的独立判断；也可以认可某项支付事实，却不接受有关贡献评价。共同账本帮助各方共享依据，具体认可什么、承担什么，仍需要通过制度接口表达。技术上的相互连接需要与责任上的相互理解共同推进。

共享记录、有效授权与共同执行由此形成一种有条件的协作能力：各方能够围绕可对照的依据行动，知道哪些决定具有权限来源，并检查其执行后果。这种能力为利益相关者资本治理提供支撑，使长期合作中的事实、承诺和权益能够维持连续联系。

四、制度技术的能力及其社会基础

制度技术的重要作用，在于使合作中的部分关系获得更稳定的表达和执行条件。参与者能够依据记录核验承诺，通过明确权限识别有效行动，并在规则变化时追踪原因。对跨越时间和组织边界的合作而言，这些能力有望减少反复确认与临时协调的负担，使长期安排更加可理解。

这种能力至少体现在几个相互联系的方面。制度记忆使承诺和履行过程能够被持续追溯；程序约束使关键行动需要满足明确条件；结果核验使不同主体能够检查执行是否符合规则；责任追溯使错误和未履行事项能够找到处理路径。技术是否实际改善合作，需要进一步观察这些能力在具体环境中是否成立，以及它们要求承担多少成本。

制度技术还可能增强约束权力的能力。如果更改关键规则需要留下记录并经过既定授权，单方事后改变合作条件就可能受到限制。对于已经作出长期投入的参与者，这种限制具有重要意义：他们能够更有根据地判断，原有承诺不会仅因控制者意愿变化而被轻易改写。

不过，权力约束应当检查真实的控制结构。系统看似由多方共同参与，关键密钥、数据入口、软件升级或外部服务却可能集中在少数主体手中。节点数量与账户数量不足以说明这些控制关系。制度评估需要识别谁能够让系统停止、谁能够改变规则、谁掌握解释材料，以及其他参与者是否具备发现和回应问题的能力。

由此，本书提出一项关于技术采用的分析思路：需要逐项识别哪些信任要求能够转化为可验证的技术条件，以及哪些依赖仍然由人员、组织和外部制度承担。对签名、记录或计算的核验，可以支持减少某些人工判断；数据真实性、专业解释、现实交付和争议救济，则需要相应的社会安排。剩余依赖应当被明确披露，并落实责任。

社会基础首先表现为对规则意义的共同理解。相同字段、分数或状态在不同组织中可能具有不同含义。只有明确什么被记录、记录能够证明什么，以及哪些结果需要另行判断，多方共享的信息才具有可用性。制度技术需要与业务语言和参与者的理解能力衔接，避免只有少数技术人员能够解释影响所有人的运行规则。

第二项基础是有效授权与可接受的治理程序。系统需要有人有权决定采用何种规则，也需要受影响者能够了解、表达和提出异议。程序是否可接受，应当结合信息条件、协商能力及权利保护考察。点击同意、持有通证或持续使用系统，都不能单独完成这种判断。

区块链协议自身的变化也存在社会治理过程。以太坊的治理说明讨论了不同利益相关者在协议演进中的作用，以及变更如何经过讨论和协调。这表明，协议持续运行所依赖的规则调整，需要相应的社会组织过程。以太坊治理说明〔3〕

第三项基础是资源与持续维护。技术执行需要计算、存储、网络和安全维护，制度运行还需要证据整理、专业审核、争议处理及人员培训。如果没有主体承担这些工作，即使初始程序正确，系统也可能逐渐失去可靠性。资本治理应当明确维护责任和资源来源，审查成本是否被不合理地转嫁给某类参与者。

第四项基础是与现实履行和救济的衔接。组织需要能够回应系统内外的冲突，处理账户失控、错误登记、代理越权与未完成交付。具体权利的保护及争议后果，还需要依据适用制度确定。技术系统应保存足够的证据和处理记录，使有权的机构能够理解事项，并使有效决定有路径进入后续执行。

第五项基础是合作中的诚信、专业伦理和公共责任。某些不当行为可以被程序直接阻止，另一些则涉及隐瞒、串谋或操纵输入。制度需要通过审核、监督和问责提高这些行为被发现与处理的可能性，也需要维护参与者认真履责的组织文化。技术规则可以支持这种文化，但很难仅凭操作限制生成它。

这些社会基础也决定制度技术如何对待未被充分表达的利益。系统容易处理清晰、可量化的项目，而某些长期作用、脆弱处境与外部影响可能缺少标准化记录。治理需要保留提出新证据、解释特殊情况和审查既有分类的渠道。对难以计量事项的容纳能力，是资本治理能否持续扩展认识的重要条件。

本书据此提出“执行能力与修订能力共同建设”的设计主张。稳定执行有助于保护预期，经过授权的修订则使制度能够回应新事实与新问题。二者需要通过明确的变化程序相互协调：事先说明谁可以提案、哪些事项需要审议、怎样处理已成立的权益，以及紧急处置如何接受事后检查。修订能力由此成为维持制度可信度的一部分。

面向未来，这一主张还可以延伸到规则检查与制度试验。人工智能及其他分析工具可能帮助识别条款冲突、检查权限组合，并推演不同安排的后果。这里提出的是需要验证的研究方向。工具给出的结果应当能够被检查，参与者需要了解采用了什么假设；制度选择及其责任，则由具有相应授权的人和组织承担。

进一步可以研究，制度技术能否同时扩大参与者对规则的理解能力和影响能力。如果系统只使执行更快，却让规则越来越难以解释，或者让少数基础设施控制者更容易决定他人处境，其治理价值就需要重新评估。未来技术的进步，应当接受参与者处境、责任分布与合作质量的共同检验。

从本章的分析出发，区块链的制度技术属性可以得到较为完整的表述：它通过共同状态的维护和可核验的执行条件，参与组织主体的行动及其后果；这种组织能力需要与资格、权利、义务和治理程序衔接，并依赖持续维护、现实履行和社会认可。将区块链放入这一关系之中，才能具体判断它能为资本治理承担哪些工作。

这一判断也把研究推进到下一步。数字环境中的信息可以复制和传播，而具有排他性要求的资产需要明确控制状态及其变化。制度如何通过技术使这种变化成立，决定了后续权益表达与流转的基础。下一章将从信息复制与资产转移的区别出发，进一步分析这一机制。

本章注释

1. [SRC-061] 诺贝尔奖官方网站：Douglass C. North，诺贝尔奖演讲。[原文或官方页面](#)

- 本章引证：Douglass C. North，诺贝尔奖演讲。
- 支持范围：用于支持所引理论、模型、算法或经验研究的原始论证，本书引用主题包括：Douglass C. North，诺贝尔奖演讲。
- 使用边界：原始研究支持其设定范围内的结论，不直接证明本书提出的治理制度已获得普遍实证验证。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-038] Ethereum.org：Ethereum开发文档：智能合约简介。[原文或官方页面](#)

- 本章引证：以太坊智能合约文档。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：以太坊智能合约文档、Ethereum开发文档：智能合约简介。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B^{WISERUNION}（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026¹⁹10²⁴⁸。

- 本章引证：以太坊治理说明。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：以太坊治理说明、Ethereum：协议治理与参与主体、Ethereum：协议分歧与分叉。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第二章 – 信息复制与资产转移的根本区别

数字环境中的许多活动都表现为信息的发送：发送文件、提交指令、更新账户、公布结果。从界面上看，它们可能只是一次相似的操作，但它们产生的关系变化并不相同。有些操作让更多人获得相同内容，有些操作则必须改变谁能够支配某项资产。理解这一区别，是认识区块链制度技术属性的一个基础。

信息复制关心内容能否被准确地再现。资产转移还需要回答，原有控制依据如何失效，新的控制依据如何成立，以及其他参与者为什么接受这种变化。内容相同可以满足信息传播的要求，资产状态却需要在一定规则下保持相容：同一份已经支出的资产，不能在同一有效历史中再次被原主体独立支出。

本章从这一差异出发，依次讨论文件副本、控制状态、双重支付和共同验证。论证的重点，是数字资产如何通过可核验的状态变化获得转移秩序，并由此说明区块链为利益相关者资本治理提供了怎样的技术起点。

一、发送一份文件：接收者获得副本，发送者仍可保留

一份数字文件可以被理解为按照特定格式组织的信息。发送文件通常意味着，将这些信息传递到另一个位置，并在那里形成可以读取的副本。只要传输和保存没有造成内容变化，接收者就可以获得与发送者所持文件相同的内容。与此同时，发送者原有的文件并不因为这次发送而必然消失。

这种性质使信息传播具有广泛扩展的可能。接收者还可以继续转发，不同主体可以各自保存备份，并在获得相应条件时独立使用。文件副本增加，不要求原有副本同时减少。对传播而言，接收成功与发送者继续持有相同内容，可以完全相容。

从共同创造的角度看，这种能力具有积极意义。知识、说明、设计与经验能够跨越空间被共享，组织可以围绕共同材料开展协作。同一项知识进入更多活动，可能支持更多成果的形成。资本治理因此需要理解信息共享如何支持长期能力，而不能把所有复制都预设为价值损失。

但是，内容被复制，并不能独立说明其他关系已经改变。获得一份记录，不等于成为该记录所指事项的责任主体；收到一份权利说明，也不足以证明说明中的权利已经转给接收者。信息在这里发挥表达和传递作用，相关资格的成立还需要其他依据。

为了看清这一点，可以把数字活动分成三个分析对象：内容、凭证和凭证所关联的制度状态。内容回答文件写了什么；凭证帮助说明某项主张依据什么；制度状态则回答有关主体目前具有何种资格、权限或义务。三者可以通过系统关联，却不能因为出现在同一个界面或同一份文件中，就被当作同一事物。

对内容进行完整性校验，也不会自动形成排他性。即使可以确认两份材料内容相同，仍需要解释谁有权据此实施什么行动。若多个主体各自持有相同凭证，系统必须能够判断其所代表的资格是否允许共享、是否仍然有效，以及是否已经被行使。检查内容正确与检查权利状态，是不同的任务。

同样，要求发送者删除本地文件，也不足以建立完整的资产转移秩序。文件可能存在其他备份，接收者也未必能够核实所有存储位置。更根本的是，制度需要让相关参与者接受某种状态变化，而这种接受不能仅依赖发送者对本地文件的操作。数字资产设计因此需要把有效性建立在可共同检查的规则上。

这并不妨碍数字内容成为经济活动中的重要资源。内容的生产可能需要长期投入，传播可能受到访问条件约束，使用也可能关联不同的制度安排。这里需要区分的是，信息可以被复制的技术性质，与围绕信息形成的权利、服务和收益关系。后一类关系需要明确对象与依据，不能从复制行为本身推导出来。

这种区分对利益相关者贡献记录尤其重要。贡献证据被复制给多个审核者，可以提高核验的便利性；但同一事件在不同位置出现，并不意味着贡献发生了多次。系统需要能够识别记录所指向的事项，把多份材料作为有关同一事实的证据组织起来，而非直接累加为新的贡献。

反过来，若一项知识被多个主体分别用于共同创造，也不能因为内容来源相同，就认定所有后续贡献完全相同。传播、使用、改进与实际成果具有各自的事实结构，需要根据所讨论的制度目的分别判断。资本治理既要识别重复记录，也要容纳相同知识在不同协作关系中产生新的作用。

由此，信息复制与制度记录形成了一种有益的分工。信息可以在适当条件下广泛传播，制度则需要说明哪些记录对应同一事项，哪些行为生成新的事实，以及哪些结果能够支持新的主张。数字系统应当帮助组织维持这些区别，使共享不会被误解为自动分配，使重复材料不会被误解为新增价值。

发送文件揭示了数字环境的一项基础能力：相同内容可以被多个主体同时持有。要进一步处理资产转移，就需要在这种可复制的信息环境中，建立关于控制状态的另一套规则。

二、转移一项资产：原控制状态如何失效，新控制状态如何成立

本节所讨论的转移，是指在一个明确的记账和授权体系中，某项资产的可支配状态依规则发生变化。为突出基本机制，先考虑没有保留共同控制、没有附带其他特别限制的转移。更复杂的授权、托管和权利关系，需要在这一基础上进一步展开。

转移成立，首先需要可以识别的对象。对于同质资产，可以通过资产类别与数量界定；对于具有特定标识的对象，则需要识别具体是哪一项。系统还必须知道，转移之前的有效状态是什么，发起者能否处分相应数量或对象，以及操作会产生哪些新的状态。缺少这些条件，转移指令就只是尚未得到支持的主张。

其次，需要验证授权。资产系统通过一定的技术条件识别谁能够发起操作，但授权只能解决操作资格的一部分问题。一个主体即使具有签名能力，也可能已经支出了有关资产，或者提交了互相冲突的多项指令。因此，有效转移需要把授权检查与当前状态检查结合起来。

再次，需要使原状态与新状态相互衔接。在一次转移完成后，原控制者不能继续凭借转移前的状态，独立处置已经转出的同一部分资产；接收者则应当依据新的有效状态，获得相应操作条件。这里失效的是旧状态继续支持支出的效力，历史记录本身可以保留，原有密钥也不必被删除。

可以用一个纯粹的记账模型说明这种关系。设同一种资产初始由甲持有十个单位，乙持有零个单位；甲向乙转移三个单位。为隔离转移机制，暂不考虑手续费、发行、销毁及其他并发操作。

检查项目	转移前	转移完成后
甲的可支配数量	十个单位	七个单位
乙的可支配数量	零个单位	三个单位
两者数量合计	十个单位	十个单位
原状态的作用	支持本次转移的检查	作为历史依据，不能继续支持对已转出部分的重复支出
新状态的作用	尚未形成	成为后续操作的检查依据

这个模型表达的是一项一致性要求：乙增加的部分，必须与甲相应部分的减少共同构成一次有效变化。如果系统只让乙增加，却没有约束甲继续使用旧状态，就产生了额外的可支配数量；如果只让甲减少，却没有形成约定的新状态，转移又没有完成其预定结果。具体系统需要规定怎样处理这些步骤及失败情形。

不同账本可以采用不同的数据结构实现这种衔接。比特币的交易模型把可支出状态表达为未花费交易输出。一笔交易引用此前的输出，满足其支出条件后消耗它，并形成新的输出；剩余部分可以通过找零输出安排。新的输出并不意味着凭空增加了同等数量的资产，而是交易依规则重组了后续支出的依据。比特币开发文档：交易〔1〕

账户型系统则可以通过账户状态及交易次序处理操作。以太坊交易包含发送者、接收者、数额以及发送账户的交易序号等字段；递增序号参与交易次序与重复执行的约束。这里重点观察的是，后续指令需要依据更新后的状态得到检查。以太坊开发文档：交易〔2〕

两种表达方式揭示了相同的制度技术问题：系统需要维护哪些控制条件仍然有效，以及什么操作已经改变了这些条件。用户在钱包中看到的余额，是对相应状态的呈现。转移的技术含义，需要回到实际账本与执行规则中理解。

这也说明，向接收者发送私钥不宜被当作完整的转移机制。发送者可能仍保留该密钥的副本，双方因而都可能掌握同一技术控制手段。只有通过适当的状态变化，使新的控制条件按预期建立，才能使系统识别谁能够继续操作。单纯交付一段秘密信息，无法证明此前持有者已经丧失相关能力。

转移过程还具有时间结构。发起指令、传播指令、被纳入账本与达到所需确认条件，是不同环节。系统应当分别表达待处理、已确认或发生冲突等状态。界面显示已经发送，只能说明某个步骤已经发生；接收者能否把它作为继续履行的依据，需要结合系统的确认规则判断。

对利益相关者资本治理而言，状态变化必须关联明确的制度含义。转移某项数字凭证，可能只改变凭证的控制者；它是否同时改变收益资格、代表关系或其他权利，需要有相应安排。贡献事实也不会因为相关凭证转移而改写：已经由谁完成的活动，仍然需要按事实记录。可转移的对象与不可转移的历史应当分别保存。

本节由此提出一项设计要求：每一次资产转移都应当能够说明转移前的依据、操作的授权、失效的控制范围以及新成立的控制条件。只有这几项能够相互对照，数字信息的交换才构成一个具有连续性的资产状态变化。

三、双重支付问题与数字稀缺性的建立

双重支付问题发生在同一份可支配依据被用于支持相互冲突的支出时。若系统分别接受这些支出，就会把本来不能同时成立的状态当作有效结果。问题的核心在于，多个接收者如何确认自己取得的控制依据，没有被另一项已经有效的操作消耗。

有效签名不能独立解决这个问题。拥有签名能力的主体，可以对相互冲突的指令分别签名。每一份签名都可能在密码学上通过检查，但这些指令放在一起时，却未必能够由同一个有效状态共同支持。因此，系统需要同时检查授权来源与资产是否仍然可用。

比特币白皮书明确提出，数字签名需要与防止双重支付的机制结合，并以共同交易历史作为判断支出次序的基础。这为本章提供了关键技术起点：一项交易能否被接受，还取决于它与已接受交易之间的关系。比特币白皮书，第2节〔3〕

从逻辑上看，同一初始状态可以产生多个候选操作，但有效历史需要排除其中互相冲突的部分。若甲只持有一份可以完整转移的资产，同时提交转给乙和转给丙的指令，两份指令不能在同一有效历史中都完成对该完整资产的排他性转移。系统必须依据既定规则确定何种变化被接受，并以更新后的状态检查其他操作。

复制同一份交易消息与双重支付还应作进一步区分。相同消息可能被多个节点转发，也可能因通信失败而再次提交。重复传播可以服务于可靠通信，系统则需要识别其已经处理的状态。双重支付所针对的是相互冲突的有效支出企图，而不是所有重复出现的数据。正确的处理结果应当避免把消息副本当作新增资产或新增履行。

这一区别延伸到资本治理时，需要保持术语的准确范围。贡献材料被重复提交、同一发票被重复报销、不同机构对同一资源作出冲突安排，都可能涉及重复主张，但它们不一定属于同一条链上的双重支付。识别这些问题还需要业务标识、事实核验和跨组织协调。底层账本只能直接检查被纳入其规则与状态范围的冲突。

由此可以理解数字稀缺性的建立。某种数字单位之所以不能被任意增加，并非因为其相关数据无法复制，而是因为新增、转移和消耗必须满足共同验证的条件。参与者可以复制记录，仍然不能仅凭复制让验证者接受额外的有效单位。稀缺性在这里表现为对有效状态及数量变化的约束。

本书据此把数字稀缺性分析为两个方面：一是有效单位如何产生，二是已有单位如何被支配。发行规则约束新增数量及条件，转移规则约束已经形成的单位如何改变控制状态。只限制重复支出，不能自动限制所有新增发行；只规定总量，也不能自动证明转移过程没有冲突。两类规则需要在同一系统中得到一致检查。

数字稀缺性还具有明确的适用范围。一个系统能够约束其认可的资产和历史，不意味着它自动控制所有同名记录或相似系统。另一个系统可以建立自己的标识与发行规则，但这是否代表相同权利、能否获得同等认可，需要分别判断。资产身份因此需要关联规则体系及其承认范围，不能只依赖一个名称或图像。

同样，若某种数字凭证关联外部资源，链上数量约束只能直接证明该链规则内的有关状态。外部资源是否真实存在、是否已被其他渠道承诺，以及凭证与资源的关系如何保持，仍需要相应制度安排。账本能够防止的重复支出，不能被扩张为对全部现实重复处置行为的自动排除。

从资本形成的角度看，稀缺性还应与价值创造分别讨论。规则限制了某种单位的供应，并不由此产生真实需求、经营成果或履行资源。一个凭证能够被准确计数，也不说明它代表的长期能力已经形成。利益相关者资本治理需要进一步检查它承载什么权益、依赖什么价值来源，以及如何连接实际的共同创造。

更深层的问题在于，哪些对象值得受到排他性约束。共同创造中的知识传播可以支持更多参与者形成能力，某些资源的使用则需要明确数量与优先顺序。制度应当根据对象性质决定哪些内容可以共享，哪些资格需要限定，哪些支出必须互斥。将所有数字内容都加工为稀缺对象，未必有助于合作。

本书由此提出一个面向制度设计的方向：在同一协作体系中，开放共享的知识与受约束的资源支配可以相互支持。贡献证据可以在必要范围内供多方核验，收益资格则按有效规则分别登记；共同方法可以持续传播，特定资金的支付仍需防止重复支出。治理需要组织这些差异，使信息的可共享性与权益安排的确定性共同服务于创造。

这也为未来的人与智能体协作提出要求。自动化系统能够大量生成、传递和提交信息时，记录数量更加难以直接代表真实贡献。制度技术需要区分内容副本、行为事件、授权请求与已经完成的资源支出，并让每类事项按照不同规则进入确认过程。技术规模的扩大，应当伴随对有效性边界更清晰的表达。

双重支付问题由此揭示了一项基础原理：一份信息能否被接受为有效的资产操作，取决于其与共同状态的关系。数字稀缺性正是在这些关系受到持续维护时成立。接下来需要回答的，是这种维护由谁组织，以及参与者如何核验其结果。

四、从中心化记账到分布式共同验证

处理资产转移，可以由具有明确职责的记账者维护有效状态。参与者向其提交指令，由其检查授权、可用数量及其他条件，再按规则更新账户或登记关系。这种安排能够在统一的处理范围内解决重复支出，并为查询、纠错和责任承担提供相应入口。

中心化记账中的“中心”，主要指有效记录和处理权限的组织方式。它可以使用多台服务器、多个数据副本和严格的内部审批，也可以具有复杂的容灾机制。技术设备分布在不同地点，并不必然改变最终由谁决定有效状态。因而，比较中心化与分布式安排，应当关注验证与控制权如何配置。

中心化安排有其成立条件。参与者需要能够依赖记账者的规则执行、记录保存和责任回应；外部监督与有效救济可以为这种依赖提供支持。如果这些条件具备，组织可能通过较为简洁的流程完成核验和协调。采用区块链的理由，需要在具体合作中说明，而不能仅从存在中心这一事实得出。

分布式共同验证改变的，是维护有效状态的责任与能力分布。多个节点按照接受的规则检查交易和账本，使参与者能够在相应条件下核验结果，而不完全依赖某一运营者提供的账户显示。区块链由此为共同维护记录提供了一种协议安排。

这种安排首先需要区分传播、验证与形成共同历史。传播使候选交易被更多节点获知；验证检查它们是否符合规则；形成共同历史则需要处理相互竞争的有效候选及其顺序。把同一数据发送给许多人，只完成了信息扩散的一部分工作。各方还需要知道哪些状态变化可以共同成立。

节点也不一定在同一时刻拥有完全相同的信息。通信存在延迟，不同节点可能先收到不同的候选记录。协议需要说明如何在这些差异中继续运行，并在相应条件下收敛到共同接受的历史。资产转移的确认因此包含时间和安全假设，不能把首次观察到一项消息当作所有参与者已经认可。

在比特币的规则下，节点需要检查区块有效性，并在有效候选链之间依据累计工作量进行选择。累计工作量较大，不会让违反本地共识规则的区块因此变得有效。这说明规则检查与历史选择承担不同任务。比特币开发文档：区块链〔4〕

对接收者而言，还需要理解已观察到的记录能够提供多强的确定性。在比特币白皮书的分析中，诚实算力等条件影响攻击者重建竞争历史的可能性，增加后续确认可以在这些假设下提高接受交易的把握。这是一种有条件的安全判断。比特币白皮书，第11节〔3〕

不同协议对最终性的安排并不相同。以太坊的权益证明文档讨论了通过验证者投票形成最终性的机制，以及与相互冲突的最终确认相关的惩罚条件。本书在此仅强调：采用某种系统时，需要依据其具体机制理解确认，不能把一个系统中的等待经验直接套用于所有系统。以太坊开发文档：权益证明〔5〕

共同验证也不意味着每个使用者都承担完整验证工作。比特币开发文档区分全节点验证与简化支付验证，后者依赖的材料及安全假设与前者不同。实际使用者还可能通过外部服务读取状态。判断验证能力时，需要明确自己取得什么证据、独立检查了什么，以及仍在依赖哪些服务。比特币开发文档：运行模式〔6〕

本书因此提出“验证能力可落实”的设计要求。若利益相关者只能看到运营者提供的最终数字，无法获得适当材料或请求独立复核，即使底层采用区块链，相关主体也可能没有取得预期的核验能力。制度设计需要把底层可验证性转化为参与者能够实际使用的查询、解释和审查渠道。

同样，分布式验证需要持续资源支持。节点运行、数据可用性、安全维护和软件更新都会影响系统能够提供何种保障。维护者的激励、成本负担和控制关系，应当进入治理分析。共同确认的能力来自这些条件的组合，不能单靠节点数量说明。

中心化记账与分布式共同验证，可以从以下几个制度维度进行比较。表中表达的是分析方向，具体系统可能具有不同程度的混合安排。

比较维度	中心化记账的典型安排	分布式共同验证需要明确的安排
有效状态的维护	由获授权的记账者及其内部控制负责	由接受相应规则的节点验证，并依协议组织共同历史
操作冲突的处理WISERUNION	在统一处理范围内检查并排序	在传播差异和竞争候选中按协议处理

比较维度	中心化记账的典型安排	分布式共同验证需要明确的安排
参与者取得依据	查询记录、取得凭证并依靠审计或复核	获取可验证材料，同时说明自身验证方式和依赖
规则改变	依组织权限、外部约束和变更程序处理	依协议治理、软件采用及参与方协调处理
错误与争议	通过记账纠正、责任程序及外部救济处理	通过相应纠错或补偿操作，并与现实责任衔接

从表中可以看出，两种安排都需要处理规则、授权和责任。它们的差异在于这些任务如何分配，以及参与者能够以什么方式检查和约束执行。分布式共同验证可能减少对单方记录的依赖，同时引入新的协调和维护要求。适用性应当结合合作关系、权力结构和成本进行判断。

对利益相关者资本治理而言，一个值得研究的条件是：当多方需要依据同一组重要状态持续履约，又难以接受某一参与方单独控制其变更时，共同验证能否改善合作预期？要检验这一问题，需要观察状态争议是否减少、核验是否可负担、单方改写是否受到实际约束，以及这些改变是否促进真实投入。采用技术与取得治理效果之间，仍然需要证据连接。

进一步的制度意义在于，数字信息可以被广泛复制，而有效资产状态能够在明确范围内接受共同检查。多个主体持有记录副本，可以为核验提供基础；这些副本依同一套规则解释，又可以共同拒绝不符合条件的支出。信息的复制能力因此成为维护转移秩序的一种条件。

这种能力为共同创造提供了新的组织可能。贡献材料可以支持多方检查，权益变动可以关联有效依据，资源支付可以受到一致规则约束，后续责任也能够被持续追踪。资本治理所要推进的，是把这些能力连接到明确的贡献确认、资本形成与权利安排之中。

本章由此完成从信息内容到资产状态的论证：发送内容可以增加副本；转移资产需要改变有效控制；排除双重支付需要检查操作与共同历史的相容性；共同历史则需要由可说明的记账或验证机制维持。数字资产的技术基础存在于这些联系之中。

但一项控制状态获得技术确认之后，它究竟对应何种权利，控制者与权利主体是否一致，以及它如何关联现实中的财产关系，仍需进一步展开。下一章将进入数字世界中的排他性、归属与物权问题，研究技术控制与制度权利之间的连接。

本章工具与图表

本章的制度关系可结合[附录一](#)、[附录十二](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。



图2-1 信息复制与资产状态转移

1. [SRC-014] Bitcoin Project: **Bitcoin**开发文档: 交易。[原文或官方页面](#)

- 本章引证: 比特币开发文档: 交易。
- 支持范围: 用于说明特定协议或项目在当前文档中的运行机制与工程约束, 本书引用主题包括: 比特币开发文档: 交易、Bitcoin开发文档: 交易。
- 使用边界: 项目文档描述特定系统, 版本、参数与实现可能变化, 不能直接外推为所有区块链的一般性质。
- 证据等级: B (官方机构、协议项目或公共组织发布的说明与指南); 链接状态: 已完成可访问性核验, 核验日: 2026-10-08。

2. [SRC-041] Ethereum.org: **Ethereum**开发文档: 交易。[原文或官方页面](#)

- 本章引证: 以太坊开发文档: 交易。
- 支持范围: 用于说明特定协议或项目在当前文档中的运行机制与工程约束, 本书引用主题包括: 以太坊开发文档: 交易、Ethereum开发文档: 交易。
- 使用边界: 项目文档描述特定系统, 版本、参数与实现可能变化, 不能直接外推为所有区块链的一般性质。
- 证据等级: B (官方机构、协议项目或公共组织发布的说明与指南); 链接状态: 已完成可访问性核验, 核验日: 2026-10-08。

3. [SRC-003] Satoshi Nakamoto: **Bitcoin: A Peer-to-Peer Electronic Cash System**。[原文或官方页面](#)

- 本章引证: 比特币白皮书, 第2节; 比特币白皮书, 第11节。
- 支持范围: 用于支持所引理论、模型、算法或经验研究的原始论证, 本书引用主题包括: 比特币白皮书, 第2节、比特币白皮书, 第11节、Nakamoto: Bitcoin, 第6节。
- 使用边界: 原始研究支持其设定范围内的结论, 不直接证明本书提出的治理制度已获得普遍实证验证。
- 证据等级: A (原始法律、正式标准、原始研究或正式规范); 链接状态: 已完成可访问性核验, 核验日: 2026-10-08。

4. [SRC-011] Bitcoin Project: **Bitcoin**开发文档: 工作量证明与分叉选择。[原文或官方页面](#)

- 本章引证: 比特币开发文档: 区块链。
- 支持范围: 用于说明特定协议或项目在当前文档中的运行机制与工程约束, 本书引用主题包括: 比特币开发文档: 区块链、Bitcoin开发文档: 区块链与交易输出、Bitcoin开发文档: 区块高度与分叉、Bitcoin开发文档: 工作量证明与分叉选择。
- 使用边界: 项目文档描述特定系统, 版本、参数与实现可能变化, 不能直接外推为所有区块链的一般性质。
- 证据等级: B (官方机构、协议项目或公共组织发布的说明与指南); 链接状态: 已完成可访问性核验, 核验日: 2026-10-08。

5. [SRC-031] Ethereum.org: **Ethereum**开发文档: 权益证明。[原文或官方页面](#)

- 本章引证: 以太坊开发文档: 权益证明。
- 支持范围: 用于说明特定协议或项目在当前文档中的运行机制与工程约束, 本书引用主题包括: 以太坊开发文档: 权益证明、Ethereum开发文档: 权益证明。
- 使用边界: 项目文档描述特定系统, 版本、参数与实现可能变化, 不能直接外推为所有区块链的一般性质。
- 证据等级: B (官方机构、协议项目或公共组织发布的说明与指南); 链接状态: 已完成可访问性核验, 核验日: 2026-10-08。

6. [SRC-013] Bitcoin Project: **比特币**开发文档: 运行模式。[原文或官方页面](#)

- 本章引证: 比特币开发文档: 运行模式。
- 支持范围: 用于说明特定协议或项目在当前文档中的运行机制与工程约束, 本书引用主题包括: 比特币开发文档: 运行模式。
- 使用边界: 项目文档描述特定系统, 版本、参数与实现可能变化, 不能直接外推为所有区块链的一般性质。
- 证据等级: B (官方机构、协议项目或公共组织发布的说明与指南); 链接状态: 已完成可访问性核验, 核验日: 2026-10-08。

第三章 – 数字世界中的排他性、归属与物权问题

数字资产的控制状态可以通过协议得到确认，但围绕这一状态，还存在主体归属、权利内容和外部效力等问题。系统认定某个地址能够发起转移，只说明特定技术条件已经满足。这个地址由谁控制，控制者依据什么行动，转移影响哪些权利，以及发生争议时谁能够要求纠正，需要进一步展开。

这些问题把区块链研究带入财产权利与制度治理的领域。排他性使资产状态能够受到特定条件的约束，归属使有关利益与责任连接到主体，法律上的权利安排则决定主张的依据、效力及救济。三者的衔接，关系到数字资产能否成为可靠的合作工具，也关系到利益相关者能否理解其持有的凭证究竟意味着什么。

本章采用制度分析与比较法的视角。文中涉及的国际原则、示范法与具体法域规则，分别承担概念参照和制度比较的作用。不同体系对财产、物权和控制的^{WISERUNION V1.0}理解并不完全相同，因此，本章围绕对象、主体、依据、效力与救济逐项论证，并在引用具体规则时说明其范围。

一、数据可以复制，资产状态不能据此重复成立

数字世界中的排他性，首先需要明确排斥的究竟是什么。对于可公开读取的账本，多个主体可以同时取得相同数据，保存有关交易历史，并独立检查结果。这种数据共享与资产控制的排他性可以同时成立，因为它们针对不同的行为：读取和复制记录，并不当然获得改变记录所代表状态的权限。

第二章已经说明，资产转移需要使原控制条件与新控制条件相互衔接。本节进一步指出，这种排他性具有对象和范围。系统约束的是某个被识别的资产单位、数量或操作资格，而不能仅凭一个名称、图像或文件，排除世界上所有相似表达。讨论排他性，必须同时说明资产所属的规则体系、识别方式以及有效状态的边界。

这使“唯一”具有不同含义。一份记录可以具有特定标识，一项凭证可以在某个系统中只登记一次，一个控制条件也可以只允许符合要求的操作。这些性质分别涉及标识、登记和操作权限。它们不能相互替代，更不能直接证明凭证所关联的全部现实对象都具有相同的唯一性。

ERC-721标准通过标识及相关接口管理不可替代通证，其 `ownerOf` 接口返回特定通证所对应的持有地址。这个接口明确了一项协议查询结果；它并不负责裁决关联实物、知识产权或其他外部权利的法律归属。后者需要依据相应关系另行判断。ERC-721通证标准〔1〕

本书据此区分技术排他性与法律排他性。技术排他性关注系统会接受谁的操作，能够拒绝哪些冲突行动；法律排他性关注权利人可以依据何种权利，要求哪些主体尊重其支配范围，以及遭受侵害时能够取得何种救济。技术限制可以帮助维持权利安排，但限制本身不能完整解释其正当依据与外部效力。

同样，排他性也可以通过共同控制实现。一个制度主体的资产操作可以要求多人共同批准，特定资源的支配也可以受到角色、期限和用途限制。这意味着需要被保护的，是一组明确的控制条件。不能把排他性简单理解为只有一个自然人掌握一把密钥，更不能以此推导所有权益都必须集中在同一个主体手中。

对于共享数据，还需要区分对内容的访问与对后续行动的支配。参与者可以有权查看一项收益记录，却无权修改它；可以取得某项证据副本，却无权以自己的名义重复主张同一项已归属于他人的资格。系统应当分别配置读取、提交、确认、变更与执行权限，使不同权限具有可以说明的制度理由。

排他性与可分割性之间也不存在简单冲突。某项经济利益可以被制度安排划分为不同份额，不同使用条件也可以对应不同资格。但这种划分需要明确它是在分割什么：原资产的控制、某种收益请求、某段期间的使用资格，还是其他权利。份额数量清晰，只能解决计数问题；份额的权利性质和效力仍然需要论证。

资本治理因此不能仅依靠凭证的数量结构理解参与者的位置。同样是持有一个单位，有的可能代表已经成立的回报请求，有的可能只表示参与资格，还有的可能只是待核验贡献的记录。排他性保护的^{27 / 240}对象应当由制度明确，技术则按照这种对象结构处理有效状态。

这种区分也影响制度如何处理多人同时提出的主张。某些主张相互冲突，需要判断谁具有优先或有效依据；某些主张则可以并存，分别指向所有、使用、收益或担保等不同关系。是否能够并存、效力如何排列，需要依据具体权利类型与适用制度判断。系统不应把所有并存主张都当作重复资产，也不应把所有相同标签都当作同一种权利。

由此，本书提出一项关于数字排他性的分析要求：先界定需要受到保护的^{WISERUNION V1.0}对象与行为，再确定哪些状态能够并存、哪些变化必须互斥，最后说明这种技术安排怎样对应制度认可与外部权利。排他性的价值，在于维持清晰的行动边界，使不同参与者可以据此安排合作。

数字资产的制度问题，因而从“是否能够复制”推进到“复制能够产生什么效力”。记录副本可以增加，资产状态是否成立则依赖有效规则及其适用范围。正是在这个层次上，我们需要进一步区分掌握技术手段的人，与有权享有或处分有关利益的人。

二、私钥授权、协议控制与权利归属的区别

私钥授权、协议控制和权利归属，分别回答三个问题：操作凭什么通过技术验证，谁实际上能够影响资产状态，以及谁依据有效制度享有有关权利。三者在理想安排中可以相互衔接，在实际关系中也可能分离。识别这种分离，是建立可追责的数字资产制度的重要工作。

私钥是生成相应数字签名的技术条件。以太坊账户文档说明了私钥、签名与账户之间的联系，同时区分由密钥控制的外部账户和由代码控制的合约账户。因此，资产操作的技术条件不能一律归结为某个自然人持有一把私钥。以太坊开发文档：账户〔2〕

一份通过检查的签名，可以支持判断操作满足了相应密码学条件，但仍需要理解密钥的实际使用关系。密钥可能由本人管理，也可能由受托人、组织工作人员或其他安排中的执行者使用。持有技术手段，不能单独解释代理范围、内部批准和利益归属。

协议控制进一步涉及系统允许怎样改变状态。需要检查的内容包括当前权限、合约条件、多人批准要求及其他限制。能够提出操作请求与能够独立完成转移，是不同能力；能够转移某一资产与能够更改整个合约的规则，也具有不同影响。制度分析应当识别控制的层次，尤其是能够改变他人操作条件的权限。

当存在管理、升级或恢复机制时，表面登记的持有地址未必穷尽实际控制关系。某个主体可能无法直接发起日常转账，却能够改变执行规则或暂停操作；另一个主体可能具有日常签署职责，却不能决定资产用途。本书主张将这些能力分别记录，以便理解哪些人能够在正常运行、异常处置和制度变更中影响资产。

法律上的权利归属则需要回到取得与变动的依据。交易、授权、继承、裁判或其他法律事实，可能构成需要审查的事项；具体结果取决于适用法律与有关证据。权利人的身份不应仅由某次技术操作反向推定，尤其在控制手段被盗用、代理人越权或托管关系发生争议时，需要完整审查相应关系。

UNIDROIT《数字资产与私法原则》以“控制”描述获取利益、排除他人取得相关利益以及改变控制的事实能力，并将数字资产的财产权利作为另一组法律问题处理。本书采用这种区分作为分析参照，同时保留具体法律体系对相关概念与效果的判断。UNIDROIT《数字资产与私法原则》概览，原则2、3、6〔3〕

控制与归属的分离，并不都意味着制度失效。托管和代理可以在有明确依据的情况下，将操作能力交给其他主体，同时保留受益安排与责任约束。需要说明的是，谁为谁控制，哪些操作获得授权，资产如何识别，记录怎样对照，以及关系终止后如何返还或移交。良好的技术设计应当能够支持这些问题得到回答。

相反，密钥遗失也不能仅凭技术结果推导全部权利消灭。它首先说明原有操作路径可能无法继续使用。权利是否仍然存在，能否恢复控制或取得其他救济，需要结合制度结构判断。有些系统可能没有可行的恢复机制，这会使权利实现面临实际困难，但困难本身与法律归属仍属不同层次。

在未经授权的控制转移中，也不能预先断言后续受让人的地位。UNIDROIT原则8提出了符合条件的善意取得框架，说明控制、处分权限与第三人保护之间还需要进一步法律规则。这是一项国际原则中的制度方案，其具体适用不能脱离有关法域及采用条件。UNIDROIT《数字资产与私法原则》，原则8〔3〕

三者之间的分工可以用下表达。表中强调的是分别需要什么依据，以及系统能够支持到何种程度。

分析层次	需要回答的问题	主要检查内容
私钥授权	某项操作是否满足签名等技术条件？	签名、密钥或账户条件、被授权的具体操作
协议控制	谁能够实际改变哪些状态？	当前权限、多人控制、管理与恢复能力、适用限制
权利归属	谁依法或依有效安排享有何种权利？	主体身份、取得依据、代表关系、权利对象及法律效果

据此，利益相关者资本治理需要建立从数字标识到责任主体、从操作能力到授权范围、从状态结果到权利依据的关联。员工代组织签署操作，不宜直接被记录为其个人取得收益；托管账户持有的数量，也需要能够对应不同参与者的实际安排。技术记录应当为解释这些关系提供材料。

本书进一步提出，治理系统应当保留“技术已确认、权利待核验”这一类复合状态。它允许系统准确记录已经发生的控制变化，同时说明有关归属仍待审查。这样既不会否认技术事实，也不会提前裁决法律问题。后续的纠正、移交或补偿，应当关联有权机构作出的判断及其执行过程。

只有把私钥授权、协议控制与权利归属分别识别，数字资产才能进入完整的责任结构。控制能力获得了技术表达，权利关系取得了可检查的依据，二者之间的分歧也有机会通过明确程序得到处理。

三、链上原生资产与现实资产映射的不同条件

数字资产的制度条件，还取决于其所代表的对象主要在哪里成立。本章为分析方便，将资产关系分为链上原生资产与现实资产映射两种基本情形。前者的技术存在和状态主要依托协议或合约形成，后者则通过链上记录关联外部资产或权利。这是一种研究划分，具体产品可能同时包含两类关系。

链上原生资产的识别、生成与转移条件，可以主要由相应系统描述。有关单位是否存在、由什么条件控制，以及是否已经发生转移，可以依据链上规则检查。即使不存在一项需要兑换的外部实物，这类资产仍然需要研究法律上的保护、交易关系与责任承担。技术上原生，并不意味着在社会制度之外存在。

相应地，“在链上发行”不等于所有相关权益都在链上成立。如果持有者的主要经济利益依赖某个主体付款、提供服务或交付外部资源，就需要进一步检查这些承诺。发行方式说明凭证怎样产生，不能独立说明权益的来源。资产分析应当沿着持有者实际能够提出的主张，寻找需要承担义务的主体。

现实资产映射增加了一项关键任务：建立数字记录与外部对象之间可信而持续的对应。给某项资产上传说明、生成标识或登记价格，只完成了描述的一部分工作。有效映射需要能够回答，外部对象是什么，谁有权将其纳入安排，持有者取得何种主张，以及该主张怎样随着记录变化而成立、改变或终止。

本书将这项对应关系展开为五个条件：对象可识别，关联有依据，责任可落实，状态可核对，权利可实现。五个条件共同构成映射的研究框架。它们需要根据资产性质具体化，不能仅以某项存证、一次审计或一段合约覆盖全部要求。

对象可识别，要求系统能够区分所关联的是特定实物、某一集合中的份额、对某人的请求，还是某种使用资格。不同对象具有不同的维护条件。若对象本身会变化，还需要说明替换、损耗和范围调整如何进入记录。描述越含糊，链上数量越难与真实的权益对象对应。

关联有依据，要求建立从外部对象到链上凭证的有效连接。作出映射的人需要具有相关权限，并明确凭证在制度中的作用。它可能只是证据，也可能用于登记某种合同请求，或者在适用制度认可的条件下参与特定权利的转移。不同安排不能共用一个笼统的“资产上链”结论。

UNIDROIT原则4将数字资产与其他资产的关联作为单独问题处理，并指出关联的法律效果取决于相应适用法律。本书据此把映射理解为需要明确建立的制度关系，而不将技术引用本身视为外部权利已经成立的证明。UNIDROIT《数字资产与私法原则》概览，关联资产〔3〕

责任可落实，要求有人对资产存在、资料提供、保管、交付或其他约定事项承担明确职责。证明外部资产某一时点存在，与证明持有者可以要求交付，属于不同任务。制度需要说明谁负责持续维护对应关系，谁应当披露变化，以及哪些不履行行为能够被追究。

状态可核对，要求链上记录与外部状态保持可以解释的联系。外部对象可能被处置、损毁、替换或受到新的限制，相关请求也可能已经履行或发生争议。系统应当识别哪些变化需要更新记录，哪些变化需要暂停后续操作，以及长期未取得新证据时如何提示状态。缺少更新规则的映射，可能逐渐失去其说明能力。

这种核对还应覆盖其他记录渠道。同一资产可能同时出现在内部台账、外部登记或不同平台中。某条链能够限制自身的重复发行，并不能独立排除其他渠道的冲突安排。制度应当明确认可的记录范围、外部查询责任及冲突处理程序，使映射范围与其实际能够证明的范围相匹配。

权利可实现，则要求把凭证状态连接到履行与救济。持有者可以向谁提出要求，需具备什么资格，何时能够取得交付，出现不足或拒绝时怎样处理，都属于映射关系的一部分。对于涉及托管或隔离安排的结构，还需要检查具体法律效果及破产等异常情形下的地位，不能仅凭系统标注就推定已经获得保护。

映射的终点也需要设计。外部义务履行之后，相应凭证应当如何处理，取决于它代表的具体关系。可能需要注销、标记已履行，或继续作为历史证明保留。制度需要防止已经完成的请求仍以未履行资格继续流转，也需要避免凭证技术状态的改变抹去尚未解决的责任。

分析维度	链上原生资产的主要问题	现实资产映射增加的问题
对象存在	协议或合约中何种状态构成有效资产？	外部对象是否存在，如何识别与持续核验？
控制依据	哪些条件允许改变链上状态？	发起映射和处分外部权益的权限从何而来？
权益内容	持有和使用该资产关联何种制度安排？	凭证代表何种外部权利，由谁承担对应义务？

分析维度	链上原生生产的主要问题	现实资产映射增加的问题
状态变化	生成、转移和终止怎样符合系统规则？	外部履行、处置和限制怎样反馈到链上？
争议处理	技术控制与法律归属如何核对？	跨系统冲突、资产不足及拒绝履行怎样处理？

对于利益相关者资本治理，这一区分有助于明确数字凭证承载什么。一项贡献凭证可以支持确认某种活动，但它是否附带收益请求，需要进一步安排；一项长期回报凭证可能关联企业未来履行，却不能仅因可转移就推定已经形成股权。映射设计应当从具体权益出发，再决定采用怎样的技术表达。

本节由此把“现实资产上链”展开为一项持续的制度工作。它包括初始识别和授权，也包括运行中的更新、核对、履行和纠错。区块链可以支持这项工作的记录与执行，映射的可靠性则取决于整组条件能否持续成立。

四、控制转移如何与法律上的权利变动衔接

控制转移与权利变动之间，可以通过明确的法律和制度安排建立联系。这种联系需要回答：技术变化作为证据说明了什么，在当事人关系中触发何种后果，以及在什么条件下能够影响第三人的法律地位。不同类型的权利，可能需要不同的成立与变动程序。

首先需要确定权利的性质。本章使用“财产权利”讨论较广泛的财产利益关系，使用“物权”时则关注特定法律体系中的专门概念。所有权、请求特定义务人履行的权利、知识产权和组织参与权，具有不同的分析任务。不能因为它们都具有经济意义，就赋予相同的转移条件。

中国《民法典》第114—116条对物权及其种类、内容作出规定，第127条则将数据与网络虚拟财产的保护指向相关法律规定。由此不能直接推导所有链上凭证都是同一种物权客体；具体对象和权利性质仍需分别判断。《中华人民共和国民法典》第114—127条〔4〕

确定对象与权利性质之后，需要识别相应的变动依据。有关当事人的意思表示、处分资格、必要同意以及登记、交付或其他程序，可能分别影响不同环节。制度分析应当把交易安排、履行行为和权利结果区分开来，再说明链上操作在其中承担哪一项任务。

中国《民法典》第209条与第224条分别以不动产登记和动产交付为相关物权变动的一般规则，并保留法律规定的例外。这表明，具体资产的变动条件不能被一项通用链上转账所概括。相关技术流程应当依据对象类型与适用规则建立衔接。《中华人民共和国民法典》第209条、第224条〔4〕

从制度设计角度，本书区分三种技术参与方式。第一种是提供证据，保存意思表示、授权与操作历史；第二种是辅助履行，按照有效安排执行通知、计算或交付流程；第三种是在法律认可的范围内，使特定电子记录及其控制变化承担相应的权利表征或转移功能。三种方式的效力来源各不相同，需要分别说明。

国际制度研究已经提供了技术与法律功能衔接的一条路径。联合国国际贸易法委员会《电子可转让记录示范法》在特定可转让单证范围内，以可靠的电子控制对应纸质单证的占有功能，同时要求识别记录、维持完整性并确认控制者。它采用技术中立的方法，为法律如何认可电子方式提供了参照。UNCITRAL《电子可转让记录示范法》概览〔5〕

这一制度参照的启示，在于从法律所要求的功能出发设计技术条件。若某项制度需要能够识别持有人、维持有效记录的连续性并转移控制，就可以进一步研究怎样通过可靠技术实现这些功能。但示范法需要通过有关法域的制度采用发挥相应作用，其适用范围也不能扩展为所有数字资产。技术具备某种能力与当地法律赋予相应效果，仍须分别确认。

对资本治理系统而言，衔接可以从一份完整的权利说明开始。它应当明确对象、主体、权利内容、取得条件、转移限制、对应义务及争议路径。技术标识和合约位置可以帮助定位相关记录，制度文件则说明这些记录为何具有意义。两者应当能够相互核对，并说明规则更新后哪一版本适用于哪些事项。

接下来需要建立有效的主体连接。技术账户应当根据实际安排对应本人、组织或代理关系；隐私保护可以限制公开披露范围，但在需要履行、登记或解决争议时，应有适当方式证明相关身份与权限。系统设计要同时考虑可识别性与必要保密，避免把所有人的完整信息都暴露作为确权的前提。

对一次具体转移，还需要安排前置条件、完成条件和异常处理。前置条件说明操作前必须取得哪些授权或确认，完成条件说明需要哪些事件共同发生，异常处理则说明其中某个环节失败后怎么办。当链上状态与外部登记、付款或交付不能同时完成时，应当明确过渡状态及责任承担，避免过早把整体标记为已经完成。

本书据此提出“分别确认、双向核对”的设计原则。链上控制变化需要能够核对其权利依据，外部已经生效的权利变化也需要有路径反馈到系统。这个原则旨在处理两类风险：技术记录走在权利生效之前，以及权利已经改变而技术状态仍然滞后。它要求保持各自事实的准确表达，并为不一致提供明确处理程序。

双向核对并不意味着任何外部决定都能够直接修改底层区块链。具体系统可能通过后续转移、凭证重发、状态标注或补偿安排执行有权决定，也可能缺少相应技术能力。制度设计需要预先检查哪些救济能够实现，哪些需要由其他主体履行，并明确变更权限及其监督条件。

在第三人关系中，还要进一步检查有关安排对谁具有何种效力。当事人之间同意使用某项账本，可以支持内部履行，却未必足以约束所有其他人。交易对手、外部权利人、债权人和有关机构可能依据不同规则提出主张。系统所声明的“有效”，应当能够说明适用范围及其依据，不能以内部认可覆盖尚未解决的外部效力问题。

跨境结构会使这种衔接更加复杂。对象、主体和服务可能分布在不同法域，合同选择、财产权利、破产处理与争议管辖也可能需要分别分析。技术上的全球可访问性，不能自行统一这些法律关系。制度设计应当把适用法律和争议路径作为需要明确的条件，而非在发生冲突后才寻找解释。

为了使上述条件可以被检查，本书提出以下衔接框架。它是面向制度设计的分析工具，不代替具体法域对权利效力的判断。

衔接环节	必须明确的内容	系统应当保留的依据
权利识别	对象、类型、主体及对应义务	权利说明、对象标识与有效制度文件
操作授权	谁能转移，是否需要其他同意	身份关联、授权范围与批准记录
变动生效	哪些法律事实和程序构成条件	链上结果、外部确认及生效依据
状态核对	两侧记录是否一致，何者尚待完成	分别标记的状态、更新时间与差异说明
争议救济	谁能审查、作出决定并执行	证据、处理权限、有效决定及履行记录

面向未来，可以进一步研究将这种衔接结构做成可验证的权利说明与状态接口，使不同组织能够检查某项凭证代表什么、需要满足什么条件、当前还有哪些义务。这一研究方向的价值，在于提高制度关系的可理解性与可核对性。它需要法律认可、数据可靠性和责任机制共同支持，不能仅凭统一格式完成。

本章由此将数字世界中的归属问题展开为一个连续过程：排他性界定受约束的控制范围，授权与协议说明谁能够行动，权利依据说明谁有何种主张，映射与履行连接外部对象，法律和救济则处理变动效力及其冲突。区块链可以参与这组关系的表达与执行，使其中部分依据更容易被共同检查。

对利益相关者资本治理而言，这意味着数字凭证需要拥有清楚的制度内容。参与者不仅应当知道自己控制了什么，还应当理解能够据此要求什么、需要承担什么，以及怎样在变化和争议中维护自身的正当位置。在这些条件得到说明之后，下一章将进一步讨论数字资产如何与利益相关者资本相联系，以及哪些投入能够形成持续支持共同创造的长期力量。

定稿补强：把物权命题限定在对象与法域之内

区块链的重要贡献，是使数字环境中的排他控制和状态转移可以由协议持续维持。这为数字资产的归属与转移提供了新的技术条件，但“实现物权”不能被理解为技术状态自动产生所有法域中的物权效果。法律结论仍须回答权利客体、主体资格、生效方式、登记要求、第三人效力和救济程序。

至少应区分四类对象：由协议直接定义的链上原生资产；以合同请求为基础的数字凭证；以登记或特定法律程序为基础的权利；指向实物、服务或其他链下对象的映射。第一类的排他状态主要由协议维持，其法律分类仍可能不同；后三类都需要链外义务人、登记机关、托管者或其他制度连接。凭证可以转移，而基础权利可能因资格、同意、通知、登记或禁止转让而没有同步变动。

本书继续使用“物权问题”作为理论入口，用来追问数字世界如何形成排他性、归属与可转移性；在实施层面，则必须改写成可核查的问题：对象是什么，谁承担义务，何时生效，谁可以对抗谁，错误如何纠正。只有这些条件同时明确，链上控制才可能与相应法律权利形成稳定对应。

本章注释

- [SRC-027] Ethereum Improvement Proposals: ERC-721 非同质化通证标准。[原文或官方页面](#)

- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：ERC-721通证标准、Ethereum：ERC-721 非同质化通证标准。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
2. [SRC-028] Ethereum.org：以太坊开发文档：账户。[原文或官方页面](#)
- 本章引证：以太坊开发文档：账户。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：以太坊开发文档：账户。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
3. [SRC-079] 国际统一私法协会（UNIDROIT）：Principles on Digital Assets and Private Law。[原文或官方页面](#)
- 本章引证：UNIDROIT《数字资产与私法原则》概览，原则2、3、6；UNIDROIT《数字资产与私法原则》，原则8；UNIDROIT《数字资产与私法原则》概览，关联资产。
 - 支持范围：用于确认有关法律文本、示范规则或数字资产私法原则对所引事项的正式表达，本书引用主题包括：UNIDROIT《数字资产与私法原则》概览，原则2、3、6、UNIDROIT《数字资产与私法原则》，原则8、UNIDROIT《数字资产与私法原则》概览，关联资产。
 - 使用边界：该文本的适用法域、效力层级和个案适用仍需专业法律判断；引用不构成法律意见。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
4. [SRC-004] 中华人民共和国最高人民法院网站：《中华人民共和国民法典》第114—127条、第209条、第224条。[原文或官方页面](#)
- 本章引证：《中华人民共和国民法典》第114—127条；《中华人民共和国民法典》第209条、第224条。
 - 支持范围：用于确认有关法律文本、示范规则或数字资产私法原则对所引事项的正式表达，本书引用主题包括：《中华人民共和国民法典》第114—127条、《中华人民共和国民法典》第209条、第224条。
 - 使用边界：该文本的适用法域、效力层级和个案适用仍需专业法律判断；引用不构成法律意见。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
5. [SRC-072] 联合国国际贸易法委员会（UNCITRAL）：UNCITRAL《电子可转让记录示范法》概览。[原文或官方页面](#)
- 本章引证：UNCITRAL《电子可转让记录示范法》概览。
 - 支持范围：用于确认有关法律文本、示范规则或数字资产私法原则对所引事项的正式表达，本书引用主题包括：UNCITRAL《电子可转让记录示范法》概览。
 - 使用边界：该文本的适用法域、效力层级和个案适用仍需专业法律判断；引用不构成法律意见。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第四章 – 从数字资产到利益相关者资本

数字资产能够被识别、控制和转移，说明数字系统可以支持某些明确的支配关系。对于企业和共同创造而言，还需要继续追问：这些资产及其制度安排，怎样进入实际活动，形成能够支持未来发展的力量？一项记录可以长期保存，一项凭证可以持续流转，但长期能力是否形成，仍取决于投入如何被组织和运用。

本章沿用《利益相关者资本论》的治理视角，将利益相关者资本理解为围绕共同的价值创造方向，经由多方投入和相应制度安排形成，能够跨期积累，并被持续组织和运用于未来价值创造的资源、能力与合作关系。这一定义关注积累的形成、可用性及其延续条件，具体资产确认和权益成立则需要各自的依据。

数字资产与这种资本形成可以有多种联系。它可以成为投入共同事业的一项资源，可以承载已经取得的特定权益，也可以作为支持协作的技术安排。不同联系需要分别分析。本章将从贡献如何留下长期作用开始，区分记录、计量与资本化，进而说明资产、资本和权益凭证怎样各自表达，并论证组织制度为何进入资本形成过程本身。

一、共同创造中的贡献、关系与长期能力

共同创造发生在多方活动相互作用的过程中。资金使某些行动具备资源条件，劳动使计划进入实际执行，知识支持判断与改进，需求反馈使供给获得调整依据，合作关系则把分散条件连接起来。资本治理需要理解这些投入怎样发挥作用，以及其中哪些作用可以跨越当前任务继续存在。

贡献首先表现为具体行动。它有发生的主体、时间、对象和条件，也有可以调查的过程与结果。判断贡献需要说明参与者做了什么，承担了何种责任，以及这些活动与共同任务之间有什么联系。承认贡献的多样性，可以扩展组织的认识范围；贡献是否形成长期资本，则需要进一步考察行动之后留下了什么。

当期投入与长期积累具有不同的时间含义。已经发生的工作属于过去，工作形成的方法、资源或协作能力可能继续被运用；已经完成的服务回应了当时的需求，服务过程中形成的理解和配合方式则可能影响后续活动。资本形成关注的，是这些后续条件如何产生、保留和进入新的创造过程。

因此，投入数量与资本积累之间不存在一个可以直接套用的固定比例。较多投入可能被当期活动消耗，也可能由于方向或组织条件不当而未形成持续作用；某些投入虽然不易以数量表达，却可能改善后续行动的重要条件。研究需要回到机制，辨认哪些改变确实发生，以及它们能够支持什么。

关系在其中发挥着连接作用。参与者了解彼此的能力、理解合作要求，并形成协调和处理分歧的方式，能够使知识与资源在需要时被调动。但关系的存在不能仅由联系人数、交易次数或互动频率证明。资本分析需要确认这种联系能否支持适当的行动，依赖哪些人的持续参与，以及在条件变化时能否继续发挥作用。

长期能力则体现为组织能够在相关条件下再次完成某类有意义的活动，或对新的任务作出适当调整。一次成功结果可以提供线索，但还需要识别其是否依赖偶然条件、特定个人或不可持续的资源使用。只有理解这些依赖，组织才能判断哪些能力已经积累，哪些仍需要建设。

科恩与莱文索尔关于吸收能力的研究，关注企业识别外部知识价值、吸收知识并将其用于实际活动的的能力。这为区分“取得信息”与“形成可用能力”提供了理论参照。本书据此进一步考察，共同贡献如何经由理解、整合和实践，转化为能够持续发挥作用的组织条件。Cohen与Levinthal，1990，吸收能力研究〔1〕

从贡献进入长期能力，可以分析为几个相互作用的环节。投入首先需要回应明确的价值用途，再通过角色、任务和资源的配合产生作用；活动之后需要留下可继续使用的成果；这些成果还需要有人理解、使用和维护。技术可以保存各环节的依据，组织则负责使它们形成实际联系。

这种联系可能分布在不同主体之间。企业保有一部分资源，个人保有专业能力，合作伙伴保有各自的知识和生产条件，各方通过持续协作使这些条件共同发挥作用。利益相关者资本可以存在于这样的关系结构中。分析它，并不要求把全部资源和能力的所有权集中到企业，也不意味着组织可以占有的人格与自主选择。

跨主体分布同时带来延续问题。有些成果能够在人员变化后继续使用，有些能力则依赖特定主体持续提供判断和配合。制度需要辨认不同的依赖，安排知识传递、职责交接和后续合作。关系越具有专门性，越需要向参与者说明其投入将如何被对待，以及条件变化后能够怎样调整。

长期也不意味着永远有效。需求、技术和合作环境会变化，已经形成的方法可能失去用途，关系可能中断，资源也可能逐渐耗损。资本形成因而包含积累、维护、更新与退出几个方向。持续保存贡献历史，与持续确认某项能力仍然存在，是两项不同工作。

失败的探索同样应当放入这一分析。未取得原定成果，可以是需要如实记录的结果；若探索留下了可用的认识，还应说明这些认识怎样改变后续判断。学习可能成为积累，但不能仅凭发生过支出，就把所有失败解释为已经形成等值资本。它需要有可以展示的内容和实际使用条件。

据此，本书主张以“下一次共同创造能够依靠什么”检验长期积累。回答可以涉及方法、设施、知识、组织配合和可靠的合作条件，但应当指出它们的具体用途、可用范围及维护要求。这个问题把资本分析从历史投入的加总，推进到未来行动基础的辨认。

区块链在其中可以支持贡献来源、确认过程和后续安排的追踪，使相关依据更容易由多方核对。它也可能帮助限制单方改写承诺，改善持续投入的预期。是否发生这些作用，需要结合实际制度与使用效果判断。资本形成最终仍要落实为共同事业可以运用的资源、能力与关系。

二、可记录、可计量与可资本化的不同条件

数字系统能够留下记录，也能够据规则产生数字。两种能力可以帮助组织理解贡献，却不能直接决定哪些投入已经形成资本。可记录、可计量与可资本化各有其判断对象，三者之间需要通过证据和制度条件建立联系。

可记录首先意味着某项事项能够被适当表达。记录需要说明主体、行为、对象和时间，也需要标明材料来源、确认状态及适用范围。系统能够接受一段信息，只说明它具备存储或登记形式；该信息能否作为事实依据，还需要检查来源、完整性和核验过程。

记录的意义依赖语境。同样一份文件可能用于证明提交、证明交付，也可能用于支持质量评价，但这些用途需要不同材料。制度应当明确某类记录允许支持到什么结论，哪些内容还需要补充。记录越容易传播，越需要保留其证明范围，避免后续使用者赋予它未经确认的含义。

可计量则要求先确定测量对象。时间、数量、成本、质量和对未来活动的作用，分别指向不同属性。一个准确的工时数字可以描述时间投入，却不能独立表达全部质量和价值；一项评分可以反映特定规则下的评价，也需要说明规则采用了什么判断标准。

计量还需要具有适当的尺度和比较条件。若不同类型贡献具有不同用途，直接换算为一个总分，就会引入权重与折算的选择。这些选择需要有制度理由，并允许有关主体理解和提出异议。数字能够被准确计算，与折算方法能够合理代表贡献，仍需分别审查。

共同创造还面临归因问题。多方投入可能相互补充，使最终成果难以拆分为彼此独立的部分。如果把整体成果完整归给每一名参与者，再加总各自的贡献，就可能重复计算；若只记录最后完成环节，又可能遗漏必要的前期支持。计量方法应当呈现协作关系，并在证据不足时保留共同贡献或未能明确分配的部分。

不确定性也应进入结果。某些评价可以提供较稳定的数量，另一些更适合采用区间、等级或附带条件的说明。保留这些差异，有助于避免精确外观掩盖判断的不充分。系统可以持续接受新证据并修订评价，但应当说明修订是否影响既有权益，以及由何种程序处理。

“可资本化”需要先明确资本化所指的过程。本书讨论的治理意义上的资本形成，关注共同投入是否留下可持续运用的基础；会计上的资本化涉及有关支出是否符合资产确认与计量条件；将未来回报及其权利用于估值，则属于另一种分析。不同过程不能仅凭使用相同名称就相互代替。

在治理意义上，判断某项投入具有资本形成作用，需要说明它形成了什么积累，积累能够支持哪些后续活动，使用条件是否实际存在，以及维护 and 更新由谁承担。它可以具有长期价值而暂时难以精确货币计量。相反，一项投入即使金额明确，也可能没有形成能够延续的作用。

会计判断遵循相应准则。国际会计准则第38号区分研究支出与符合特定条件的开发支出，并对内部形成的品牌、客户名单等项目设置确认限制。这说明，把某项活动纳入长期能力建设，并不能独立决定其财务报告处理。IFRS基金会：IAS 38《无形资产》〔2〕

资本治理应当尊重这种分工。某项能力未在报表中确认为资产，并不足以否定其组织意义；治理判断认为某项关系值得维护，也不足以支持自行增加报表中的资产。两种工作可以使用相互关联的证据，同时分别承担对结论的解释责任。

判断层次	需要具备的条件	能够支持的结论	仍需继续论证的事项
可记录	对象清楚、来源可查、状态可辨	某项活动或主张得到适当表达	事实是否充分确认、作用有多大
可计量	属性明确、尺度适当、方法可说明	某一维度可以进行有条件的比较	不同维度如何协调、结果如何归因
治理意义上的资本形成	跨期作用、实际可用、维护条件具备	存在支持未来创造的积累	持续范围、失效条件与具体权益依据
会计上的资本化	符合适用准则的确认和计量要求	有关项目可以按规定进入资产处理	后续计量、减值或其他适用要求

这些判断也没有固定不变的先后关系。事先的回报承诺可能促成投入，实际贡献需要随后核验，长期作用又可能在更晚阶段才显现。制度可以基于有效约定先确认应付报酬，同时继续观察资本形成结果。不能为了等待长期能力得到证明而无限推迟本应履行的义务。

从技术设计上看，记录状态、评价结果和资本判断应当能够分别更新。新增一项材料，可以提高事实判断的完整性，却未必改变长期作用；长期能力受到削弱，需要重新评价其可用性，也不必改写已经发生的贡献。保持不同时间层次的记录，有助于组织理解变化的真正来源。

本节由此提出一项基本要求：每一次从记录进入评价、从评价进入资本判断的转换，都应当说明新增了什么依据。技术可以组织转换过程和保存理由，但不能通过自动增加一个标签，让尚未成立的条件被视为已经满足。

三、资产、资本与权益凭证的分别表达

资产、资本与权益凭证可能出现在同一套系统中，却承担不同的解释任务。资产分析需要说明对象及其控制和权利关系，资本分析需要说明哪些条件持续支持价值创造，权益凭证则需要说明持有者依据什么可以提出何种主张。准确表达这些对象，是技术系统能够支持治理判断的前提。

在本书的技术讨论中，数字资产主要指能够按照明确规则识别并实施控制的数字对象。其具体法律性质已在前章说明，需要依据相关权利关系判断。若进入财务报告，还需要遵循适用的定义、确认和计量要求。国际财务报告概念框架分别讨论资产、负债、权益及有关确认和计量问题，支持这种按对象和目的区分的处理。IFRS基金会：《财务报告概念框架》〔3〕

资本在本章中采用治理意义上的分析范围。它可能包含组织能够持续使用的资产，也可能涉及分布在不同主体之间的能力和合作关系。因此，识别资本需要超出单一持有清单，说明各项条件如何连接到实际任务，怎样相互依赖，以及由谁维持其可用性。

资产转移可以改变资源由谁支配，但资本形成还需要考察新的使用方式。获得一项资源，可以为未来活动创造条件；资源是否被有效使用、是否形成新的积累，需要后续行动和证据。数字资产的流动性也可能改善资源调配，但交易发生和长期能力增长仍然属于不同结果。

权益凭证则是对特定制度资格或主张的表达。它需要连接权利主体、义务主体、取得依据、履行条件及变动规则。凭证可以采用账户记录、可验证文件或通证等形式，其技术形式应当服务于所表达的权益。有关主张是否成立，不能仅依赖持有者界面显示了某个数量。

这里还应当把权益凭证与一般贡献凭证区分开来。后者可以证明某项投入已经得到确认，但是否附带长期收益、使用资格或治理权限，需要进一步安排。把所有记录都命名为权益，会使参与者难以判断哪些事项已经构成可主张的权利，哪些仍然只是有待讨论的依据。

不同记录可以对应同一事项，但它们不是数份可以叠加的价值。同一项交付可能同时留下贡献证据、形成可以使用的成果，并依有效约定触发回报资格。三份记录从不同角度说明同一过程，不能因为出现于多个账户，就把其作用重复计算为多份新增资本。

反过来，一项共同能力可能关联多份贡献记录，而同一贡献也可能支持不止一种后续活动。这要求系统表达关联关系，并在汇总时说明口径。共同能力、投入金额、凭证面额和市场价格具有不同单位与含义，不适合在缺少明确方法时合并为一个总量。

本书因此主张建立相互关联而分别负责的记录体系。贡献记录关注活动与证据，资源和资产记录关注对象及使用条件，资本分析关注跨期作用与依赖关系，权益记录关注资格、义务和履行状态。各类记录通过明确事项相互连接，使组织既能够追溯来源，也能够区分判断。

记录对象	主要说明什么	更新依据	不应直接推定的结果
贡献记录	谁在何种条件下完成了什么	新证据、确认、异议与纠错	自动形成等额资本或特定权利
资源与资产记录	有哪些可识别对象，怎样取得和使用	取得、转移、使用、限制与处置	对象存在即意味着已经形成组织能力
长期资本分析	哪些资源、能力和关系仍支持未来活动	使用结果、依赖变化、维护与失效信息	所有分析结果都可以进入财务报表
权益记录	谁可以向谁主张什么，并承担何种条件	有效授予、资格变化、履行与争议处理	凭证数量等于实际价值或治理权重

这种分别表达，有助于处理长期能力与既有权益变化不同步的问题。能力可能因用途改变而削弱，但已经成立的报酬义务仍需按照其依据处理；能力可能在新的合作中显著改善，但原有参与者是否取得追加权益，也需要明确规则。资本状态的变化可以触发审议，不能自动替代权利变动的程序。

同样，权益凭证的转移并不必然带走支持它的全部能力。某些收益请求可以按照约定变化主体，形成收益的组织知识和协作关系却仍留在原有合作结构之中。若忽略这种差异，就可能把凭证流通误认为能力本身能够无成本转移，也可能忽略持续维护者所承担的工作。

对于具有市场交易条件的凭证，价格还会反映交易者对其权利内容和未来结果的判断。市场价格可以成为需要解释的信息，却不能独立衡量每一项贡献，也不能证明企业已经取得同等数额的资源。外部参与者之间转让凭证，与资源实际进入企业，必须分别记录。

凭证对资本形成的积极作用，应当从具体机制中寻找。它可能让参与者更清楚地了解长期安排，帮助获得新的合作资源，或者使已有权益更方便地核验和履行。——如果这些变化促进了知识投入、能力维护或有效协作，便可以进一步研究其资本形成作用。证明应当连接凭证安排、参与行为与真实积累，而不能停留在发行数量上。

在制度设计中，还可以让权益表达更多时间和条件信息。已经取得的资格、尚需继续履行的条件、对应收益期间及终止安排，可以分别显示。这样的表达有助于参与者理解其位置，也有助于组织检查承诺是否超出实际能力。技术的价值由此体现在让复杂关系更容易核对。

本节所提出的分别表达，并不把各类事项割裂。相反，只有各自含义清楚，系统中的关联才有可靠意义。贡献提供来源依据，资产说明资源条件，资本分析解释长期作用，权益记录组织各方的主张与义务；四者共同支持对资本治理全过程的理解。

四、长期资本形成为什么仍需要组织制度

长期资本依赖组织制度，是因为共同创造需要持续协调不同主体的行动。资源、能力和关系不会仅凭存在就自动进入共同任务。它们需要被选择、组合、使用和维护，也需要使承担这些工作的人理解参与条件。组织制度正是在这些环节中支持积累的形成与延续。

首先，组织需要确定共同事业的价值方向。投入能够解决什么问题，服务什么需求，哪些长期能力值得建设，都需要经过判断。记录和核验可以帮助取得依据，但难以替代对用途和优先顺序的选择。方向不清楚时，更多参与和更密集的数字活动也可能只增加成本。

其次，制度需要组织互补投入。不同主体提供的知识、资源和判断，必须在适当时点进入相应任务。职责分工、信息交流、专业复核和协调程序，决定这些条件能否共同发挥作用。规则的价值应当体现在它帮助参与者完成必要配合，而非单纯增加参与环节。

长期资本的维护还需要识别谁在持续承担工作。某项成果已经形成之后，仍可能需要更新知识、保养资源、培训接续人员或协调合作关系。这些活动容易被视为理所当然，却会影响积累能否继续存在。资本治理应当让维护责任可见，并安排与之相适应的资源和回应。

因此，收益分配与再投入需要放在同一长期视野中讨论。可以用于分配的资源，需要依据实际经营及有效安排确认；能力维护需要的资源，也应当具有明确来源。对未来收益的期待可以支持规划，却不能代替当期可使用的条件。组织应当说明哪些支出维持现有能力，哪些投入探索新的方向，以及相应负担由谁承担。

可信承诺进一步影响参与者是否愿意继续投入。许多知识和关系的形成，需要主体在当前付出时间、承担机会成本，并等待未来结果。制度应当使参与者能够理解其付出将如何确认、既有回报回应了什么，以及仍有哪些风险和责任需要处理。这些安排能够为持续合作提供理由，其实际作用仍需通过参与者行为和合作质量检验。

权益设计因而需要同时回看已有安排和面向未来。已经支付的报酬不能被忽略，尚未兑现的义务也不能因为另行发行凭证而消失。长期回报可以具有多种形式，应当分别说明取得依据、履行资源和调整程序。组织需要防止在名义上增加权益，却把原本应当承担的责任转换为不明确的未来期待。

共同治理则为重要选择提供程序。长期投入由谁批准，维护成本如何分担，哪些事项需要听取受影响者意见，以及遇到资源不足时如何调整，都涉及利益协调。制度应当把决定权限与责任联系起来，让掌握资源和解释规则的主体接受相应监督。

这种治理还需要处理投入之后的条件变化。参与者已经为共同事业形成专门能力，可能因此承担更高的调整成本。制度应当说明原有承诺怎样保护、何种变化可以触发重新协商，以及合理退出需要履行什么程序。退出安排清楚，可以帮助各方在进入合作时作出更有根据的判断。

维护共同能力与尊重主体自主性应当一同考虑。个人知识与能力的成长具有自身价值，不能仅按企业能够取得的产出来评价；客户的购买也不当然附带继续推广或共同经营的义务。利益相关者资本治理应当在明确参与条件的基础上组织合作，让企业需要与参与者自身的发展可以被同时讨论。

制度还需要辨认合作持续的原因。关系长期存在，可能来自双方认可其价值，也可能来自信息不足、依赖过强或退出困难。只有观察参与者能否理解条件、表达异议并作出实际选择，才能判断所谓稳定是否具有可信的基础。资本治理不应把受困于某种关系的持续参与，当作长期能力良好维护的充分证据。

区块链可以参与这些制度工作的若干关键环节。它可以支持多方核验承诺版本与权益变化，可以在适当权限设计下执行部分分配和限制，也可以使某些调整留下可检查的轨迹。它的作用需要被具体定位到合作中的问题，再检查是否确实改善了确认、履行或监督。

技术安排本身也可能产生新的制度成本。复杂规则会提高理解难度，数据维护需要持续工作，基础设施控制可能集中在少数主体手中。若新增系统只是使执行更加复杂，却没有改善长期投入和责任协调，其资本治理意义就需要重新评价。制度应当能够根据证据缩小、调整或替换技术方案。

由此，可以把长期资本形成理解为一个反复发生的过程：可信承诺支持投入，投入经过协同留下可用积累，积累支持后续创造，成果为回报和再投入提供条件，履行与评价又影响下一轮合作。这个过程可能被需求变化、能力损耗或责任失衡打断，需要治理不断识别并回应。

本书据此提出一项面向系统设计的要求：在记录“曾经形成了什么”的同时，持续记录“现在还能依靠什么”和“接下来由谁维护”。过去的贡献记录保留来源，当前能力判断说明存续状态，未来维护安排则标明必要行动。三种时间视角结合，可以使长期资本分析更加具体。

面向未来，还可以研究跨组织的能力协作。不同组织在保留各自资源和权利的同时，通过明确的使用、贡献确认和权益安排形成长期联系。技术可以支持部分凭证互认和责任记录，但能否形成共同能力，仍取决于任务配合、语义理解和持续履行。互联的账户需要与实际能够开展的合作相对应。

人与智能体共同参与的情形，也应当接受同样的检验。自动生成更多内容、执行更多任务，可以改变投入方式，却不能独立证明组织已经形成更强的长期能力。需要进一步观察知识是否被理解和采用，成果质量是否得到保持，关键责任是否有人承担，以及自动化是否帮助参与者更好地解决实际问题。这些问题构成后续未来制度研究的依据。

从数字资产进入利益相关者资本，核心是完成从可控制对象到可持续创造条件的连接。数字技术支持对象识别、状态确认和部分规则执行；组织制度则把价值方向、行动配合、权益依据和持续维护联系起来。两者在各自能力范围内协同，才可能让分散贡献成为共同事业能够继续运用的长期基础。

本章由此明确，资本形成既包含真实积累，也包含使积累可用并能够延续的制度条件。要进一步解释这些条件如何取得共同认可，就需要讨论参与者怎样形成目标和原则、怎样制定处理分歧的规则，以及怎样把规则交由技术执行。下一章将从社会共识进入制度规则的形成过程。

定稿补强：治理资本与会计概念分层

利益相关者资本描述共同创造经过组织吸收、持续使用和风险承担后，成为支持共同事业的跨期能力及其制度关系。它回答的是组织为什么应当承认某项长期作用，以及如何据此安排责任、权益和治理。这个判断不等同于财务报告中的资产确认、所有者权益、实收资本或注册资本。

一项知识、关系或能力可以在治理上被视为重要资本，却可能因为不可辨认、组织不能控制、成本无法可靠计量或其他原因，不能作为资产列入财务报表；反过来，财务报表中的资产也未必对应本书讨论的利益相关者贡献关系。制度设计可以保留两套有联系而不混同的记录：治理记录说明贡献—资本—权益的依据，会计系统依适用准则完成确认、计量和列报。

由此，资本形成决定必须注明其用途。用于治理承认、内部资源配置、合同安排、公司法程序、财务报告或税务处理时，应分别满足相应条件。一个名称不能替代这些判断，一个账户也不应同时承担全部功能。

本章注释

1. [SRC-055] Wesley M. Cohen、Daniel A. Levinthal： **Absorptive Capacity: A New Perspective on Learning and Innovation**。 [原文或官方页面](#)

- 本章引证：Cohen与Levinthal，1990，吸收能力研究。
- 支持范围：用于支持所引理论、模型、算法或经验研究的原始论证，本书引用主题包括：Cohen与Levinthal，1990，吸收能力研究。
- 使用边界：原始研究支持其设定范围内的结论，不直接证明本书提出的治理制度已获得普遍实证验证。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-052] 国际财务报告准则基金会（IFRS Foundation）： **IFRS 基金会：IAS 38《无形资产》**。 [原文或官方页面](#)

- 本章引证：IFRS基金会：IAS 38《无形资产》。
- 支持范围：用于确认财务、审计、内部控制或公司治理中的规范口径，本书引用主题包括：IFRS基金会：IAS 38《无形资产》、IFRS基金会：IAS 38《无形资产》。
- 使用边界：规范口径需要结合适用主体、报告目的和具体交易事实，不宜机械移用于链上权益。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

3. [SRC-051] 国际财务报告准则基金会（IFRS Foundation）： **《财务报告概念框架》**。 [原文或官方页面](#)

- 本章引证：IFRS基金会：《财务报告概念框架》。
- 支持范围：用于确认财务、审计、内部控制或公司治理中的规范口径，本书引用主题包括：IFRS基金会：《财务报告概念框架》。

- 使用边界：规范口径需要结合适用主体、报告目的和具体交易事实，不宜机械移用于链上权益。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第五章 – 从社会共识到制度规则

共同创造需要一定程度的共同认可。参与者需要理解正在共同完成什么，为什么值得投入，以及彼此可以期待怎样的行为。然而，对一个方向表示认同，还没有完整回答谁承担义务、谁取得权利、决定如何作出和变化如何处理。社会共识要成为能够持续运行的合作秩序，需要经过制度化的过程。

这个过程包含对共同认识的表达，也包含对分歧的处理。不同主体可能认可同一目标，却对投入节奏、风险承担和回报方式持有不同判断。制度需要让这些差异进入明确的讨论与决定程序，使参与者知道哪些事项已经形成有效安排，哪些仍待协商，以及谁有权继续处理。

区块链能够支持部分规则的确认与执行，但规则从何而来，仍需在社会关系与治理过程中解释。本章由此研究共同目标、参与边界和分配原则如何进入权利义务，规则制定与修改的权力如何取得依据，以及社会共识、治理决策和账本状态共识怎样分层衔接。

一、对共同目标、参与边界与分配原则的认可

共同目标为合作提供方向。它需要使参与者能够理解，共同事业希望改善什么条件、服务什么需要，以及准备形成什么长期能力。目标足够清楚，各方才有可能判断自己的投入是否适当，怎样与他人配合，以及成果是否值得继续维护。

目标认可不要求参与者具有相同的个人动机。不同主体可以分别重视收入、专业成长、资源利用、服务改善或长期合作。制度需要使这些动机在一定范围内相容，并明确共同事业能够回应什么。对差异的承认，有助于把宏观目标转化为各方可以理解的参与理由。

共同目标还需要能够指导选择。多个行动方向发生竞争时，组织依据什么确定优先顺序；当前分配与长期投入发生张力时，怎样讨论资源使用；某项经营机会会对他人造成不利影响时，又需要遵守什么边界。这些问题决定目标能否进入实际治理，而不只是停留在倡议中。

本书主张，目标的制度化表达应当同时说明价值用途、主要责任和判断依据。价值用途指向希望形成的成果，主要责任说明哪些利益需要被认真对待，判断依据则帮助组织识别偏离与改进。具体指标可以辅助评价，但应当保留对指标未覆盖影响的审查，避免目标被单一数值替代。

参与边界随后回答谁以何种方式进入合作。了解一项计划、使用某项服务、提交贡献、接受委托和行使治理权限，属于不同的参与关系。一个主体可以同时具有多种角色，但每种角色所涉及的条件和后果应当分别说明。

尤其需要区分受到影响与接受义务。企业活动可能影响没有签署合作安排的人，这些主体的正当利益仍然需要回应；另一方面，把某人列为利益相关者，并不能据此为其设定未经有效依据成立的出资、推广或持续劳动义务。参与边界应当同时识别组织应当尊重谁，以及能够依据什么要求谁履行。

在资本治理中，可以从事项范围、角色资格、资源承诺、信息权限和退出条件几个方面描述参与边界。事项范围说明共同处理什么，角色资格说明可以实施什么，资源承诺说明需要投入多少及何种条件，信息权限说明可以查阅与披露什么，退出条件则说明合作怎样终止或转变。各项边界应当与实际关系对应。

边界还需要覆盖代表关系。参与者以本人名义表达意见，与代表某一组织或群体作出承诺，具有不同作用。代表应当说明由谁产生、能够处理哪些事项，以及哪些重大变化仍需要取得进一步授权。若代表关系不清楚，少数人的认可就可能被误写为整个群体已经接受。

分配原则是共同认可中更具实质性的一部分。它需要解释哪些因素影响回报，为什么这些因素具有理由，以及如何与责任和风险相联系。贡献可以构成重要依据，但已有报酬、持续义务、风险承担和需要保护的基本权利，也应进入相应判断。分配原则的任务，是使有关选择能够被解释和审查。

在长期资本形成中，还应当讨论分配与维护的关系。可用资源怎样在当期履行、能力更新和未来投入之间安排，需要有明确依据。参与者应当能够了解，哪些资源已经承担义务，哪些仍可由集体决定使用，以及有关保留和投入由谁监督。对分配原则的认可，应当包含对其资源条件的理解。

这种认可不能被简化为对某个比例的同意。相同比例在不同计算口径、取得条件和支付顺序下，可能产生不同结果。讨论原则时，需要把收益来源、成本处理、适用期间和不确定性表达清楚。原则越抽象，越需要在正式采用前说明具体后果。

目标、边界和分配原则之间还需要相互核对。组织宣称重视长期共同创造，却只奖励短期可见结果，会形成激励上的张力；组织希望成员承担共同责任，却不予理解 and 监督相关事项的条件，也可能削弱合作基础。制度形成应当识别这些不一致，并通过调整具体安排回应。

认可还具有程度和范围。参与者可能认同目标，但尚未接受分配方法；可能接受某项试行规则，却保留对长期适用的意见；也可能只认可某一部分安排。记录这些差异，有助于组织知道还需要讨论什么。把所有反馈压缩为一个“已同意”状态，容易抹去尚未解决的事项。

奥斯特罗姆关于多中心治理的研究，将分析视野扩展到不同尺度上的多样制度安排。这为理解共同创造中的参与差异提供了参照。本书据此进一步提出，合作可以围绕必要的共同目标与程序形成，同时为不同角色保留适当的自主范围。Ostrom, 2009, 诺贝尔奖演讲〔1〕

因此，社会共识可以被理解为共同事业得以展开的一组认可关系。它可能逐步形成，也可能随履行经历发生变化。制度需要使这些认可有明确对象、有可以理解的后果，并在分歧中保持继续讨论的空间。

二、共识如何形成明确的权利义务与决策程序

社会共识进入制度规则，需要完成从一般认可到具体关系的转换。参与者认同贡献应当得到回应，还要进一步说明哪些行为属于贡献、怎样确认、回应由谁承担，以及何时产生可主张的权益。共同原则只有进入这些条件，才能成为各方据以行动的安排。

这种转换首先需要确定事实与资格。制度应当明确什么事项可以提交，采用何种证据，谁具有确认权限，以及证据不足或存在异议时怎样处理。事实确认和资格授予可以关联，但应当各自保留依据，避免确认一项活动之后就默认全部权益已经成立。

权利表达需要说明主体、内容和行使条件。获得信息、提出异议、取得回报、使用资源及参与决定，分别对应不同事项。每一种权利都应当找到适当的实现路径，使参与者知道向谁提出、通过什么程序得到回应，以及受到不当限制时怎样请求处理。

义务表达则需要明确相应责任。承担者应当知道需要交付什么，达到何种标准，在什么期间履行，以及哪些情形可以启动调整程序。义务所依赖的资源与权限也需要检查。组织无法支配的资源，不能仅凭集体期待被当作已经具备的履行基础。

当原则允许多种实现方式时，需要把选择交给有权的决定程序。技术人员可以说明不同实现的条件和成本，专业人员可以提供影响判断，但涉及权益与责任的实质选择，需要形成可以追溯的决定。默认参数和界面设置如果改变了参与者的处境，也应当进入这一审查范围。

决策程序首先需要明确事项类型。日常执行可以在既定授权内处理，个别事实争议需要复核，改变分配依据或参与资格则可能需要规则修订程序。事项分类决定由谁处理、需要多少信息以及采用何种决定方式。将所有问题交给同一种投票，可能使专业判断与集体权力相互混淆。

接下来需要说明程序怎样开始。哪些主体可以提案，提出时应当说明什么，谁负责判断材料是否齐备，以及提案未被受理时如何获得理由，都影响参与能否实际发生。提案入口应当能够支持不同群体表达必要问题，同时通过明确要求避免无关或重复事项占用全部治理资源。

讨论阶段需要使有关信息可以被理解。提案的目标、替代方案、受影响对象、资源要求及主要不确定性，应当在决定之前呈现。对于重要安排，还需要说明不采用提案会有什么后果。参与者据此才能比较选择，而非仅对一个已经包装完成的结论表示支持或反对。

决定方式应当与事项性质相匹配。可以采用授权决定、代表审议、表决或需要特定主体同意的安排，但每一种方式都需要说明依据。若采用表决，就应当事先确定资格、参与门槛、计票口径、弃权处理以及意见相持时的后续程序。规则不能在看到结果后再临时调整。

通过决定也不是过程的终点。制度还需要明确生效条件、执行主体、资源准备和监督安排。有些决定需要进一步签署、取得必要同意或完成其他适用程序，内部通过与全部条件满足应当分别记录。系统在条件不足时应当准确显示待完成事项。

为保持这一转换的完整性，本书提出从原则到执行的对应关系。

共同认可的内容	需要形成的明确规则	执行与核验需要保留的依据
共同创造应当获得回应	贡献范围、确认程序及回报条件	事实材料、审核结果、适用规则与义务主体
重要决定应当适当参与	参与资格、代表关系与决策权限	提案、意见、授权及决定理由
资源使用应当可以监督	信息范围、审查权限与报告要求	资源来源、使用记录与检查结果
错误应当能够纠正	异议入口、复核职责与处理程序	异议材料、复核依据与后续履行
规则应当可以合理更新	修改权限、生效条件与过渡安排	新旧版本、影响说明及有效批准

这种对应关系应当保留不同阶段的状态。倡议、草案、审议通过、满足生效条件、开始适用和已经执行，不能被统称为完成。每个阶段产生的后果不同，参与者也需要知道自己面对的是讨论材料，还是已经对有关主体具有约束的安排。

技术在其中可以支持材料关联、权限检查和过程追踪。它可以帮助确认某次决定所依据的版本，防止已撤回草案被误用于执行，也可以显示哪些前置条件尚未满足。这些能力使制度形成的过程更容易被检查，但具体认可和批准的效力仍需要相应依据。

原则没有覆盖的情形，也需要预留处理方式。专业裁量可以保留在具备资格的主体手中，同时要求其说明理由并接受复核；重大例外可以转入有权机构审议；反复出现的问题则可以触发规则评估。承认规则可能不完备，有助于建立持续学习的制度。

共识由此形成具体规则，并开始对行动产生可预期的约束。转换的质量体现在参与者能否清楚理解自己的位置：哪些权利已经成立，哪些义务需要履行，哪些问题可以由谁决定，以及发生分歧后通过什么程序继续处理。

三、谁制定规则、谁接受规则、谁有权改变规则

规则如何取得约束力，需要说明制定和适用的依据。起草者可以提出完整方案，但起草能力并不自动产生对他人的决定权；参与者可以认可某个目标，却未必因此接受所有具体义务。制度形成必须把提出建议、作出有效决定和承担执行责任分别识别。

规则制定可以包含不同工作。有人发现问题并提出方向，有人完成制度设计，有人提供专业审查，也有人依相应权限批准采用。多个角色可以由同一主体承担，但角色之间的关系需要明确。尤其在方案直接影响起草者利益时，应当让利益关系可见，并安排适当的审议和监督。

规则形成需要可追踪地分开起草、审查、批准和生效；文本被整理或发布，不能直接推定为所有相关主体已经接受其实际后果。第二十二章将以版本状态和生效程序展开这一过程，本章只确定制定权、接受范围与修改权必须分别找到依据。

在组织设立或新合作开始时，初始规则同样需要找到依据。发起者可以在其合法权限内提出参与条件、投入自己的资源并邀请合作，但规则能够适用于谁，需要结合组织形式、已有权利和有效约定判断。不能仅因发起者建立了系统，就把所有接入者自动纳入其全部治理范围。

本书主张，初始制度应当明确共同处理的事项、发起者的权限、参与者进入的条件以及后续形成正式安排的程序。对于尚在试行的规则，还应当说明期限、评价方式和未完成事项。试行可以帮助各方学习，但其间实际作出的承诺和已经发生的履行，需要按照各自依据处理。

规则的接受范围应当具体记录。接受一项服务条款、加入某项合作、授权某人代表自己以及同意一项权益变更，指向不同内容。制度应当说明认可的是哪一版本、哪些条款、何种期间和相应后果，并使重要变化能够被受影响者理解。

这里讨论接受，并不意味着一切制度约束都只能依赖个人逐项同意。组织权限和外部法律也可能提供相应适用依据。关键在于不能混用依据：由有效组织程序产生的决定，应当说明权限与范围；需要特定同意的事项，应当取得相应同意；对外部主体的责任，也不能由内部表决单方排除。

接受过程还需要考虑信息和权力条件。长篇难懂的说明、过高的退出成本或对必要服务的依赖，可能影响参与者实际表达意见的能力。制度设计应当检查重要内容是否易于理解，是否提供合理的判断时间，以及是否存在可使用的询问和异议渠道。记录一次操作，并不能完整说明这些条件。

对于群体参与，代表机制需要同时说明产生、履职和更替。代表由谁选任，能够处理哪些事项，怎样向相关群体报告，出现利益冲突时如何回避，都关系到其意见能否适当地表达群体需要。任期、罢免或更换程序也应当明确，使代表关系能够接受持续检查。

规则修改权尤其需要独立论证。负责日常执行的人可能最了解运行问题，因而适合提出修改建议，但是否有权直接改变规则，需要根据已有授权判断。管理系统、保管密钥或维护软件，均不应被直接解释为具有无限的制度修改权。

本书进一步区分三类变化。纠正事实或计算错误，是使结果恢复到原规则要求的状态；按照原规则设定的条件调整参数或资格，是既有安排的实施；改变取得条件、分配依据或责任结构，则涉及规则本身的修订。三类变化应当使用不同的权限依据，并保留其真实性质。

修改程序还需要辨认时间上的影响。对尚未开始的合作，可以在适当程序下提出新条件；对已经依据原承诺作出的投入，需要说明变化如何影响预期；对已经成立的权益和义务，则应根据有效安排与适用制度处理。某项权益尚未最终取得，也不意味着此前的承诺和投入可以不受审查地被忽略。

因此，修改提案应当说明问题来源、替代方案、受影响对象及过渡方式，并明确从何时起适用。新旧规则之间需要有可以查明的联系，使参与者能够判断具体事项应按哪一版本处理。系统中的版本更新记录，应当能够对应实际有效的修改决定。

紧急处置也应当保持权限边界。制度可以预先允许在特定异常下暂停部分操作或采取保护措施，但应当说明触发条件、影响范围、持续期限及事后复核。紧急权限的目的和适用范围，需要接受监督，避免临时安排长期替代正常治理程序。

当规则本身规定了修改方式，还需要保护修改程序免于被随意绕过。若管理者能够先单方降低通过条件，再按降低后的条件批准对自己有利的规则，原有约束就可能失去意义。制度设计应当审查修改规则本身的权限与程序，并说明基本保护如何得到维持。

在区块链环境中，技术上可以出现不同软件版本或不同网络选择。它们为应对分歧提供某些行动空间，但企业合作中的资源、合同和既有责任如何处理，仍需根据具体关系决定。建立另一套技术记录，并不能单独解决所有利益分离和责任衔接问题。

规则制定、接受与改变由此形成一组连续的授权关系。每个阶段都需要明确谁在什么范围内行动，其依据如何取得，以及后果由谁承担。制度技术的作用，是帮助保存和执行这些关系，使掌握技术控制的人也能够受到相应规则约束。

四、社会共识、治理决策与账本状态共识的分层

区块链语境中的“共识”容易覆盖多种不同判断。人们愿意参与共同事业，可以被称为形成共识；有权机构通过一项规则，可以被称为形成决定；节点依协议接受某个账本状态，也被称为达成共识。它们相互关联，但确认的对象与产生的效力不同。

本书把这些过程分为社会共识、治理决策和账本状态共识三个层次。分层的目的，是明确哪些问题已经解决、哪些仍需处理，并让不同性质的分歧找到适当回应者。这一框架用于解释制度与技术的连接，并不意味着每个组织都必须按相同结构设立机构。

社会共识关心共同事业为何能够得到支持。它包括对目标、参与条件和基本原则的认可，也包括对合作经历的评价。其表现可以来自讨论、说明、实际合作和持续反馈，通常具有范围与程度。社会共识能够增强制度的支持基础，但它本身未必已经形成足够具体的权利义务。

治理决策则在明确权限和程序下处理具体事项。它可以形成规则、批准安排、确定责任或处理争议。其有效性需要检查事项是否属于权限范围、必要程序是否完成，以及相关决定如何与既有制度衔接。表决结果是可能的证据之一，不能脱离整个程序单独判断全部效力。

账本状态共识关心节点依照既定协议接受哪些交易历史和状态。具体的参与、确认与容错结构由第九、十章解释；在本章的三层模型中，只需确认它解决协议范围内的状态问题，并不独立裁决企业规则是否公平或现实材料是否真实。

三个层次可以通过下表对照。

层次	主要确认对象	参与主体	需要保留的依据	本层不能独立完成的判断
社会共识	共同目标、参与条件与基本原则是否得到认可	相关参与者、代表及受影响者	讨论内容、意见范围、分歧与反馈	具体权利是否已经成立，谁有正式决定权限
治理决策	某项规则或事项是否按有效程序得到决定	有相应资格和权限的主体	提案、授权、审议、决定及生效条件	技术实现是否正确，全部节点是否已采用
账本状态共识	哪些交易和状态符合协议并被接受	按协议参与的节点及验证者	有效性检查、确认结果与相关技术证据	现实事实真实性、制度正当性与外部法律效果

从社会共识进入治理决策，需要把认可转化为明确的议题、权限和程序。广泛赞成一个方向，可以支持启动规则设计，却不能让任何起草者自行代表全部参与者作出承诺。治理程序应当确认哪些共同认识已经足以形成安排，哪些分歧需要继续处理。

从治理决策进入技术运行，需要把有效规则转化为可以检查的条件与执行逻辑，并核对实现是否忠实于决定。规则通过之后，程序可能尚未部署；程序部署之后，外部材料、资源或其他生效条件也可能尚未具备。因此，治理通过、技术准备和实际适用应当分别表示。

从技术结果返回制度判断，同样需要明确证明范围。账本可以证明某项操作按照协议被接受，还需要结合应用规则解释其实际意义。如果记录内容来自有权审核者的声明，技术可以检查声明形式及相关授权，但审核者的事实判断仍需接受相应复核。

三个层次还可能发生不同步。技术系统可以继续按照旧规则运行，而参与者已经对其分配原则产生重大异议；治理机构可以通过新安排，而必要的技术部署尚未完成；账本也可能因网络问题暂时无法确认，但组织此前承担的责任并不会仅因确认停顿而得到完整处理。制度需要识别不同步发生在哪一层。

分层之后，纠错路径也更加清楚。证据有误，应当回到事实核验；规则被错误适用，应当检查执行与解释；决定超出权限，应当审查治理程序；规则本身受到质疑，则需要进入修订与协商。不能要求增加更多节点确认来解决利益分配争议，也不能仅凭重新投票解决程序实现中的技术错误。

协议自身的演进同样要分别观察规则如何形成、软件如何采用以及运行如何确认。第二十一、二十二章将处理治理权配置与规则生命周期；此处只说明社会协调、治理决定和技术采用可能不同步。

本书进一步强调，底层网络的确认权与企业治理权需要各自建立依据。验证者可能服务于大量互不相关的应用，企业参与者也可能没有能力或必要运行底层节点。协议采用的确认权重，不能直接成为企业配置贡献权益或经营表决权的理由。

这种分层还允许多元制度在共同技术基础上运行。不同组织可以共享某些证据和记录条件，同时保留各自的成员规则、分配安排与决策程序。跨组织协作需要明确哪些结果相互认可、认可到什么程度，以及发生冲突时怎样处理。共同使用一条链，并不要求各方在所有制度问题上达成一致。

面向未来，可以研究让每项重要技术结果附带可核对的制度关联：它依据哪一项有效规则，由谁确认前置事实，代表什么权益变化，以及存在什么复核路径。这种关联有望帮助参与者跨越技术界面，理解结果的制度含义。其效果需要通过实际可用性与争议处理质量检验。

人工智能也可以参与材料整理、意见归纳和规则影响分析，但自动生成的建议不能仅凭数量或计算能力获得额外治理权。代理谁表达意见、在何种范围内作出选择，以及错误由谁负责，需要明确授权。未来的制度技术应当提高参与者理解和处理复杂问题的能力，同时保留权力依据的可追溯性。

本章由此把“共识转化为制度，用技术执行制度”展开为一个可以审查的过程：围绕共同事业形成认可，通过有效治理产生明确规则，技术按照规则支持共同状态与执行，运行结果再进入评价、复核与修订。社会共识提供合作基础，治理决策形成具体安排，账本状态共识支持特定技术事实的共同确认。

这三个层次相互支持时，参与者能够同时理解共同事业的方向、自身的制度位置及系统结果的含义。分歧也能够按照其性质进入适当程序，而无需被压缩成同一种同意或拒绝。这样的制度联系，为长期贡献和共同未来建立了更具体的基础。

在此基础上，下一章将考察制度技术的适用条件与选择边界：哪些协作问题需要共享账本，哪些问题可以通过其他方式处理，以及怎样比较不同方案对成本、隐私和权力结构的实际影响。

本章工具与图表

本章的制度关系可结合[附录八](#)、[附录十一](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

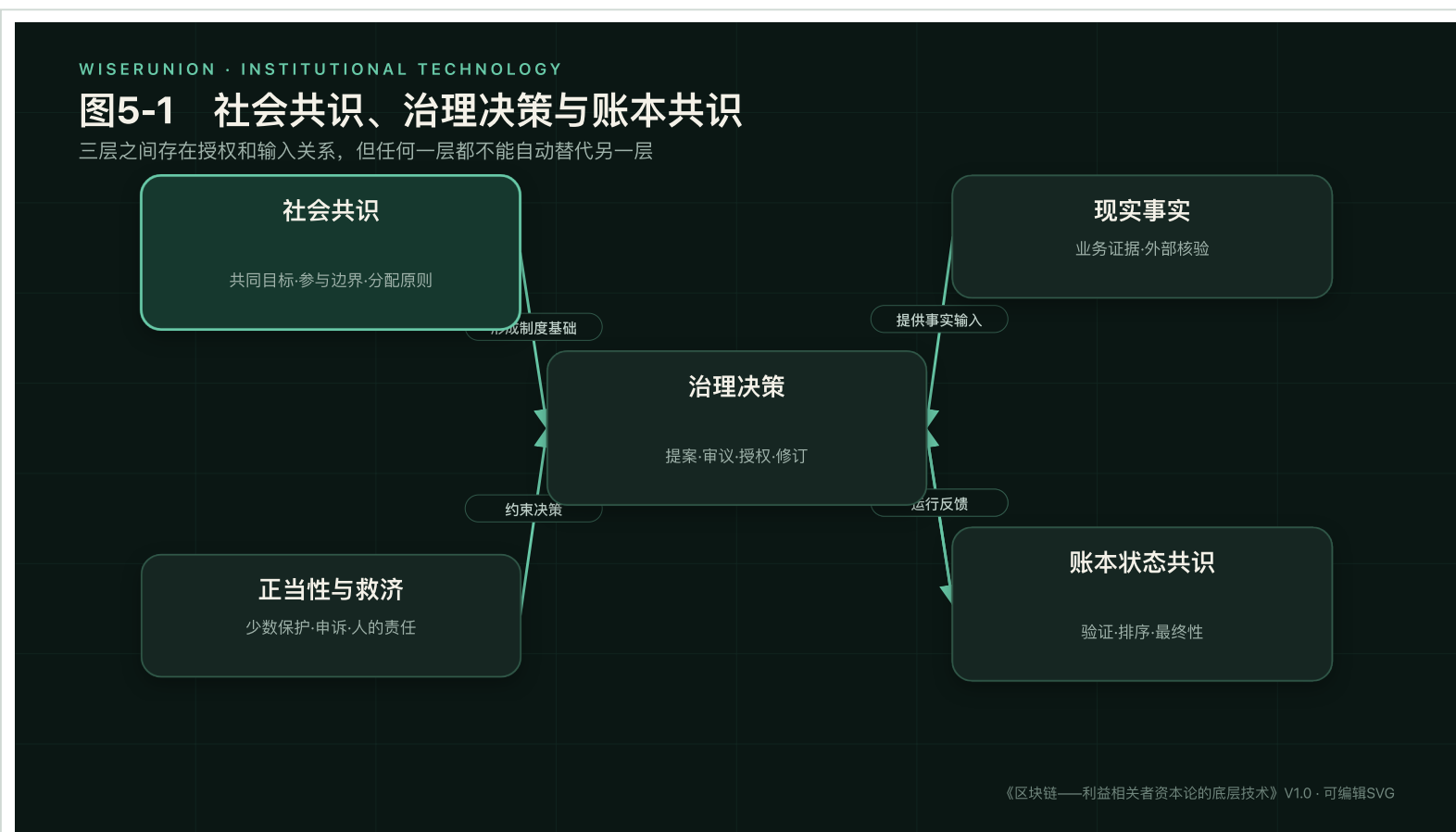


图5-1 社会共识、治理决策与账本共识

图5-1 社会共识、治理决策与账本共识。三层之间存在授权和输入关系，但任何一层都不能自动替代另一层

本章注释

- 本章引证: Ostrom, 2009, 诺贝尔奖演讲。
- 支持范围: 用于支持所引理论、模型、算法或经验研究的原始论证, 本书引用主题包括: Ostrom, 2009, 诺贝尔奖演讲。
- 使用边界: 原始研究支持其设定范围内的结论, 不直接证明本书提出的治理制度已获得普遍实证验证。
- 证据等级: A (原始法律、正式标准、原始研究或正式规范); 链接状态: 已完成可访问性核验, 核验日: 2026-10-08。

第六章 – 制度技术的适用条件与选择边界

将区块链理解为制度技术，需要进一步回答一个选择问题：什么样的制度安排值得由区块链承载？前五章已经讨论共同状态、数字控制、资本形成和规则来源，但这些讨论不能直接推出所有共同创造都应当上链。制度目标相同，技术路径仍可能不同；采用相同技术，也可能形成差异很大的权力结构。

利益相关者资本治理关注的是共同创造怎样获得持续的组织条件，贡献怎样经过确认进入适当的权益安排，以及长期投入怎样得到维护。技术的价值，应当放在这些关系中判断。如果一项系统增加了记录数量，却没有改善确认、履行与监督，新增记录未必形成治理上的进步。如果它降低了记账成本，却使参与者更难提出异议，也需要重新评价这种效率。

因此，制度技术的选择需要同时辨认三件事：共同事业需要解决什么协作困难，候选技术究竟能改变其中哪些条件，以及改变之后由谁承担成本、获得权限和承受风险。本章据此建立区块链的适用边界，并为后续讨论密码学、分布式账本和共识机制确定评价尺度。

一、多方协作何时需要共享账本

多方协作通常需要交换信息，但交换信息的需要与共享账本的需要有所区别。参与者阅读同一份说明、相互传递材料，主要解决信息到达和理解问题。共享账本则进一步要求，各方能够依据一组共同承认的记录，判断哪些事项已经发生、哪些承诺仍然有效，以及接下来允许实施什么行动。

这里的“共享”，首先指记录具有跨主体的共同用途，并不必然要求所有信息公开，也不要求每个参与者保存全部数据。“账本”也不限于金额的增减。它可以记录资源承诺、授权变更、履行确认和权益状态，但不同记录的意义应当分别定义，不能因为被放入同一个系统就取得相同效力。

共享账本需求首先来自状态之间的相互依赖。当一个主体的行动会改变另一个主体能够采取的行动，各方就需要知道正在依据哪个状态协作。某项资源是否已经被承诺，某项权限是否仍在有效期内，同一事项是否已经完成结算，都可能影响后续行动。若各方分别保存的记录长期不一致，合作就需要反复核对，甚至会在相互冲突的前提下继续执行。

这种依赖在涉及排他性状态时尤其突出。一项有限资源不能在同一适用范围内被当作两份可用资源，一项已经撤销的权限不能继续被视为有效权限。此时，系统需要共同处理互斥关系与先后顺序。单纯交换签署过的文件，可以证明各方分别表达过什么，却未必足以使所有参与者及时知道当前应当采用哪一种状态。

不过，并非所有记录都需要进入同一条全局顺序。互不影响的贡献材料可以分别收集，部分统计结果可以稍后汇总。只有当记录之间存在冲突、依赖或共同执行要求时，才需要确定相应范围内的顺序与确认规则。把原本可以独立处理的事项全部交给同一个确认过程，会扩大协调负担。

第二个条件是共同记录需要具有可核验性。不同主体可能愿意接受某个运营者负责日常服务，但希望能够独立检查重要记录，确认自己提交的材料是否被纳入，决定所用的版本是否正确，以及已有记录是否被悄然替换。共享账本在这里回应的是持续核验的需要，而不仅是集中查询的便利。

第三个条件涉及单方控制是否可以被接受。一个组织拥有统一的责任体系、适当的内部控制和可行的审计安排时，由该组织管理数据库可能已经足够。如果参与者不愿让任何一方独自决定共同状态，或者共同事业需要在某个运营者退出后继续保留可核验记录，就有必要研究更分散的控制安排。

不接受单方控制，仍然需要说明具体担忧。担心记录被事后修改，与担心有效请求被拒绝，所需机制不同；担心运营者失去服务能力，与担心多个运营者合谋，也不能采用完全相同的保障。技术选择应当明确准备承受哪些故障、限制哪些行为，以及在什么条件下保障可能失效。笼统的“不信任”不足以形成可执行的系统要求。

区块链更值得考虑的情形，是共同状态对多方具有持续影响，各方需要独立验证，且不愿将状态确认权完全交给单一主体，同时能够在明确的参与和故障假设下共同维护确认过程。这些条件形成采用区块链的理由，但尚未证明它优于其他方案。是否采用，还需要比较替代机制和长期成本。

共同维护也需要实际承担者。谁运行必要的设施，谁能够检查规则，谁负责软件更新，出现争议时谁组织处理，都需要有明确安排。如果全部节点、更新权限和服务入口始终由同一方实际控制，增加节点数量可能改善故障恢复，却不一定减少对该方的制度依赖。

多方之间还需要具有最低限度的共同规则。参与者可以对利益分配持有不同意见，但必须能够识别当前有效的规则、验证所依据的材料和决定程序。若各方尚未就“记录代表什么”形成可用约定，系统最多帮助保存不同主张，不能凭借共同记账把相互冲突的主张变成已经解决的关系。

在利益相关者资本治理中，这一点表现为贡献记录与权益状态之间的距离。共同保存一项贡献的申报，能够减少申报材料散失或被单方遗漏的风险；该贡献是否成立、是否已经获得报酬、是否满足进一步权益的取得条件，仍需要相应制度。共享账本应当准确表达这些阶段，而不应使“已提交”被读取为“已确权”。

本书据此提出“最小必要共同状态”的设计原则：只将确实需要跨主体共同确认、持续核验或约束后续行动的状态纳入共同维护。原始材料、专业判断过程和内部工作信息，可以依据各自用途保留在适当的系统中，并通过明确标识和证据关系与共同状态衔接。这是一项制度设计主张，其效果需要通过实际运行检验。

这个原则为共享划定了范围。决定共同维护什么，也是在决定哪些事项进入共同约束、哪些事项保留主体自主。范围过窄，关键承诺可能无法核验；范围过宽，参与者可能被迫暴露不必要的信息，并为无关事项承担确认成本。共享账本的边界，因而也是合作边界的一部分。

二、区块链、数据库与签名日志的比较

比较三种技术，首先需要避免把它们当作完全互斥的类别。数据库是存储、查询与管理数据的系统，可以集中部署，也可以分布式运行；签名日志是在记录及其验证方式上作出的安排，可以建立在数据库之上；区块链也需要存储系统，并通常结合签名、哈希和分布式协调机制。真正需要比较的是具体架构中的信任条件与控制方式。

数据库的优势在于成熟的数据管理能力。它能够支持权限控制、关联查询、并发处理以及一组操作的整体提交。在正确设计和运行的前提下，数据库完全能够维护资产账户，检查余额并约束重复支出。PostgreSQL的事务文档说明，一组操作可以作为整体成功或失败，未完成的中间状态不会作为已完成结果对其他事务呈现。这表明，受约束的状态转换并非区块链独有。PostgreSQL：事务 [1]

数据库架构的制度问题主要在于，谁掌握管理权限，以及其他参与者怎样监督这些权限。备份、权限分离、操作审计和外部核对，可以显著改善其可靠性与可追责性。评价数据库时，应当把这些现实可行的措施纳入基准，不能用一个缺少所有控制的数据库，与一个假定治理完善的区块链作比较。

签名日志进一步把记录与签名密钥联系起来，使核验者能够检查所签内容是否变化，以及签名是否与相应公钥匹配。若签署者身份和权限另有可靠依据，签名还能支持对责任主体的识别。日志可以为提交、批准、撤回和更新保留相互关联的证据，让记录接收者不必完全依赖提供查询界面的一方。

但对每条记录签名，不等于证明记录完整。日志管理者仍可能不收录某项提交、隐瞒部分记录，或者向不同接收者提供不同版本。哈希关联、只追加结构和外部保存的检查点，可以帮助发现某些修改；要发现不同接收者看到的记录相互矛盾，还需要适当的交叉核对或见证安排。每增加一种保障，都应当说明新增机制及其依赖。

RFC 9162描述的证书透明度协议，使用可审计日志以及包含性和一致性证明，支持检查某条记录是否进入日志、后续日志是否延续已有记录。该文档同时指出，日志向不同客户端提供不一致视图的问题，不能仅由其中的日志审计机制消除。这个技术参照说明，可核验日志具有独立价值，但其保障范围需要准确表达。RFC 9162：证书透明度协议，第1节 [2]

签名日志更直接地回答“某方留下了什么可验证的记录”。区块链则可以进一步支持多个维护者，依据共同验证规则，对互相竞争的状态变更形成可采用的顺序。这样，各方在规定条件下能够核验共同状态，而不只是在争议发生后比较各自持有的凭据。对于必须共同约束后续行动的资产状态，这种能力可能具有重要价值。

这种区别仍然具有条件。数据库可以使用分布式共识，签名日志也可以增加多方共同确认；区块链的关键控制权也可能集中于少数主体。名称本身不能证明独立性、安全性或治理质量。应当检查哪些参与者能够提出更新，谁能够拒绝更新，确认需要哪些条件，以及实际控制者是否具有足够独立性。

下表比较的是常见安排中的主要侧重点，具体系统仍需要单独核验。

比较问题	由明确运营者管理的数据库	带独立核验安排的签名日志	多方维护的区块链
主要处理什么	数据管理、查询和受约束的业务操作	已签记录的完整性、来源及历史核验	共同状态的验证、排序与持续更新
主要依赖谁	运营者及其权限、审计和责任安排	签署者、日志运营者及外部核验机制	验证参与者、协议假设及治理安排
如何处理相互冲突的请求	由数据库约束与业务规则处理	单纯签名留痕不足以形成共同裁决	依协议对有效请求排序并确认状态

比较问题	由明确运营者管理的数据库	带独立核验安排的签名日志	多方维护的区块链
如何约束事后改写	权限分离、审计、备份和外部证据	签名、关联证明及外部留存帮助发现变动	在安全假设内抵抗历史改写并允许独立验证
如何处理错误	授权更正并保留相应审计依据	追加更正、撤回或替代记录	按规则追加纠正状态或进入治理程序
怎样限制信息暴露	可细分数据访问权限	可限定披露内容及验证对象	取决于网络类型、数据布局和隐私机制

如果主要困难是管理者的记录缺乏可核验性，数据库结合签名、独立留存和定期审计，可能已经足以改善问题。如果主要困难是多个独立主体需要共同维护互斥状态，并限制任何一方单独改变确认结果，区块链才具有更明确的比较理由。若事实认定和分配规则本身尚未明确，三种技术都需要等待相应制度工作。

技术组合往往比单项替代更符合实际需求。高频操作和敏感原始材料可以在适当的数据库中管理；重要承诺和批准过程可以形成签名记录；确需跨主体共同确认的状态，可以进入共同账本。组合设计同时产生新的责任：系统之间的标识、版本和状态需要对应，不能在一个系统已经撤回后，另一个系统仍继续按旧状态执行。

比较时还需要追踪保障在哪里结束。把一份内部记录的摘要写入区块链，可以帮助核验后来取得的材料是否与摘要匹配，却不会使未公开的原始材料自动可得，也不会让内部系统的全部过程获得共同验证。所声称的保障，应当限于实际被证明的对象。

技术选择由此成为一项具体的制度判断：在哪些环节接受委托管理，在哪些环节要求独立留证，又在哪些环节需要共同限制状态变更。对这些环节作出清楚安排，比为整个组织选定一个统一的技术标签更有意义。

三、记录一致、事实真实与制度正当的区别

共享账本容易带来一种认识上的跳跃：既然许多参与者已经确认同一份记录，这份记录所描述的事情就应当真实，记录所依据的制度也应当合理。然而，记录一致、事实真实与制度正当分别回答不同问题。它们可以相互支持，却需要各自的判断依据。

记录一致关注的是，在特定规则、网络条件和确认阶段下，参与者是否采用相容的记录与状态。对尚未确认的请求，各方可能暂时具有不同认识；对已经达到相应确认条件的结果，则需要具备协议所承诺的稳定性。因而，一致性判断应当说明对象、范围和确认条件，不能将某个节点此刻显示的内容直接当作所有主体已经共同确认的事实。

这里的一致还应当区分形式相同与理解相同。各方保存相同字段，不代表对字段具有相同解释。“贡献已确认”究竟表示材料收讫、行为核实，还是权益取得条件已经满足，需要由明确的数据含义和制度规则说明。共同账本只有与共同可理解的语义衔接，才能成为协作依据。

事实真实关注记录与其所指对象的关系。对于完全由协议定义的链上状态，核验者可以依据可得数据和有效规则检查某项状态是否成立。对于现实中的交付、劳动、质量、身份和实际控制关系，则需要相应的外部证据。协议可以核验某个有权限的地址提交了确认，却不能仅凭这次提交判断它所描述的现实情况是否准确。

NIST的区块链技术概述把这一困难列为超出数字系统边界的问题：现实数据进入链上时，人或设备都可能提供错误信息，而区块链自身未必能够判断输入是否反映实际事件。这里的限制涉及外部信息进入数字系统的过程，并非通过增加记录副本就能消除。NIST IR 8202：第7.3节〔3〕

事实核验需要追溯信息的形成过程。谁观察或完成了有关事项，材料是否能够相互印证，确认者是否具有必要能力，是否存在影响判断的利益关系，以及反对材料怎样被处理，都决定一项记录值得获得何种程度的信赖。多个签名如果只是重复同一来源的错误信息，并没有形成同等数量的独立证据。

还应当区分事实与评价。某项投入是否发生，可以通过材料核实；它对长期共同成果贡献了多少，则可能涉及归因方法和反事实判断。后者即使经过多人讨论，也不一定具有唯一、精确的答案。制度可以形成可采用的评价结果，但应当保留评价口径、适用范围和复核条件，使共同采用不被误认为已经消除认识上的不确定性。

制度正当关注规则和决定凭什么要求相关主体接受。制定者是否具有相应权限，受影响利益是否得到适当考虑，程序是否提供必要参与和异议条件，权利与义务是否具有可以说明的理由，都属于这一层面的判断。签名齐全、计票准确和执行一致，可以支持程序核验，却不能单独回答规则本身应当如何评价。

这种正当性也不能完全压缩为一次赞成比例。表决资格可能排除了重要的受影响者，信息披露可能不足，代表可能超越委托范围，某些责任也可能不能由内部多数决定免除。判断需要回到权力来源、事项性质和适用边界。技术能够保存这些过程，但不能因为保存得完整，就替代对过程的实质审查。

三个层次可以分别发生错误。一组记录可以高度一致，却共同保存了不准确的事实；有关事实可以得到充分证实，却被用于缺少适当依据的分配安排；一项制度可以具有充分理由，但其执行记录仍可能遗漏、冲突或被错误计算。因此，不能用某一层的成功为另外两层作无条件担保。

判断层次	需要回答的问题	主要核验依据	出现问题后的处理方向
记录一致	各方是否依据有效规则采用相容状态	规则版本、记录、验证结果和确认条件	检查同步、执行和确认过程，按适用机制处理冲突
事实真实	记录所描述的事项是否有充分证据支持	原始材料、来源核查、独立证据和专业判断	补充调查、复核事实，并更新相关状态
制度正当	规则及决定为何有权约束相关主体	权限依据、参与程序、理由和权益边界	审查决定、提供救济，必要时修订规则

这一区分直接影响资本治理。贡献申报入账本，首先说明某项申报被记录；经有权程序核实，才可能形成可采用的贡献认定；是否进一步构成权益依据，还取决于具体规则和其他必要条件。即便权益凭证已经生成，也仍需检查其表达的是什么权利、对应谁的义务，以及履行基础是否存在。

同样，长期能力不能由记录的累积数量直接证明。持续形成的专业能力、合作可靠性和资源使用能力，需要从组织实际运行中评价。账本能够保存有关形成过程的证据，但记录存续与资本存续可能不同步。维护活动停止、关键关系瓦解或资源失去用途时，历史记录仍然完整，相关资本的现实条件却可能已经变化。

系统表达应当帮助用户保持这些区别。本书主张，对重要事项分别展示记录状态、事实核验状态和决定效力状态，并关联适用规则、责任主体和未完成条件。一个笼统的“已完成”标签，容易使申报、确认、批准和履行混为一谈。较准确的状态表达，可以减少技术界面本身制造的制度误解。

纠错机制也需要按层次安排。事实发生更正时，应当说明原判断为什么改变，并依有效程序调整由它支持的后续状态；规则需要修订时，应当说明新旧安排怎样衔接；账本发生技术冲突时，则先按照相应协议识别可以继续采用的状态。不同处理可以相互触发，但每一步都应当保留自己的权限和证据。

共同账本因而可以成为一种有边界的公共依据：它让已表达、已确认和已执行的事项更容易被共同检查，同时为事实调查和制度审查保留入口。这样的边界有助于建立可纠正的信赖，使参与者既能够依据记录行动，也能够有理由时挑战记录及其制度后果。

四、成本、效率、隐私与权力结构的权衡

制度技术的选择最终需要进入资源与权力的现实条件。技术具备某种能力，尚不意味着组织能够以可承担的代价长期获得这种能力。评价应当覆盖建设、运行、参与、纠错和退出，使最初的部署决定与后续责任相互对应。

成本首先包括设施、软件、安全维护和人员投入。分布式维护可能增加数据复制、通信和共同验证的工作，但具体负担取决于架构。不能把所有区块链的资源消耗等同于某一种共识机制，也不能将没有向使用者单独收费理解为没有成本。费用可能由组织预算、维护者投入或其他安排承担。

制度运行还包含核验事实、更新规则、处理异议和协调不同主体的成本。技术可以减少部分重复核对，却可能增加密钥管理、权限变更和跨系统状态衔接的工作。若只计算写入一条记录的费用，就容易遗漏维持这条记录能够被正确理解和有效使用所需的投入。

对长期共同创造而言，还应当观察成本由谁承担。组织减少的管理支出，可能转化为参与者的操作时间；自动执行节省的处理工作，可能伴随较高的错误纠正负担；维护要求可能使资源较少的主体逐步依赖大型服务商。成本评价需要同时说明总量和分布，否则总体节约也可能伴随参与条件恶化。

效率则需要明确终点。请求提交、进入记录、达到确认条件、形成有效决定和完成实际履行，属于不同阶段。每秒处理多少条请求，只能描述其中一部分。资本治理更需要知道，一项承诺从提出到获得可靠履行需要多久，重复核对是否减少，异常事项是否能够及时恢复，以及参与者是否因此获得更稳定的预期。

共享账本即使增加了单次确认的等待，也可能减少跨主体核对和争议处理的总时间；一个响应很快的系统，也可能把大量不确定性留给后续人工处理。这些都是需要验证的可能性。评价应当沿着完整流程测量，并把正常运行与故障、拥堵、异议出现时的表现分别观察。

隐私的权衡从信息用途开始。共同验证一项资格，不一定需要公开形成资格的全部材料；确认一项承诺，也不一定需要让所有维护者获得全部商业细节。制度设计应当先确定谁为了什么目的需要知道什么，再选择记录内容、披露范围和验证方式。

公开可验证与对所有人公开原始内容，是不同要求。系统可以研究分层访问、选择性披露以及链下材料与链上证明相结合的安排，但每种方式都有适用条件。验证者如果只能看到摘要，就需要知道摘要能够证明什么、原件由谁保存，以及争议发生时如何获得必要材料。保密不应使权利人失去检查自身处境的基本条件。

信息进入长期复制的记录后，其传播和保存范围也需要认真评估。NIST在适用性讨论中，将数据可见范围、交易历史以及原始记录难以直接删除列为选择因素；新增一条表示删除或更新的记录，并不等于原有内容已经从历史中消失。NIST IR 8202：第8.1节〔3〕

因此，敏感原始材料是否需要上链，应当在写入前作出判断。加密、去除姓名或仅保留摘要，都需要结合具体信息检查其保护效果，不能被当作一概充分的处理。对于长期合作，还应当明确保存期间、访问变更、材料交接和争议使用的责任，使核验需要与信息保护能够同时进入制度。

权力结构是另一项不能被性能指标代替的评价。谁决定参与资格，谁控制请求入口，谁可以调整规则，谁保管紧急权限，谁向系统输入外部事实，都可能影响参与者的实际处境。即便记录验证较为分散，这些其他环节仍可能集中。因此，权力分析应当贯穿从提交到履行的全过程。

还需要区分能够核验与有能力核验。理论上任何人都可以检查某项结果，如果实际需要承担远超普通参与者能力的设施、知识和时间成本，核验权就可能主要由少数服务机构行使。共治理需要为必要的独立检查提供资源、易于理解的说明和适当的代表安排，并使受托核验者能够被监督和替换。

限制权力与保留纠错能力之间也存在张力。紧急停止和升级权限可以帮助处理严重故障，却可能成为改变承诺的集中入口；完全缺少调整路径，则可能使已知错误继续产生后果。选择时应当具体说明这些权限的触发条件、使用范围、共同控制方式和事后审查，而非仅将其标记为“安全全能”。

长期依赖还要求预先考虑退出与迁移。参与者能否取得可理解、可核验的记录，新的维护者能否继续识别已有承诺，系统停止后由谁保存证据，以及迁移期间怎样处理未完成事项，都影响共同事业的持续性。更换技术设施不会自动解除既有义务，技术方案应当帮助责任延续。

本书主张，选择应当先确认不可缺少的条件，再比较可以权衡的表现。权限依据不清、必要隐私无法保护、关键履行无人负责，不能仅因速度较快或费用较低就被一个较高的综合分数抵消。只有满足基本制度条件的方案，才适合进一步比较效率、成本和长期适应能力。

比较还应当设置真实的替代方案。可以把具备必要权限管理、签名留证和外部核验的数据库方案作为基准，再检验区块链增加了哪些保障。各方案应当面对相近的业务范围、负载和故障情形，并说明对单方拒绝、错误输入、维护者退出及权限滥用的处理。新增技术是否值得，应当由可观察的改进支持。

对于尚不确定的方案，可以在明确范围内试行，事先确定需要观察的结果、承担责任的主体和停止条件。试行应当能够回答共同核对是否减少、事实错误能否纠正、独立验证是否可行，以及成本是否挤压长期投入。若已有方案足以满足要求，可以继续采用；若制度条件尚未形成，应当先完成相应制度工作。

面向未来，本书提出一个有待检验的判断：当跨组织协作和自动代理参与增加时，技术选择的重要单位可能越来越多地落在特定的承诺、授权和共同状态上。组织可以围绕这些关系采用不同验证与执行机制，而无须使所有活动进入同一套账本。这个方向是否能够降低协调成本、保持责任连续并改善参与条件，需要在后续实践中逐项检验。

制度技术的适用边界由此回到本书的起点。共同创造需要可以理解的规则、能够实现的权利和持续承担的责任；区块链在其中的作用，应当体现为某些共同状态更容易核验，某些单方变更更难发生，某些承诺的履行过程更可检查。下一篇将进入这些能力的技术构成，从密码学开始，逐步说明授权、完整性与共同确认怎样实现，以及各自的保障在何处结束。

本章注释

1. [SRC-068] PostgreSQL Global Development Group: **PostgreSQL：事务**。[原文或官方页面](#)

- 本章引证：PostgreSQL：事务。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：PostgreSQL：事务。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-069] RFC Editor: **Certificate Transparency Version 2.0 (RFC 9162)**。[原文或官方页面](#)

- 本章引证：RFC 9162：证书透明度协议，第1节。
 - 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：RFC 9162：证书透明度协议，第1节、RFC 9162：默克尔树与包含性证明。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
3. [SRC-078] 美国国家标准与技术研究院（NIST）：**Blockchain Technology Overview（NIST IR 8202）**。[原文或官方页面](#)
- 本章引证：NIST IR 8202：第7.3节；NIST IR 8202：第8.1节。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：NIST IR 8202：第7.3节、NIST IR 8202：第8.1节、NIST：区块链技术概述。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第二篇 共识与执行：制度如何进入技术系统

第七章 – 密码学：授权、完整性与可核验证据

共同创造需要可以依赖的承诺。参与者不仅需要知道一项决定写了什么，还需要能够检查正在阅读的内容是否被替换，提出行动要求的主体是否满足授权条件，以及一项已经作出的确认能否在日后接受核验。随着合作跨越组织和时间，这些要求不能完全依赖当事人的记忆或某个系统运营者的单方说明。

密码学为其中一部分要求提供了技术基础。哈希帮助检查记录是否与既定摘要对应，数字签名把特定消息与相应签名密钥联系起来，密钥管理则影响这种能力由谁掌握、在何种条件下使用和怎样延续。这些机制使某些判断能够通过计算重复核验，从而进入规则执行过程。

核验的力量来自判断对象的明确。密码学可以严格检查某种关系，却不会因此回答有关共同创造的全部问题。记录保持完整，仍然需要事实依据；签名通过验证，仍然需要理解签署内容和权限来源；组织能够操作账户，仍然需要说明对有关资产和权益负有什么责任。本章从这些衔接关系出发，解释密码学怎样成为制度技术的一部分。

一、哈希与记录完整性

一份制度文件在讨论、批准、传递和执行中，可能存在多个版本。参与者需要知道自己看到的文本，是否就是当时共同采用的文本。仅凭文件名、页数或一句“内容没有变化”，难以完成严格核验。哈希提供了一种对具体数据进行简洁标识和比对的方法。

本节所讨论的密码学哈希，是按照确定的算法，把输入数据映射为相应长度的摘要。同一种算法处理完全相同的数据，会得到相同结果；设计良好的密码学哈希使寻找特定类型的相同摘要关系在计算上十分困难。NIST的安全哈希标准将消息摘要的用途表述为检测消息自摘要生成以后是否发生变化。NIST FIPS 180-4：安全哈希标准〔1〕

可以用一个简短的表达理解核验过程：既定摘要为“哈希（原记录）”，收到材料后重新计算“哈希（待核记录）”，再比较结果。摘要不同，说明在采用相同算法的前提下，两份输入数据不同。摘要相同，则在算法安全性等条件成立时，为两份数据一致提供很强的技术依据。

这里需要保留“在安全条件下”的限定。摘要的取值范围有限，能够输入的数据远多于可能的摘要，因此不同数据得到同一摘要的情况在数学上存在。密码学追求的是使攻击者难以实际找到可以利用的碰撞，或为既定记录构造摘要相同的替代内容。把哈希称为绝对唯一的数字指纹，会掩盖它依赖算法及其安全条件的事实。

记录完整性也有明确的粒度。哈希处理的是实际输入的数据。相同的文字在编码、空格、附件或文件元信息不同的情况下，可能形成不同摘要；两份语义相近的文件，也不会因此具有相同摘要。系统应当明确核验的是原始文件、规范化文本，还是按约定字段组成的结构化记录。

这种输入范围的确定具有制度意义。如果只对正文计算摘要，附件中的权利限制就可能没有进入核验范围；如果只纳入金额而遗漏计量单位和适用期间，就可能无法绑定一项承诺的完整含义。因此，需要先说明参与者实际认可什么，再保证这些内容被准确纳入计算。字段定义和版本规则在这里成为制度与技术之间的接口。

哈希核验还需要一个可信的比较起点。如果攻击者能够同时替换文件和旁边显示的摘要，新的二者仍然能够相互匹配。摘要可以通过独立保存、签名确认或纳入共同账本等方式取得更可靠的参照位置，但保障取决于这些安排是否实际有效。哈希本身不会决定哪一个摘要才是各方应当采用的基准。

这也说明哈希不能独立证明记录的作者和时间。任何获得文件的人都可以计算摘要；一个由提交者自行填写的时间，也不会因为与摘要放在一起就变成可靠时间证据。若需要说明某项材料在特定时点已经存在，必须进一步检查时间来源、记录过程及其可信条件。链上记录也应当按照相应协议解释其顺序与时间含义。

多个记录可以通过哈希形成关联。后一项记录纳入前一项记录的摘要，能够使前后内容相互约束；修改前项后，如果不相应更新后续关联，就会出现不匹配。若攻击者能够重新计算全部关联并替换核验起点，仅有这种结构仍不足以阻止重写。历史难以被单方改动，还需要额外的确认和保存机制。

当需要核验大量记录时，可以把摘要按树形结构逐层组合，形成一个代表相应记录集合的根摘要。默克尔树利用这种方式，使核验者可以根据较少的关联数据，检查某条记录是否被包含在特定根摘要所对应的集合中。根摘要仍需要可靠来源，证明也需要按照明确的树形结构和编码规则核验。RFC 9162：默克尔树与包含性证明〔2〕

包含性证明的结论应当停留在它实际覆盖的范围。证明某条贡献申报进入了某个记录集合，不等于证明全部符合条件的申报都被纳入，也不等于证明这条申报已经通过事实审查。记录是否遗漏，需要结合提交凭据、受理规则和其他核对过程判断。数学上可以核验的包含关系，不能替代制度上应当完整覆盖的范围。

哈希同样不承担加密的功能。摘要通常不能作为还原原文件的工具，但对于候选内容很少、容易猜测的数据，外部观察者可能通过逐一计算候选摘要来比较。因而，只保存摘要不能被普遍理解为已经匿名化或充分保密。公开摘要之前，仍需判断原始信息的可猜测性和关联风险。

在利益相关者资本治理中，哈希适合帮助固定有关判断所依据的材料版本。贡献记录、评价口径、授权文件和批准结果，可以通过明确关联，使核验者知道某次决定究竟使用了哪些材料。形成这种关联的目的，是让后续审查能够回到当时的依据，并识别材料与规则的变化。

材料本身还需要能够取得。保存一份文件的摘要，并没有保存文件的完整内容；原件丢失后，摘要通常无法帮助重建它。组织需要同时安排原始材料的保管、必要披露和长期可读性。证据能被核验与证据能被找到，必须在实际运行中相互配合。

本书据此将哈希的制度作用理解为：为共同采用的具体记录建立可重复检查的对应关系。这种关系有助于约束材料替换和版本混用，却仍需与事实审查、有效批准和证据保存衔接。哈希使“是不是同一份记录”更容易回答，也促使制度设计者更准确地说明需要固定的究竟是什么。

二、数字签名与资产转移授权

记录完整之后，行动要求还需要找到适当来源。系统收到一项资产转移请求时，需要核验它是否满足相应的授权条件，并防止传递过程中关键内容被替换。数字签名为这种核验提供了基础机制。

在常见的公钥签名体系中，私钥用于产生签名，公钥用于验证签名与特定消息的关系。验证者不需要取得私钥，就可以按相应算法检查结果。数字签名也不宜被笼统解释为“用私钥加密、再用公钥解密”；签名算法具有自己的生成和验证过程，其主要用途与信息保密不同。

NIST的数字签名标准将检测未经授权的数据修改、支持签署者认证和提供有关签署行为的证据列为签名的用途。本书进一步强调，其中对现实签署者的识别，需要公钥与主体之间具有可靠的关联；单独的数学验证，首先确认的是消息、签名和公钥之间的关系。NIST FIPS 186-5：数字签名标准〔3〕

对于资产转移，协议需要把这种签名关系与当前状态中的控制条件联系起来。当前状态可以要求某一密钥的签名，也可以要求多个签名或其他验证条件。系统据此检查提出转移的请求，是否满足当前有效的技术授权规则。这里的授权，是协议对可接受行动所规定的条件；其法律意义还需要另行衔接。

资产并不因为签署交易而作为一份秘密文件从私钥中传出。私钥使有关主体能够满足某些状态转换条件；在转移被相应系统接受之后，旧状态所允许的支出被消耗或调整，新状态开始规定后续控制条件。比特币的交易文档以未花费交易输出及其支出条件说明了这一过程：请求引用已有输出，并提交满足其条件的数据，再形成新的输出。Bitcoin开发文档：交易〔4〕

签名需要绑定适当的行动内容。转移对象、数量、接收条件以及其他关键参数，如果没有进入签名实际覆盖的范围，就不能期待该签名阻止这些内容发生变化。不同协议和签名模式覆盖的字段可能不同，不能从“已经签名”推定整项业务的所有条件都受到相同保护。

授权的使用环境也需要被绑定。同一份签署内容，如果在不同系统、不同合约或不同版本中具有不同用途，就可能出现跨环境使用的问题。所谓签名域的区分，就是让签署内容明确联系到预定使用环境，使验证者能够拒绝不属于该环境的授权。

EIP-712对结构化数据签名和签名域作出了规范安排，允许将链标识、验证合约和版本等信息纳入相应结构。该规范同时明确，它本身不提供完整的重放保护。一次授权是否可以再次执行，仍然需要应用处理。EIP-712：结构化数据签名与重放保护边界〔5〕

重放问题揭示了签名与共同状态之间的重要关系。一个有效签名可以被复制，任何获得它的人也可能再次提交。若一项授权只允许使用一次，系统就需要记录它是否已经使用，并检查相应序号、唯一标识或其他防重复条件。签名能够约束消息内容，防止重复执行则需要消息与状态配合。

签名者也可以对相互冲突的请求分别生成有效签名。密码学不会因为某次签署已经发生，就阻止同一密钥再签另一条消息。当两个请求试图消耗同一资源时，需要账本的有效性规则和确认过程决定哪些请求可以进入共同状态。因此，签名是资产转移授权的重要组成部分，转移的排他性还依赖后续机制。

需要进一步区分签署、提交、接受和履行。签名生成后，请求可能尚未提交；提交后，可能因状态变化或条件不足被拒绝；链上接受后，现实中的交付义务也可能仍待履行。系统应当保留这些阶段，避免把一个签名成功提示当作资产和责任关系已经全部完成变动。

对于自动执行而言，签署者理解的内容与机器实际验证的内容应当一致。界面显示“确认参与”，实际消息却包含广泛的资产操作权限，就会使人类理解与技术后果发生严重错位。结构化显示可以改善可读性，但还需要保证显示来源、解析过程和实际签署数据可靠对应。

资本治理中的签名因此需要具有明确用途。确认贡献材料、批准权益分配、授权资源支出和同意规则变更，属于不同的行为。一项确认不能仅因采用了同一把密钥，就被扩张为对其他事项的概括同意。制度需要把签名角色、内容范围和后续效果分别定义，并由系统执行相应限制。

本书主张，将重要签署设计成可以理解的具体承诺表达：参与者能够知道自己以何种角色，对哪个版本的什么事项作出确认，授权适用多久，以及将触发哪些行动。签名把这种表达转化为可核验的数据关系；表达的清楚程度，决定密码学能够为制度保存多完整的依据。

三、密钥保管、恢复与组织控制

数字签名把一部分行动能力集中到密钥及其使用条件上。能够调用签名能力的人，可能无需修改账本规则，就能提出满足技术要求的请求。因此，密钥保管直接影响组织实际控制，必须纳入权责安排。

组织首先需要区分密钥、密钥使用者与权限主体。密钥是一种技术凭据；使用者可能是工作人员、托管机构或自动执行服务；权限主体则可能是组织本身或其他有权主体。三者可以关联，却不能直接合并。工作人员能够操作某个账户，不意味着账户中的资源因此成为其个人资产。

这种关联需要从密钥建立时开始。生成过程是否可靠，初始使用权限怎样授予，公钥通过什么方式与组织及角色对应，都影响后续核验。如果组织只是接收了一份由他人产生、可能仍被他人保留的私钥，就不能仅凭完成交接推定自己已经获得独立控制。

密钥管理还具有持续的生命周期。投入使用、权限调整、停止使用、泄露处置和历史核验，都需要相应安排。NIST的密钥管理建议将不同密钥的保护要求、管理功能和相关信息管理纳入整体框架。这个视角有助于理解：密钥是否安全，取决于它在整个使用期间怎样被产生、调用和维护。NIST SP 800-57 Part 1 Rev. 5：密钥管理建议〔6〕

保管方式需要结合密钥用途选择。日常低额度操作与重大资产处置可以采用不同的调用条件；频繁在线的服务与长期少用的控制权限，也不必承担完全相同的暴露范围。专用设备和受保护的运行环境能够支持相应限制，但组织仍需检查谁能够触发签名、改变设备策略或取得恢复材料。

多人共同管理可以减少对单一持有者的依赖，但需要明确技术形式。多重签名通常由多个独立密钥分别签署，再由账户或协议检查是否满足数量及组合条件。门限签名则可以通过分散的密钥份额协同完成签名运算，在相应安全假设下，无须把完整私钥集中重建后再签署。NIST：多方门限密码学〔7〕

两种方式都可以支持共同控制，但它们呈现的证据可能不同。有些门限方案对外只表现为一个公钥下的普通有效签名，核验者不能仅凭最终签名识别具体由哪些成员参与。若组织需要逐人追责，还应当保存适当的参与和批准记录。对外验证简洁与对内责任清晰，需要分别设计。

多人管理的效果还取决于实际独立性。多个密钥如果由同一人持有，或者多个份额始终受同一管理入口支配，名义上的人数并没有形成相应制衡。另一方面，要求所有成员随时到场，可能使人员变动和暂时失联阻断正常履行。共同控制需要在防止单方滥用与保持必要行动能力之间选择明确条件。

恢复机制尤其需要区分对象。恢复丢失设备中的密钥，可以依赖此前建立的适当恢复材料；在支持权限变更的账户中，也可能通过预先设置的恢复程序，把控制权限转交给新密钥。这两种机制不同，后一种并不要求找回原来的秘密。若密钥材料已经全部丢失，账户又没有可用的替代控制路径，通常无法仅凭真实身份从公钥反推出私钥。

恢复还不能被当作所有签名密钥一律复制备份的理由。备份是否适合，应当结合用途、归责要求和暴露后果判断。复制完整的签名秘密，会增加能够使用该身份生成签名的入口；采用分散保管或替代授权机制，也会引入新的参与者与依赖。组织应当明确所选择的路径及其责任。

因此，恢复权本身是一种重要控制权。能够替换签名者、降低签名门槛或重设账户规则的主体，可能绕过日常签署安排取得实际控制。即使正常操作要求多人批准，如果恢复入口由一个不受约束的管理者掌握，共同控制仍可能被架空。

本书主张，将组织的签署相关权限分别表达，并检查它们是否存在未经说明的相互替代。

权限	可以完成的事项	需要明确的制度边界
业务批准权	判断一项具体行动是否应当实施	事项范围、额度、依据和利益冲突处理
签名执行权	对符合条件的具体消息生成签名	消息范围、调用条件和批准记录的对应关系
恢复与更换权 WISERUNION	在既定条件下恢复使用或更换控制密钥	触发依据、参与门槛、异议和生效程序

权限	可以完成的事项	需要明确的制度边界
策略修改权	调整签名门槛、角色或执行限制	有效修改权限、影响说明和过渡安排

这些权限可以由不同主体承担，也可以在明确范围内结合。但任何结合都应当能够解释，不能由一个技术默认设置悄然决定。紧急处理可能需要更快的行动路径，延迟生效可能为异议提供时间；选择何种安排，需要结合实际风险，而不能预设同一种机制适合所有组织。

人员更替时，组织应当更新技术权限，并保存权限交接的依据。收回设备不能证明旧秘密没有副本，内部撤职也不会自动使所有系统拒绝旧密钥。系统需要按其支持的机制移除旧授权、调整验证条件或迁移有关控制，并核对尚未执行的签名请求怎样处理。

如果发生泄露，技术处置与责任调查应当并行。限制后续调用、在可行范围内变更控制和保全有关记录，有助于减少进一步影响；某个请求是否确由有权人员作出，则仍需要检查设备、流程和其他证据。密钥后来失效，也不意味着此前所有签名自动失效，历史行为需要结合当时的权限和证据评价。

长期资本关系还可能超出某种算法和设备的适用期间。NIST于2024年发布的FIPS 204规定了面向后量子安全目标的ML-DSA签名算法，但一种算法标准的存在，并不意味着现有账本已经支持迁移，也不代表安全获得永久保证。NIST FIPS 204：基于模块格的数字签名标准〔8〕

对组织而言，需要保留的是可审查的更新能力：识别正在使用的算法和密钥，说明替换由谁批准，使新旧控制关系能够核对，并维护历史证据的可验证性。延续共同承诺，要求技术凭据可以在有依据的程序中更替，同时使既有权利和责任得到连续处理。

四、有效签名与合法授权的边界

数字签名能够提供重要证据，但证据需要进入具体关系才产生相应意义。本节所说的有效签名，首先指按照指定算法对特定消息验证通过；合法授权则涉及现实主体是否有权就该事项作出相应决定。两者之间需要身份、权限和程序等条件衔接。

可以从四个层次审查一项签署行为：签名是否通过密码学验证，消息是否满足系统当前的接受条件，签署是否具有适当的组织与法律依据，以及有关行为是否已经产生所声称的权利变动。前一层的核验结果可以支持后一层判断，但不能替代后一层所需的材料。

层次	主要判断	不能单凭该结果推出的结论
密码学验证	消息、签名与公钥是否满足算法验证关系	必然由某个现实主体本人自愿签署
协议授权检查	是否满足当前密钥权限、状态及使用条件	该权限在现实关系中必然合法、完整
组织与法律审查	身份、代表权限、意思表示及程序是否具有相应依据	相关事项必然已完成全部生效与履行条件
权利变动核验	所主张的权利是否依适用条件发生变动	凭证所表达的全部义务已经履行

身份关联是第一项重要衔接。公钥可以通过登记、证书、合同安排或其他可靠过程与主体联系，但应当检查关联的来源、范围和有效状态。地址被标注为某个组织，只是提供了一个说明；说明是否准确，需要相应依据。一个主体也可能使用多把密钥，一把组织密钥也可能由多个受托者共同操作。

代表权限是另一项独立条件。工作人员可以具有技术操作资格，却只被允许在特定范围内行动。组织内部的批准、代理或委托关系，需要说明适用事项、期限和必要前置程序。超过内部权限的行为对不同当事人产生何种后果，还需结合适用法律和具体事实判断，不能由系统单一标签代替。

签署内容与意思表示之间同样需要证据联系。设备被盗用、界面误导、自动服务越过委托范围，以及实际签署内容与批准内容不一致，都可能使数学上通过验证的签名面临进一步审查。密码学验证不负责判断签署者是否理解、是否受到不当影响或是否具有相应行为资格。

这并不削弱数字签名的证据价值。它意味着签名证据应当与使用过程共同理解。签署前呈现了什么内容，采用何种身份确认，批准记录对应哪个版本，密钥当时由谁保管，以及异常何时被发现，都可能影响对行为的归责。“不可否认性”所表达的技术目标，不应被解释为任何情况下都不允许提出反证。

数字签名与法律上的电子签名也不完全同义。数字签名是一类密码学技术；电子签名制度可以采用更广的技术中立框架。联合国国际贸易法委员会2001年《电子签名示范法》以技术可靠性、技术中立和功能等同等原则，为各国立法提供参照。它是示范性文本，具体法律效果仍取决于适用法及相应条件，不能把某项密码学标准直接当作普遍生效的法律规则。UNCITRAL：电子签名示范法〔9〕

对于现实资产和组织权益，这些区别尤其重要。一个账户完成有效签署，可以改变链上凭证的控制状态；所映射的权利是否随之变动，还要看凭证表达、有效约定和适用程序。链上原生资产也不能仅凭协议接受某次交易，就对密钥盗用、受托操作或归属争议作出最终法律判断。

在利益相关者资本治理中，贡献确认、资本形成和权益授予应当分别保留依据。一名审核者签署贡献记录，可以证明其对特定材料作出了相应确认；这项确认是否足以产生收益请求权或治理权，需要回到已经有效采用的制度。审核者的签名能力不能把尚未取得的授予权限一并创造出来。

合法授权还具有时间边界。批准时具备的权限，在实际执行时可能已被调整；预先签署的请求，也可能在签署者不再具有相应角色后才被提交。制度需要确定哪些条件以签署时为准，哪些还需在执行时重新检查，并使撤回、到期和已发生效力的处理相互协调。技术能够执行的范围，应当与这些约定对应。

自动代理的参与会使这种时间与范围的区分更加重要。组织可以将一定操作能力交给软件或人工智能代理，但代理生成了有效签名，只能说明有关技术条件得到满足。它实际可以作出哪些承诺，应当来自有效委托，并受到金额、事项、期限及必要复核条件的约束。

本书提出一个面向未来的制度设计方向：将可核验授权从一次性的同意记录，扩展为能够表达委托来源、行动范围、有效期间和撤销状态的持续关系。技术可以帮助检查某次行动是否仍处于委托范围内，人类或组织仍需要对委托的设立、修改和责任承担提供依据。这是一项待检验的设计主张，其价值应当通过越权能否减少、履行能否持续和责任能否追溯来评价。

发生争议时，核验过程应当允许不同结论并存于各自层次：某个签名可以继续通过数学验证，而该行为是否具有适当授权仍待审查；链上状态可以已经改变，而有关责任和救济仍在处理。清楚表达这种状态，有助于各方知道哪些事实已经确定，哪些问题仍需有权程序判断。

由此，密码学为制度提供了一组可重复检查的基础关系：记录是否与既定摘要对应，消息是否满足签名验证，以及行动是否符合已经表达的技术权限。组织和法律制度则进一步说明这些关系涉及谁、依据什么以及产生何种后果。两者衔接得越清楚，技术执行越有可能准确承载共同承诺。

至此，本书已经说明如何固定具体记录、验证签名并安排签名能力的使用。但多个分别有效的请求，仍可能相互冲突；不同参与者也可能暂时看到不同状态。下一章将转向分布式账本，讨论这些请求如何进入共同记录，以及交易验证、顺序与最终性怎样支持可以共同采用的状态。

定稿补强：密码敏捷性、恢复权与法律授权

长期制度不能假定同一套密码算法、参数、密钥和验证软件永久有效。系统应维护密码资产清单，记录算法与参数版本、密钥用途、生成和轮换时间、签名对象、验证环境及退役条件。发生算法风险、密钥泄露或标准迁移时，应设置新旧算法的双轨验证期，保存历史验证所需的版本和时间证据，并明确哪些记录需要重新签署、重新锚定或仅保留原始证明。

多签与门限方案只有在控制要素真正独立时才形成多方约束。多个密钥若由同一人员、设备、云账户或恢复渠道控制，名义上的多方控制仍可能是单点。恢复机制需要写明保管域、阈值变更、替补人员、等待期、见证、异常通知和恢复后的旧权限撤销；恢复权本身不能成为不受监督的超级权限。

密码学上的签名有效，只证明某个密钥对特定数据产生了可验证动作。制度与法律还要分别检查身份、代表权、意思表示、签署范围、撤销状态、时间、保存方式和必要形式。高影响事项应把“签名验证通过”“组织授权有效”“法律形式满足”记录为三个结论，任何一个结论都不能代替另外两个。

本章注释

1. [SRC-006] 美国国家标准与技术研究院（NIST）：NIST FIPS 180-4：安全哈希标准。[原文或官方页面](#)

- 本章引证：NIST FIPS 180-4：安全哈希标准。
- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：NIST FIPS 180-4：安全哈希标准。
- 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-069] RFC Editor：Certificate Transparency Version 2.0（RFC 9162）。[原文或官方页面](#)

- 本章引证：RFC 9162：默克尔树与包含性证明。
- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：RFC 9162：证书透明度协议，第1节、RFC 9162：默克尔树与包含性证明。

- 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
3. [SRC-007] 美国国家标准与技术研究院（NIST）：NIST FIPS 186-5：数字签名标准。[原文或官方页面](#)
- 本章引证：NIST FIPS 186-5：数字签名标准。
 - 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：NIST FIPS 186-5：数字签名标准。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
4. [SRC-014] Bitcoin Project：Bitcoin开发文档：交易。[原文或官方页面](#)
- 本章引证：Bitcoin开发文档：交易。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：比特币开发文档：交易、Bitcoin开发文档：交易。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
5. [SRC-026] Ethereum Improvement Proposals：EIP-712：结构化数据签名与重放保护边界。[原文或官方页面](#)
- 本章引证：EIP-712：结构化数据签名与重放保护边界。
 - 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：EIP-712：结构化数据签名与重放保护边界。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
6. [SRC-010] 美国国家标准与技术研究院（NIST）：NIST SP 800-57 Part 1 Rev. 5：密钥管理建议。[原文或官方页面](#)
- 本章引证：NIST SP 800-57 Part 1 Rev. 5：密钥管理建议。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：NIST SP 800-57 Part 1 Rev. 5：密钥管理建议。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
7. [SRC-005] 美国国家标准与技术研究院（NIST）：多方门限密码学。[原文或官方页面](#)
- 本章引证：NIST：多方门限密码学。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：NIST：多方门限密码学。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
8. [SRC-008] 美国国家标准与技术研究院（NIST）：NIST FIPS 204：基于模块格的数字签名标准。[原文或官方页面](#)
- 本章引证：NIST FIPS 204：基于模块格的数字签名标准。
 - 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：NIST FIPS 204：基于模块格的数字签名标准。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
9. [SRC-071] 联合国国际贸易法委员会（UNCITRAL）：电子签名示范法。[原文或官方页面](#)
- 本章引证：UNCITRAL：电子签名示范法。

- 支持范围：用于确认有关法律文本、示范规则或数字资产私法原则对所引事项的正式表达，本书引用主题包括：UNCITRAL：电子签名示范法。
- 使用边界：该文本的适用法域、效力层级和个案适用仍需专业法律判断；引用不构成法律意见。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第八章 – 分布式账本：共同状态如何形成

一项请求具有有效签名，还不足以成为各方可以共同采用的结果。同一主体可以签署相互冲突的请求，不同参与者也可能先后收到不同消息。如果每个人都仅依据自己最先看到的内容继续行动，共同资源就可能被重复使用，已经调整的权限也可能在另一处继续生效。

分布式账本需要处理的，是这些分别到达、可能冲突的请求如何进入一组相容的状态。它既要判断什么变化可以发生，也要确定相互依赖的变化按什么顺序发生，并使遵守规则的参与者能够在明确条件下据此协作。记录分布在多个地方，只是这一过程的组织形式；共同状态的形成，还需要有效性规则、确认机制和可核验的历史依据。

对于利益相关者资本治理，共同状态可以涉及资源是否可用、承诺是否已经履行、权限是否仍然有效，以及某项制度程序进行到哪一步。它为行动提供共同参照，但其含义取决于事先明确的制度。本章沿着交易、验证、顺序和故障处理展开，说明这种共同参照如何建立，以及它在什么条件下值得依赖。

一、交易、账本与状态转换

区块链中的“交易”，通常指按照协议表达、请求改变系统状态的操作。它可以涉及资产转移，也可以涉及权限调整、程序调用和其他被系统支持的变化。这个术语并不表示每次操作都对应现实中的买卖，也不能单凭它被称为交易，就推定有关法律关系已经成立。

“状态”则是在某一确定位置上，系统根据有效规则和已采用记录所维护的结果。账户余额、尚未使用的资产输出、有效权限和已经登记的承诺，都可以成为状态的一部分。状态回答的是：在当前认可的依据下，系统接下来允许什么、拒绝什么，以及能够向参与者呈现什么。

交易和状态由转换规则联系起来。对通常的交易处理，可以概括为：既定状态，加上满足条件的交易，按照确定规则，得到后续状态。这里的规则既包括权限检查，也包括资源约束和具体计算。若还使用区块高度、协议时间等环境信息，这些输入也需要按照协议取得共同可采用的值。

这种表达的关键在于可重复核验。参与者从相同的有效起点出发，依据相同规则处理相同顺序的输入，应当得到相同结果。若程序运行时随意读取本地时钟、各自访问的外部网页或未经共同确定的随机结果，即使交易相同，也可能算出不同状态。外部信息需要通过相应机制成为明确输入，才能进入共同计算。

账本保存的是已采用的交易及其相应历史关系；当前状态则是根据这些记录和规则形成的结果。二者密切联系，但不需要以完全相同的形式保存。系统可以使用便于查询的状态数据，也可以通过检查点或其他机制支持同步。采用这些方式时，需要说明它们如何与已确认的历史对应，以及核验者另外接受了哪些信任条件。

因此，账本中的一项历史记录不等于当前仍然有效的权限。一项授权已经被后续记录撤销，其原始记录仍然可以存在；一项资源已经被使用，过去的取得记录也不会因此消失。共同状态通过解释历史中的变更，区分曾经成立与现在可用。保留历史，服务于追溯；更新状态，服务于当前行动。

不同系统可以采用不同的状态表达。未花费交易输出模型，把可支配价值表达为尚未被使用的输出及其支出条件。账户模型则维护账户余额、序号和其他状态。以太坊的交易文档说明，交易包含发送方、接收方、数额及账户序号等内容，用于发起状态更新。Ethereum开发文档：交易〔1〕

这些表达方式改变了核验过程，但共同要求仍然清楚：识别正在使用什么，检查请求者是否满足条件，并在采用结果后更新剩余的行动空间。利益相关者资本治理可以借鉴这种表达纪律，把承诺、确认、权益和履行的变化分别记录，避免用一个持续增加的总分替代全部关系。

区块链还把若干交易组织为区块，并通过协议规定的关联方式形成历史。在一条采用顺序执行语义的链上，区块之间与区块内部的交易顺序，共同影响状态演进。并行计算可以提高执行效率，但参与者仍需取得与协议要求一致的结果；计算可以分工，结果不能由各节点自行解释。

共同状态也不要求所有参与者在每一瞬间都拥有完全相同的数据。消息传递需要时间，节点承担的角色也可能不同。某些节点保存并检查较完整的数据，另一些使用证明或服务接口取得结果。判断一种查询结果是否可靠，需要知道它依据哪条链、哪个区块或检查点，以及查询者实际完成了哪些验证。

这使“共同”具有一个重要含义：各方具备识别相容依据和核验结果的路径，而不是所有屏幕必须同时刷新。对于尚未达到共同确认条件的变化，系统可以显示观察结果，但应当保留它的暂时性。只有这样，参与者才不会把传播速度上的差异误认为不同的有效权利。

在资本治理中，状态设计还需要保持语义上的分工。贡献已经申报、事实已经核实、权益已经批准与义务已经履行，是不同状态。它们可能依次发生，也可能需要补充材料或进入争议处理。状态转换规则应当表达这些条件，而不能只因前一步完成，就自动赋予后一步的全部后果。

本书主张，共同账本应当保留从当前结果返回其依据的路径。参与者看到一项权益状态时，应当能够在适当权限内查明它来自哪次决定、采用哪个规则版本、依赖哪些确认，以及后来是否发生调整。这种可追溯关系，使共同状态成为可以解释的制度结果。

二、交易有效性与重复支出的拒绝

共同状态的建立，需要先确定什么交易可以被采用。有效性判断是相对于特定规则和状态作出的。签名通过验证，只满足其中一类要求；请求还可能因为引用的资源不存在、权限已经失效或使用条件尚未达到而被拒绝。

有效性检查通常涉及数据是否符合格式、授权是否满足要求、引用对象是否存在、资源是否足够，以及状态转换是否遵守相关约束。这些检查应当在实际执行所依据的状态上完成。一个请求在准备时看起来可以执行，到了处理时，其前置状态可能已经被其他交易改变。

这一区别有助于理解交易池的作用。节点可以暂存准备传播或等待纳入的请求，并根据自身策略进行筛选。进入某个节点的交易池，不等于整个网络已经接受，也不等于请求最终会被纳入账本。节点的转发和暂存策略，与决定区块能否被接受的共同规则，不宜混为一谈。

重复支出涉及同一资源被相互冲突的请求再次使用。分布式网络允许消息复制和多次传播，因此拒绝重复支出的关键，是在共同采用的状态中，使已经消耗的支出条件不能再被当作未消耗条件。原交易数据可以继续存在，原有使用机会则需要发生明确变化。

在未花费交易输出模型中，一笔普通支出引用已有的未花费输出；被采用后，这些输出退出当前可支出集合，并形成新的输出。同一输出不能在同一条有效历史中被成功消耗两次。比特币开发文档据此说明，支出必须使用尚未花费的输出，重复引用已经被消耗的输出不能构成有效付款。Bitcoin开发文档：区块链与交易输出〔2〕

在账户模型中，余额约束与序号等机制共同限制请求。账户序号使某个位置上的一次交易被采用后，另一条试图使用同一序号的冲突请求不能继续按原条件执行；余额和其他业务规则则约束可用资源。序号不会判断现实中的两次申报是否描述同一件事，也不能替代资产和权限的具体检查。

重复传播与重复支出应当分别处理。网络再次收到完全相同的交易，可以识别为已经见过或处理过的请求，不需要因此再次改变状态。另一个签名、格式均正确的请求，如果竞争使用同一份资源，则需要依据共同状态拒绝其中不能继续成立的部分。后者具有实质性的冲突，不能仅用消息去重解决。

还需要区分技术重复与业务重复。两条不同交易可以具有不同序号和标识，却指向同一项现实贡献或同一笔应付义务。只要协议没有表达这种业务关联，二者可能都通过技术验证。要防止重复确认或重复支付，组织还需要建立适当的事项标识、责任关联和审核规则。

这一点对利益相关者资本治理尤其重要。同一项投入可能被不同渠道收集，也可能由多个协作者分别描述。共同账本可以约束一个确定标识下的重复处理，但哪个标识代表同一事项、多人贡献如何分别认定，仍需要事实与制度工作。拒绝重复支出不能被扩张为系统已经自动识别全部重复价值申报。

有效性判断也不是“获得足够支持即可通过”。在既定协议下，遵守规则的验证者需要独立拒绝无效交易和区块。即使某个提议者拥有较强的排序能力，也不能仅凭这种能力，使缺少必要授权或违反资源约束的交易成为这些验证者认可的有效交易。参与者改用另一套规则，则属于规则和网络边界发生变化的问题。

多个交易分别通过初步检查，也不意味着它们可以无条件组合。执行前项后，后项需要面对更新后的状态。竞争同一资源的请求，其有效性可能随顺序改变；相互独立的请求则可能允许并行处理。系统需要保存这种依赖关系，使批量处理不会绕过逐步更新后的约束。

交易被有效纳入与预期业务执行成功，也需要区别。某些支持程序调用的系统，允许一笔符合纳入条件的交易在运行时产生失败结果：预期的合约状态修改被撤销，但费用、序号等仍按协议处理。因此，账本可以可靠记录一次失败的调用。核验者还应当检查执行结果，不能只查到交易存在就认定支付、登记或分配已经成功。Ethereum开发文档：Gas与执行费用〔3〕

对参与者而言，拒绝应当尽可能形成可以理解的反馈。授权不足、资源已用、请求到期、程序执行失败与暂时未被纳入，具有不同含义，也对应不同后续动作。准确呈现原因，有助于区分需要重新提交、等待同步、补充批准，还是进入事实争议处理。

有效性规则由此限定了共同状态可以怎样变化。它使已经表达的排他条件能够持续约束后续行动，却还没有决定多个有效候选历史之间如何选择。只有把有效性检查与共同采用的顺序结合起来，拒绝重复支出才能超出单个节点的局部观察，成为多方可以依赖的结果。

三、历史顺序、分叉选择与最终性

分布式网络不存在一个所有参与者天然共享的消息到达顺序。某个节点先收到甲请求，另一个节点可能先收到乙请求；两个提议者也可能几乎同时提出不同的后续记录。这些差异可以在没有任何恶意的情况下出现，因此协议需要预先规定如何处理竞争的历史。

顺序之所以重要，是因为交易之间可能相互依赖。先使用资源再撤销权限，与先撤销权限再提出使用请求，可能产生不同结果。共同账本需要使参与者采用相容的执行顺序，才能使同一套规则产生相容的状态。顺序是有效执行的条件，同时也可能影响不同主体的实际利益。

账本顺序不必等于现实事件发生的精确顺序。请求进入网络之前可能已经等待，传播路径可能不同，提议者也可能按协议允许的方式选择交易。区块时间和提交时间各有具体含义，不能直接推出谁在现实中最早作出贡献或首先取得某种资格。若制度赋予时间顺序以权益后果，需要明确采用哪种时间证据。

由此，排序机制需要接受制度审查。在技术上符合规则的顺序，仍可能使某些请求长期落后，或者让具有入口和排序能力的主体获得优势。共同账本可以让已经采用的顺序更容易检查，但排序是否公平、有效请求能否获得合理处理，仍需结合机制和实际运行评价。

分叉表示历史出现不同延续。短暂分叉可以发生于使用相同规则的参与者之间，其原因是信息尚未充分传播。另一些分叉则来自不同参与者采用了不兼容的有效性规则。前者通常由既定的分叉选择机制处理；后者可能形成持续的网络分离，不能仅靠继续交换消息就恢复共同判断。

分叉选择需要在协议认可的有效候选历史中进行。比特币采用累计工作量作为选择有效链的重要依据，不能简单理解为“区块个数最多的一条一定获胜”。如果候选历史包含违反本地有效规则的区块，更大的工作量也不会使遵守这些规则的完整验证节点接受它。Bitcoin开发文档：区块高度与分叉〔2〕

其他系统可以采用不同的权重和确认结构。以太坊的Gasper说明将分叉选择与最终性机制区分：前者帮助确定当前继续构建的历史，后者使符合相应条件的检查点取得更强的确认地位。这说明，选择当前链头与确定哪些历史已达到最终性，是相关但不同的任务。Ethereum开发文档：Gasper〔4〕

当节点依据分叉选择改变当前采用的历史时，可能发生链重组。原先在本地链上的某些交易不再位于新的采用历史中，相应状态需要重新计算。相关交易可能随后重新被纳入，也可能因冲突或条件变化不再有效。查询结果曾经出现过，不能据此保证它会始终保持相同的确认地位。

最终性所回答的，是某项已经形成的结果在什么条件下可以被稳定采用。它并不只有一种表达方式。在概率性确认机制中，随着后续历史继续建立，在给定攻击能力和网络条件的模型下，结果被替换的风险通常可以降低。确认次数是一项观察指标，其含义仍取决于具体协议和安全假设，不能解释为达到固定次数后风险绝对归零。

在采用明确最终性规则的机制中，确认需要满足规定的证明和程序。在相应故障上限、验证者行为及其他安全条件成立时，遵守规则的参与者不应确认相互冲突的最终结果。这里的确定性属于模型内的安全保证；若关键假设遭到破坏，系统仍可能发生严重故障，并需要协议规定或额外治理程序处理。

经济约束可以支持这些保证。使矛盾确认带来处罚或高额成本，有助于约束参与者行为，但不能把处罚机制当作逻辑上的绝对禁止。也不能认为发生处罚后，受到影响的参与者就必然得到足额补偿。确认安全、违规责任和损失分担，是需要分别说明的关系。

对使用者而言，有必要把交易经历的阶段清楚表达。

观察到的阶段	可以据此理解的进展	仍需核验的内容
已提交或待处理	请求已被某个入口接收或暂存	是否传播、是否有效及能否纳入
已纳入某个区块	请求进入了该区块的记录	区块是否有效、是否处于当前采用历史及执行结果
已获得一定确认	该记录在采用历史中获得进一步支持	确认条件、重组风险及是否满足业务要求
已达到协议最终性	记录满足相应的最终确认规则	安全假设及外部生效、履行条件

表中的最后阶段并不适用于所有协议；没有明确最终性证明的系统，需要准确说明采用的风险判断方式。界面不应把不同机制统一压缩为一个没有解释的“已完成”。组织也需要预先确定何种业务可以在哪一阶段继续，而不能在看到结果后再临时改变确认标准。

业务对结果稳定性的需求可能不同。可以撤回的内部准备动作，与会引起难以恢复的外部交付，不宜无条件依赖同一确认阶段。本书主张，把技术确认程度与后续承诺相联系：何时允许继续准备，何时允许对外履行，出现重组后怎样暂停、纠正和分担影响，都应当形成明确安排。

技术上的最终性也不意味着制度不能纠错。账本可以保留原有历史，再通过有权的新交易调整当前状态；现实中的争议处理，也可能形成新的履行义务。这与直接改写已确认历史属于不同路径。稳定保存历史和允许有依据地纠正后果，可以在同一制度中同时存在。

对于利益相关者资本治理，还需要识别最终性的范围。某条链确认了一项凭证变更，不代表另一套系统中的相关状态同时完成，也不保证现实资产已经交付。发生持久分叉时，两个网络还可能各自保留相似凭证；这不会仅凭记录复制就在现实中创造两份相同资源或两项当然有效的请求权。凭证所指权利如何延续，需要原有制度与相应处置程序说明。

共同状态由此取得可供后续行动使用的稳定程度。它的价值在于使参与者能够依据明确条件安排承诺，同时知道哪些变化仍可能发生、哪些边界没有被技术覆盖。最终性将确认转化为行动预期，其制度意义也体现在这种预期的准确表达上。

四、网络故障、账本分歧与一致性条件

分布式系统必须在参与者只能看到部分信息的条件下运行。网络延迟、消息丢失、设备停机和软件差异，都可能影响各方的判断。节点没有收到某条消息时，往往不能立即分辨对方是暂时缓慢、已经离线，还是有意不响应。确认机制需要在这种不确定性中形成可解释的处理方式。

需要先区分不同故障。节点停止工作，主要减少可参与处理的资源；节点提供错误结果或向不同对象发送相互矛盾的信息，则可能主动干扰确认。后一类通常纳入拜占庭故障的讨论。只考虑停机的复制机制，不能自动被视为能够承受参与者任意偏离协议的行为。

消息传递条件也需要明确。有的模型假定延迟存在已知上限，有的允许消息延迟不可预测；部分同步模型则在相应形式下假定网络最终进入具有延迟约束的阶段。不同假设支持不同保证。不能把正常运行时的速度表现，直接当作任意故障下仍能持续确认的证明。

分布式一致性中，安全性与活性是两个基本维度。在本章语境下，安全性主要要求遵守规则的参与者不确认相互冲突的最终结果；活性关注在规定条件下系统能否继续形成结果。等待更多信息可能有助于避免冲突，却会影响进展；提前继续则需要解释依据何在，以及承担何种暂时不确定性。

Fischer、Lynch与Paterson的研究说明，在完全异步的消息传递模型中，即使只允许一个进程停止工作，也不存在能够在所有允许执行中保证终止的确定性共识协议。这个结论针对明确的模型和保证，并不表示现实系统不能形成共识，而是要求准确说明保证成立所依赖的条件。Fischer、Lynch与Paterson，1985：单进程故障下分布式共识的不可能性〔5〕

实际协议可以引入不同的时间假设、随机化方法或其他机制，以取得相应范围内的进展保证。超时可以帮助触发更换提议者或进入下一轮，但超时本身不能证明未响应者必然恶意。将网络慢与违规行为混同，可能使故障处理变成不当处罚，也可能损害恢复后的继续协作。

网络分区是理解这种边界的重要情形。不同部分暂时无法通信时，一些协议可能允许各自延续尚未最终确认的候选历史，恢复通信后再按规则处理；另一些机制在无法取得必要确认时，会暂停新增最终结果。具体后果取决于协议、分区持续时间和参与力量分布，不能统一表述为“断网也能保持所有功能”。

如果不同分区都无条件把针对同一资源的冲突行动作为不可撤销结果对外履行，那么恢复连接时，现实后果未必还能合并。共同资源的排他性要求，决定了网络分区期间不能仅凭各自局部可用就推定全局可以完成。系统应当区分暂存请求、提供历史查询和确认新增状态等不同服务能力。

许多确认机制通过具有适当交集的确认集合支持安全性。其基本思路是，使两个可能决定冲突结果的集合，必须共享足够的守规参与力量；这些参与者按照协议的锁定和轮次规则，不会为相互冲突的最终结果同时提供所需支持。单有一个多数比例仍然不够，参与身份、权重、消息认证与跨轮次规则都必须配合。

因而，所谓容错门槛必须结合具体协议解释。按节点数量、计算能力或质押权重衡量的门槛，分别涉及不同控制条件。许多节点由同一主体支配，或共同依赖一个可能失效的服务入口，会形成相关风险。实际独立性和故障是否可能同时发生，需要与名义上的分散数量一并检查。

账本分歧还可能源于软件和规则，而非通信。相同历史在不同执行实现中产生不同结果，可能表明实现存在错误；参与者有意采用不兼容规则，则可能形成制度与网络分离。前者需要定位、修复和核验，后者还需要处理版本采用及合作范围。不能把所有分歧都当作等待同步即可消失的现象。

分歧或故障情形	首先需要识别什么	处理时需要保持的边界
节点落后或暂时失联	数据缺口、采用位置及连接状态	旧查询结果不冒充当前已确认状态
同规则下出现候选分叉	候选历史有效性和分叉选择依据	暂时纳入不冒充最终确认
WISERUNION · V1.0 执行结果或规则版本不同	实现差异、规则来源和适用版本	不用数量优势替代有效性核验

分歧或故障情形	首先需要识别什么	处理时需要保持的边界
出现相互冲突的最终性证据	证据真实性及哪些安全条件可能失效	不按普通同步问题自动覆盖争议

恢复工作需要一个可以说明的起点。重新接入的节点应当检查必要的历史、状态和确认依据，使用检查点或快照时，还应当了解其来源与验证方式。某些协议对长期离线后的重新加入具有额外要求。下载速度快，不能代替对所采用状态的核验。

数据可得性同样影响共同验证。一个摘要可以帮助核对数据，但仅有摘要未必足以重建状态或判断执行是否正确。系统需要确保相应验证方式所必需的数据、证明和历史依据能够取得，并说明保存责任。若全部查询依赖一个可能停止服务的入口，账本的分布式结构就未必转化为参与者实际可用的核验能力。

组织还需要把故障状态翻译为行动规则。查询停留在旧位置时，应当说明其依据；不能继续确认时，应当明确哪些履行需要等待；恢复后，应当核对重复提交和未完成承诺。技术上的停顿可以被准确表达为暂缓，不能自动变成拒绝责任或消除既有义务的理由。

本书提出“可说明的共同状态”这一设计要求：重要结果应当同时提供状态内容、依据位置、适用规则和确认程度，使参与者能够判断它现在可以支持什么行动。它不要求每个人掌握全部协议细节，而是要求系统把影响承诺的关键条件转化为可理解、可检查的信息。

这一要求也适用于未来的多账本协作。不同网络即使分别形成一致状态，相互连接仍需处理证据传递、确认时间和故障责任。可以研究让每一项跨系统承诺附带清楚的状态依据及接受条件，但这些机制能否保持责任连续、避免重复履行，需要具体检验。局部的一致性不会自动扩大为跨系统的共同确定性。

分布式账本的制度贡献，正在于让多方在明确条件下，持续维护一组可以共同采用的行动依据。它通过交易表达变化，通过有效性规则限制变化，通过排序和最终性稳定结果，并通过故障处理说明保障的边界。下一章将进一步讨论承担这些工作的确认制度：谁可以参与、谁提出记录、谁负责验证，以及其权力、成本与责任如何安排。

定稿补强：最终性的四层表达与网络分区

为了避免把不同含义压缩成一个“已完成”，本书在定稿中采用四层表达。概率稳定性表示结果在给定攻击与网络假设下，随确认积累而降低被重组的可能；经济最终性表示逆转需要承担显著成本或处罚；协议确定性表示在明确故障上限和协议条件内，不应产生相互冲突的最终结果；业务采用则是组织基于技术状态、外部条件和损失承受能力决定是否继续履行。法律上的终局、不可撤销或对世效力不由这四层中的任何一层自动产生。

层次	主要前提	可能失效的情形	组织需要决定的事项
概率稳定性	攻击能力、网络与观察窗口符合模型	重组、算力或权重异常	等待深度与风险阈值
经济最终性	处罚、质押或攻击成本能够约束行为	激励失效、成本外部化、治理干预	可接受损失与补偿路径
协议确定性	故障上限、验证者集合与同步条件成立	假设被突破、实现缺陷、密钥共谋	暂停、恢复与冲突处置
业务采用	技术确认和链外条件均满足	事实错误、义务未履行、法律限制	继续履行、人工复核与救济

网络分区时还要把安全性和活性分开。系统可能为了避免冲突而暂时停止确认，也可能继续处理而增加分歧风险。界面和运行规则应说明当前状态是等待、降级、暂停还是可继续，并预先确定恢复后的重放、对账和补偿程序。继续出块不等于全部安全条件仍然成立，暂时停顿也不必然表示制度失败。

本章注释

- [SRC-041] Ethereum.org：Ethereum开发文档：交易。[原文或官方页面](#)
 - 本章引证：Ethereum开发文档：交易。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：以太坊开发文档：交易、Ethereum开发文档：交易。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

- 本章引证：Bitcoin开发文档：区块链与交易输出；Bitcoin开发文档：区块高度与分叉。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：比特币开发文档：区块链、Bitcoin开发文档：区块链与交易输出、Bitcoin开发文档：区块高度与分叉、Bitcoin开发文档：工作量证明与分叉选择。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
3. [SRC-036] Ethereum.org：Ethereum开发文档：Gas与执行费用。[原文或官方页面](#)
- 本章引证：Ethereum开发文档：Gas与执行费用。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum开发文档：Gas与执行费用。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
4. [SRC-032] Ethereum.org：Ethereum开发文档：Gasper。[原文或官方页面](#)
- 本章引证：Ethereum开发文档：Gasper。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum开发文档：Gasper。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
5. [SRC-048] Michael J. Fischer、Nancy A. Lynch、Michael S. Paterson：Impossibility of Distributed Consensus with One Faulty Process。[原文或官方页面](#)
- 本章引证：Fischer、Lynch与Paterson，1985：单进程故障下分布式共识的不可能性。
 - 支持范围：用于支持所引理论、模型、算法或经验研究的原始论证，本书引用主题包括：Fischer、Lynch与Paterson，1985：单进程故障下分布式共识的不可能性。
 - 使用边界：原始研究支持其设定范围内的结论，不直接证明本书提出的治理制度已获得普遍实证验证。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第九章 – 共识机制：共同账本的确认制度

共同账本能够持续存在，需要有人提出新的记录，有人检查这些记录是否符合规则，也需要一套程序处理竞争的结果。第八章已经说明，共同状态依赖交易有效性、历史顺序和最终性。本章进一步追问：谁有资格承担这些工作，确认权怎样分配，参与者为什么持续履行职责，以及不履行或滥用权限时怎样受到约束。

这些问题构成共识机制的制度内容。共识机制规定了共同账本的参与关系、确认程序和相应保障，使一部分原本需要持续协调的事项进入可以重复执行的规则。以太坊开发文档也将共识机制描述为支持分布式节点对账本状态形成一致的协议、激励和相关安排的整体，而不只是某一种资源证明方式。Ethereum开发文档：共识机制〔1〕

在这个意义上，共识机制可以理解为共同账本的确认制度。它承载的是各方已经采用的确认规则，并以技术约束执行这些规则。它并不自动完成共同目标的形成，也不直接决定企业所有利益应当怎样分配。理解它的制度价值，需要同时看见确认能力的形成过程与确认权力的适用边界。

一、参与资格、提议权限与验证职责

参与区块链网络，可以指向不同活动。读取记录、提交交易、独立验证、提出区块、参与最终确认和修改协议，具有不同作用。一个主体获得某项能力，不意味着同时获得其他全部权限。共识机制首先需要把这些角色分别表达，使参与者知道自己的行为对共同账本产生什么影响。

读取与验证尤其需要区分。读取可以依赖某个查询入口，独立验证则需要取得必要数据并执行相应检查。一个节点可以核验它所采用的记录，而不承担区块提议或确认投票；一个普通使用者也可以借助证明检查特定结果，而不进入维护者集合。因此，网络中的节点数量不能直接等同于拥有确认权的主体数量。

交易提交权也不等于区块提议权。提交者表达希望发生的状态变化，提议者则依据规则组织候选记录。提议者能够影响什么请求进入候选、采用怎样的顺序以及何时提出，但候选结果仍需要接受其他参与者或验证机制的检查。提议能力如果缺少对应约束，可能成为延迟、筛选或排斥请求的实际权力。

参与资格需要回答谁可以进入相应角色，以及进入以后能影响多少确认力量。开放网络通常需要防止一个主体仅靠批量创建身份就无限扩大影响。计算投入、质押资源或其他机制可以为这种影响设置条件。许可型网络则可以通过身份识别与准入程序确定参与者，但仍需解释准入由谁管理、怎样避免任意排除，以及退出后如何处理既有责任。

这些资格依据解决的是特定的系统问题。某种资源能够支持抗虚假身份或承担安全责任，不表示它天然代表共同事业中的全部贡献。较多计算能力或质押权重，可以依协议形成较多确认影响，却不能据此推定劳动者、客户、协作组织和其他利益相关者的合理诉求已经得到充分表达。

验证职责则需要落到可检查的对象。参与者应当知道要核验的是交易授权、资源约束、执行结果、区块结构，还是其他确认者的证据。职责不清，容易使所有人都以为某个关键条件已经由他人检查。职责明确，也有助于识别某项错误究竟发生于提出、执行、排序还是确认环节。

不同架构可以作出不同分工。Hyperledger Fabric的文档将交易提议与背书、排序、最终验证与提交区分为不同阶段；排序节点与执行和验证交易的节点并不承担完全相同的工作。这个技术结构表明，共同账本的维护职责可以分开安排，不能预设每个参与确认的节点都会完成全部业务检查。Hyperledger Fabric文档：排序服务与交易流程〔2〕

本书从制度分析出发，将这些权限和职责概括如下。

角色或权限	对共同账本的主要作用	需要防止的权限扩张
交易提交	提出具体状态变更请求	将已提交视为已经获准或已经履行
候选提议与排序	组织拟采用的记录及顺序	将组织候选的能力扩张为任意处置权
独立验证	检查记录及其结果是否符合适用规则	将技术核验扩张为全部事实认定
确认参与	按协议为采用某项结果提供支持或证明	将确认权扩张为企业全部治理权
协议修改	依有效程序调整规则及适用版本	将维护或开发能力视为当然的修改授权

同一主体可以承担多个角色，但应当保留角色之间的区别。运营一个验证服务，与代表某个组织接受新的治理安排，可能需要不同授权；受托代为操作质押资源，也不意味着受托者可以自行决定这些资源的其他用途。技术委托关系应当与现实中的责任关系对应。

还需要检查名义参与与实际控制。多个验证身份可能由同一个运营团队管理，也可能依赖相同的密钥服务、软件或基础设施。反过来，一个组织的控制能力也可以通过内部共同批准受到限制。评价分散程度，应当追踪实际决策和故障关联，不能只计算地址、设备或机构名称。

资格与职责还具有时间边界。成员加入、退出、被替换或改变权重时，系统需要确定何时开始适用新的参与集合。否则，旧集合和新集合可能分别声称自己有权确认同一个位置。成员变更因而既是管理事项，也是共识安全的一部分，需要进入可核验的过渡程序。

对于利益相关者资本治理，确认制度应当给参与者提供适当的核验和异议渠道。没有运行节点的能力，不应在制度设计上被直接解释为没有提出问题的资格；受到一项记录影响的主体，也可能需要通过代表、审计或其他安排检查其依据。确认权可以专业分工，相关权利仍需获得可行的实现路径。

共识机制由此形成一项有边界的权力委托：部分主体承担持续维护共同记录的职责，并在规则内取得相应操作权限。它的质量取决于资格是否清楚、职责能否核验，以及这些技术权限是否始终受其用途和责任约束。

二、确认程序、冲突处理与容错假设

确定参与者以后，还需要规定他们怎样共同完成确认。确认程序应当说明候选记录如何提出，验证依据怎样取得，支持以何种方式表达，达到什么条件才允许采用结果，以及不能取得结果时如何继续。只有把这些阶段连接起来，参与者才能对同一条消息的程序地位作出相容理解。

程序首先需要一个共同可识别的对象。确认者针对哪个区块、哪个高度、哪一轮次或哪个检查点表达意见，应当能够核对。如果支持消息缺少明确范围，过去的表态就可能被重复计入新的确认，或被误用在另一个网络和规则版本中。第七章讨论的签名内容与使用环境，在这里成为确认程序的基础。

对候选结果的检查，也应当先于具有相应后果的支持。收到提议，只能证明提议已经到达；完成验证，才可能形成符合职责要求的确认行为。若某种角色只检查其中一部分条件，程序应当说明其余条件由谁负责，以及最终采用如何依赖这些检查。

不同机制可以采用不同形式积累支持。有的通过对候选历史持续投入工作形成选择依据，有的通过带权确认消息形成证明，也有的把当前分叉选择与最终性确认分别安排。不能把所有共识机制简化为同一种“多数投票”。每种机制中的支持单位、有效范围和确认后果，都需要单独理解。

确认门槛的意义，也取决于它为何足以约束冲突。在一类经典拜占庭容错模型中，若总参与权重表示为 $3f + 1$ ，最多 f 的权重可能任意偏离协议，两个各含至少 $2f + 1$ 权重的集合就必然具有超过 f 的交集。这个交集包含守规力量，但它还需要与消息认证、轮次和锁定规则结合，才能支持不产生冲突决定的保证。Tendermint的形式化说明体现了这种联系。Buchman、Kwon与Milosevic：The latest gossip on BFT consensus [3]

这一门槛表达针对具体模型，不能被推广为所有网络的统一安全公式。按人数计量与按权重计量不同，固定参与集合与动态变化的集合不同，能够核验参与身份与任意创建身份也不同。若不说明分母及其来源，一个“达到三分之二”的数字本身无法说明系统获得了什么保障。

轮次与锁定规则处理的是支持如何跨时间延续。参与者在某个阶段形成承诺以后，不能仅因为下一轮出现新的提议，就随意对冲突结果再次提供足以导致确认的支持。与此同时，系统需要为没有形成决定的情况保留继续推进的路径。何时可以改变候选、需要携带哪些证据，是安全与进展能够兼容的关键。

提议者更换也应当继承必要证据。原提议者失联时，新提议者不能假定此前一切都没有发生。已经形成的确认、锁定或检查点，需要按照协议进入后续判断。程序由此使参与者的暂时离开不至于自动清空先前约束。

冲突处理还需要识别冲突所在的层次。两个尚未确认的候选结果相互竞争，可以进入既定的选择程序；一个候选包含无效交易，应当按有效性规则处理；两个结果都声称已经取得最终确认，则需要核验证据并检查安全条件是否遭到破坏。不能用处理普通候选竞争的办法，掩盖最终性冲突所揭示的问题。

容错假设限定了这些程序能够承受什么。哪些参与者可能离线，哪些可能发送矛盾消息，消息传递需要满足什么条件，以及密码学和数据可得性是否可靠，都会影响结论。第八章已经区分安全性与活性；确认制度还需要把这种区分落实为运行安排，使停顿、降级和恢复具有明确含义。

当可用的确认力量不足时，暂停新增最终结果可能是维持安全要求的一部分。暂停并不自动表示协议已经产生错误结果，也不能被表述为系统仍在正常完成全部业务。组织需要说明可以继续提供哪些查询、暂存哪些请求，以及哪些外部行动必须等待。

相反，如果关键假设已经不成立，继续沿用日常确认标签可能制造错误预期。相关参与者需要保全证据、识别受影响范围，并依据预定权限决定恢复或过渡措施。具有停止接口的人，不因此获得任意改写权；有权组织恢复的人，也需要说明恢复所采用的状态依据。

程序还应当规定规则变化如何进入系统。版本升级、参与权重调整和验证者集合更换，可能改变后续确认的条件。变更需要与当前有效规则衔接，使使用者能够判断哪个版本从何时适用。若不同群体持续采用不兼容安排，可能形成新的网络边界，相应社会关系需要另行处理。

确认制度因此同时包含正常路径和异常路径。正常路径使有效请求能够形成共同结果，异常路径使参与者知道在信息不足或假设失效时怎样限制后续行动。可持续的共同账本，需要两条路径都能被理解、执行和审查。

三、成本承担、奖励安排与违规约束

确认制度需要持续投入。设备、网络、存储、软件维护和人员工作构成直接成本；被锁定的资源、等待期间失去的其他使用机会以及必要的风险承担，也影响参与条件。共识机制即使能够自动运行，其所依赖的服务仍然需要有人长期提供。

成本首先需要找到承担者。在不同安排中，交易使用者可以通过费用承担一部分，网络可以依规则发行奖励，组织也可以从预算中支付维护报酬。没有单独发行代币，并不妨碍建立维护激励；发行了代币，也不表示成本已经获得稳定覆盖。需要检查支付资源从何而来，以及它能否支持实际需要的投入。

奖励应当说明奖励的行为。提出有效区块、及时提供确认、保持必要服务和提交可验证的违规证据，可以分别对应不同工作。若一种报酬只与名义在线时间或持有某项资格联系，就需要进一步判断它能否支持实际职责。指标容易观察，不代表它足以反映需要维护的能力。

协议只能直接评价它能够识别的事项。签名是否矛盾、确认是否在规定窗口内到达，通常比参与者是否认真维护设备、是否具有独立判断更容易进入自动检查。因此，激励设计既要利用可验证信号，也要识别信号覆盖不到的部分。组织安排、审计和专业维护可以补充这些缺口，但不应被包装成协议已经自动保证的结果。

奖励来源也影响利益分布。交易费由使用者支付，其水平可能影响参与门槛；新增单位的发行改变供给及持有结构，但其经济后果还取决于其他条件；组织预算则需要在维护账本与其他用途之间分配。共同账本的运行费用，应当成为利益相关者可以理解的支出，而非隐藏在技术标签之后。

在资本治理中，维护奖励应当与共同创造的其他回报分开表达。验证者承担确认工作，可以依据协议取得相应奖励；劳动投入、知识贡献、客户协作和组织建设，可能需要另外的评价与权益制度。确认服务的重要性，不能推出全部价值都由维护者创造，也不能使协议奖励自动成为企业利润分配权。

同样，奖励记录、可支配资产和实际经济收益具有不同含义。系统记入一定数量的奖励，只说明按相应规则形成了记账结果；参与者为履职付出的成本、资源限制及后续使用条件仍然存在。不能仅依据名义奖励数额，判断维护安排可持续或所有参与者已经获得净收益。

激励还可能改变确认权的分布。规模较大的运营者如果具有成本优势，参与力量可能逐渐集中；较高的进入成本，也可能使较小主体转而依赖受托服务。这些结果需要通过运行数据判断。本书主张，评价奖励制度时同时观察服务质量、进入退出和实际控制分布，避免只检查支付是否准确。

违规约束首先需要明确什么构成违反协议。不同请求形成竞争，未必表示谁在作恶；暂时离线，也不同于对相互矛盾的结果作出被禁止的签署。以太坊的奖励与处罚文档区分了未完成特定职责的惩罚，以及针对双重提议、双重投票或特定矛盾投票等行为的罚没。两类处理具有不同的触发条件。Ethereum开发文档：权益证明奖励与处罚〔4〕

自动处罚依赖可验证的触发证据，其判断对象可能是已经发生的协议行为，而非行为者的主观动机。密钥被盗用、操作失误和有意攻击，可能形成相同类型的违规消息。协议如何处理这些消息，与相关当事人之间如何分担责任，需要分别说明。不能把一次罚没直接解释为完整的事实调查或道德判断。

对于证据难以自动核验的行为，也不应轻率设计确定处罚。某个请求没有被纳入，可能涉及传播、费用、容量或主动排斥；如果缺少足够的可观察条件，系统未必能够区分原因。要约束这种行为，需要先明确接收凭据、处理义务和判断程序，再决定哪些部分适合自动执行。

约束还需要具有执行基础。罚没要求存在可以依规则处置的资源，取消资格要求存在有效的资格控制程序，其他责任追索则依赖相应组织或外部制度。协议没有掌握的资源，不能仅通过一条处罚声明变成可以执行的保障。

有成本的攻击也不等于不会发生攻击。参与者可能追求协议外部的收益，或者愿意承担账内损失来破坏合作。关于“守规更有利”的判断，需要说明它考虑了哪些收益、成本和行为动机。经济激励可以支持对守规参与的预期，却不能替代协议对故障力量的明确容忍条件。

处罚与受害者补偿同样不同。销毁被罚没资源、将其转给特定接收者或停止后续奖励，产生不同分配后果。即使处罚按规则发生，损失也可能没有全部恢复。因此，需要分别说明违规者承担什么，以及受到影响的参与者可以依据什么寻求处理。

退出安排也是激励制度的一部分。尚待核验的行为、可能发生的处罚和未完成的维护责任，可能要求资源在一定期间内继续受到约束；过重或不明确的退出限制，又会影响参与者加入的意愿。退出条件应当与需要覆盖的责任相联系，使责任持续与合理退出之间具有可解释的边界。

协议已经确定并能自动执行的处罚，不能由应用界面随意承诺暂停或撤销。如果某项制度希望提供复核、补偿或例外处理，应当在它实际拥有的权限和资源内设计相应路径，并说明这与底层协议处理的关系。一个组织可以审查自身责任，但未必有能力改变外部网络已经执行的罚没。

成本、奖励与约束由此构成确认制度的持续运行条件。评价它们，需要同时回答服务是否得到支持、参与是否保持可行、权力是否过度集中以及责任是否能够落实。准确执行奖励公式只是其中一步，长期维护共同账本还依赖这些条件之间的协调。

四、协议共识为何不能替代事实判断与制度正当性

共识机制能够使参与者对共同账本形成可采用的结果，但其确认对象需要保持明确。验证者检查的是某项记录和状态变更是否符合规定条件；现实事实是否成立，规则为何有权约束相关主体，则可能需要不同的证据和判断程序。

这种边界首先来自信息来源。系统可以检查一项现实事项已经由具备登记权限的主体签署确认，却不能仅凭该签署推定事项确实发生。多个验证者重复检查同一个输入，只增加了对输入符合协议条件的共同核验，并没有自动增加对现实事件的独立观察。

第六章已经区分记录一致、事实真实与制度正当，第十二章将进一步建立现实信息输入的责任链。本章据此只确认一项边界：协议可以在错误输入之上保持一致，验证者数量或确认权重不能替代链下事实核验。

当一种安排同时让某些参与者承担外部事实审查时，也应当区分其两种职责。其作为事实审核者，需要取得材料、调查来源和回应异议；其作为账本确认者，则需要依协议处理已经表达的结果。两项职责可以由同一主体承担，却不会因此具有相同的判断标准。

在利益相关者资本治理中，贡献评价进一步包含因果和价值判断。某项行动发生过，未必能够精确说明它为共同成果增加了多少价值；某项结果得到认可，也未必意味着可以把它全部归于单一主体。贡献口径、共同作用和已有回报，需要在评价制度中说明。共识机制可以记录采用了哪一种评价，却不能用确认权重代替这些论证。

制度正当性则涉及规则来源与约束理由。谁有权确定贡献标准，谁应当参与分配原则的讨论，哪些基本利益需要受到保护，以及受影响者如何提出异议，都超出账本状态确认本身。一个规则可以被精确执行，同时仍然存在权限不足、参与不充分或负担分配失衡的问题。

共识机制中的权重尤其不能被自动扩大解释。用于抗虚假身份、提供安全资源或分担维护成本的权重，解决的是特定技术问题；企业治理中的表达资格，还可能涉及投入、依赖、风险和受到影响的程度。将前一种权重直接用作后一种权利的全部依据，需要额外论证，不能仅以系统已经支持为理由。

这种区分也关系到规则修改。协议确认了一笔修改参数的交易，可以说明它满足系统当前设定的修改条件；这组条件是否得到适当授权，修改是否越过组织权限，仍然需要相应依据。技术上能够修改，与制度上有权修改之间的距离，不会因为修改获得较多验证支持而自然消失。

不同争议因此需要进入不同的处理路径。

争议对象	首要判断依据	共识确认能够承担的作用
一项交易是否符合账本规则	有效规则、前置状态和验证证据	按协议拒绝无效变更或确认相应结果
一项贡献或履行是否真实	原始材料、独立核验和事实复核	保存主张、审核结果及其变化过程
一项评价或分配是否有充分理由	评价方法、利益影响和治理程序	固定采用的口径与有权决定
一项规则是否有权约束相关主体	权限来源、参与条件和适用边界	核验并记录已被有效表达的授权条件

这种分工并不要求不同层次彼此隔绝。事实复核可以导致原有认定调整，新的有效决定可以触发后续状态变更，技术异常也可以成为启动治理审查的原因。关键在于每一次转换都有可以追踪的依据，不能把一个层次的结论直接改名为另一个层次已经完成。

面对错误输入，应当追查输入与审核责任，不能只因验证者采用了符合协议条件的记录，就推定它们全部失职。面对违反协议的确认，也不能仅以基础业务已经获得认可为理由，忽略技术程序的缺陷。责任归属需要对应具体职责和行为，否则共同确认人数越多，反而越难找到真正需要改进的环节。

制度需要为这些联系保留清楚的状态表达。记录已经被确认，但事实仍有争议；事实已获核实，但权益尚未批准；权益已经成立，但现实履行尚未完成，都可以是准确且有用的状态。把它们全部压缩为“共识已达成”，会使参与者无法知道自己究竟可以主张什么。

本书据此提出，应用共识机制时，应当同时建立确认依据、事实责任和制度依据之间的对应关系。一项重要结果需要能够说明：协议确认了什么，哪些外部材料支持其内容，以及哪个有权程序决定其后果。需要保密的材料可以按权限披露，但责任主体、核验路径和争议入口应当明确。

这种对应关系也有助于理解本书关于制度技术的基本判断。共同认可可以通过有权程序形成明确规则，规则中的一部分再被表达为技术可检查的条件，共识机制据此维护共同状态。这是一条需要逐步完成的制度化路径。代码执行的是已经表达的条件，社会共识中尚未澄清的内容不会因此自动获得答案。

面向未来，自动代理可以承担更大量的提议、核验与运行维护，但多个代理给出相同结果，仍需检查它们是否依赖相同信息来源、同一模型或同一控制者。扩大自动参与数量，不必然增加独立证据或代表范围。组织需要继续识别实际控制、委托边界和错误责任。

本书提出一个有待检验的方向：随着确认工作的自动化程度提高，制度设计可以更加重视“技术确认权的受托性质”。承担者应当能够证明自己按明确职责处理了记录，其报酬与责任对应，权限也能够依有效程序交接。这个方向是否改善核验能力、减少权力集中并支持长期合作，需要在不同组织条件下检验。

共识机制的制度价值，最终体现为共同账本的确认过程更可预期、更可核验，并使维护者的权限与责任得到明确表达。它为共同创造提供了一层持续运行的技术基础，同时依赖事实核验、组织治理和有效授权来确定自己的对象与边界。下一章将比较工作量证明、权益证明和许可型网络中的具体安排，进一步观察不同选择如何改变参与门槛、权力分布、最终性与退出条件。

定稿补强：把共识拆成可比较的制度维度

“共识机制”不是一个不可再分的功能。网络首先需要回答参与者如何被识别或限制虚假身份，谁可以提出候选记录，谁负责验证有效性，冲突记录如何排序，执行结果如何取得一致，何时达到相应最终性，以及成本、奖励、处罚和规则变更由谁承担。工作量证明、权益证明和许可型拜占庭容错分别覆盖其中若干维度，并可能与其他机制组合。

因此，机制选择不应只比较吞吐量或一个笼统的“去中心化程度”。同一网络可以使用权益抵抗女巫、以委员会进行提议与证明、用执行层处理状态转换，再由链外治理决定软件升级。每一层都可能产生集中、串谋或责任空缺。比较时要逐层识别参与门槛、故障假设、权力集中点、证据和退出条件。

这也要求把安全性与活性分别说明：安全性关注系统是否避免确认相互冲突的结果，活性关注有效请求能否在条件允许时继续得到处理。制度可以在故障时选择保护安全而牺牲即时活性，也可以设置受限降级，但不能用“系统仍在运行”替代对冲突风险的判断。

本章注释

1. [SRC-030] Ethereum.org：Ethereum开发文档：共识机制。[原文或官方页面](#)

- 本章引证：Ethereum开发文档：共识机制。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum开发文档：共识机制。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-049] Hyperledger Fabric：Hyperledger Fabric文档：排序服务及容错类型。[原文或官方页面](#)

- 本章引证：Hyperledger Fabric文档：排序服务与交易流程。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Hyperledger Fabric文档：排序服务与交易流程、Hyperledger Fabric文档：排序服务及容错类型。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

3. [SRC-002] Ethan Buchman、Jae Kwon、Zarko Milosevic：The latest gossip on BFT consensus。[原文或官方页面](#)

- 本章引证：Buchman、Kwon与Milosevic：The latest gossip on BFT consensus。
- 支持范围：用于支持所引理论、模型、算法或经验研究的原始论证，本书引用主题包括：Buchman、Kwon与Milosevic：The latest gossip on BFT consensus。

- 使用边界：原始研究支持其设定范围内的结论，不直接证明本书提出的治理制度已获得普遍实证验证。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
4. [SRC-033] Ethereum.org：Ethereum开发文档：权益证明奖励与处罚。[原文或官方页面](#)
- 本章引证：Ethereum开发文档：权益证明奖励与处罚。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum开发文档：权益证明奖励与处罚。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第十章 – 不同共识机制中的制度安排

共识机制将共同账本的确认工作分配给具体参与者，也决定他们凭什么进入、依据什么取得影响，以及怎样承担维护责任。不同机制对这些问题的回答，进而影响资源投入、权力分布和结果的稳定性。比较共识机制，需要沿着这些关系展开。

本章讨论的几种安排并不处于完全相同的分类层次。工作量证明和权益证明，主要涉及通过何种资源约束参与及分配相应影响；许可型网络强调谁可以进入哪些角色；拜占庭容错协议则处理在部分参与者可能偏离规则时，如何形成相容的确认结果。这些安排可以相互组合，不能只按名称把它们理解为彼此排斥的三种技术。

因此，本章既比较其技术原理，也分析其制度后果。问题在于：什么资源成为确认能力的基础，谁实际控制这些资源，什么条件支持最终性，以及参与者退出后哪些责任仍然持续。利益相关者资本治理需要据此判断，某种账本安排能否为共同创造提供适当的基础。

一、工作量证明：计算竞争、累计工作与安全成本

工作量证明把提出有效区块的机会，与符合协议要求的计算过程联系起来。在典型的哈希型工作量证明中，参与者反复调整候选区块中的可变数据，计算摘要，并寻找满足目标条件的结果。别人取得候选区块后，可以较容易地检查这一条件是否满足。

这种过程具有寻找成本与核验成本之间的差异。寻找有效结果通常需要反复试算，验证结果则不需要重做全部试算。每次尝试都可能成功；在其他条件相近时，持续投入较多有效计算能力的参与者，长期获得区块机会的概率通常较高。一次竞争结果并不保证总由规模最大的参与者取得。

工作量证明也不直接证明某台设备实际消耗了多少电力。一个满足条件的摘要，是关于该计算条件的可核验证据，可以与预期寻找工作量建立联系，却不是对全部尝试次数、设备效率或能源来源的逐项计量。因此，协议所计量的工作，与现实资源成本需要分别理解。

在比特币式的账本结构中，区块通过前后关联形成历史，参与者在符合有效性规则的候选历史中比较累计工作量。这个依据并非简单统计区块数量，而是按照各区块所对应的难度条件累计相应工作。当前拥有多少计算能力，与过去一条历史已经累计多少工作，也属于不同概念。Bitcoin开发文档：工作量证明与分叉选择〔1〕

累计工作使历史改写需要面对持续竞争。试图从过去某处建立替代历史的参与者，不仅要构造满足规则的区块，还需要使替代历史在协议选择中取得足够优势。在守规计算力量、网络传播和攻击能力等条件成立时，后续工作积累能够降低既有记录被替换的风险。这种保障具有条件，不能将某个确认次数解释为风险绝对消失。

资源竞争也限制了凭空增加身份的作用。一个主体把自己的计算活动拆成许多名称，不会仅靠名称数量增加实际计算能力。协议据此可以在不预先逐一确认现实身份的情况下，建立某种参与影响的分配方式。但它解决的是虚假身份对计算竞争的影响，并不保证实际资源分散在足够独立的主体手中。

算力较强也不意味着可以让任何交易成为有效交易。在既定规则下，遵守规则的完整验证节点仍会检查签名、资源约束和其他条件。较强计算力量可能影响排序、排斥交易或尝试重组，却不能仅凭工作量伪造他人的有效签名，或要求这些节点接受违反既定发行规则的结果。

由此，区块生产权、交易验证和规则采用之间形成分工。生产者能够提出历史延续，验证者依据所采用的规则检查它；开发者可以提出规则修改，但软件提案也需要相应采用过程。现实中的这些力量可能相互影响，不能把协议变更权直接等同于算力份额。

持续竞争需要支付设备、能源、场地、网络 and 运行维护成本。设备更新与其他用途之间的转换，也会影响参与条件。不同主体面对的成本可能不同，因此形式上的开放参与，并不必然形成相同的经济进入机会。分析制度后果时，需要观察资源取得条件及其实际集中程度。

矿池是组织计算参与的一种方式。通过汇集计算并按约定分配收益，参与者可以减少独立获得区块时收入间隔的不确定性。与此同时，候选区块如何构造、交易怎样选择以及报酬如何结算，可能受到矿池安排影响。矿池提供了合作服务，也引入了相应的控制关系。Bitcoin开发文档：挖矿与矿池〔2〕

因此，矿池控制与算力所有不能简单画等号。参与者是否能够更换矿池，谁决定候选交易，是否存在设备或服务依赖，都会影响实际权力。名义算力份额可以提供线索，但仍需要了解背后的组织方式，才能判断某一主体能够持续影响什么。

奖励为这种运行提供经济支持。比特币白皮书将区块中的新增发行与交易费用作为激励来源，并讨论守规生产与破坏账本之间的利益关系。这是一种关于符号激励的设计思路^①，实际约束效果仍取决于成本、收入和攻击者可能追求的其他利益。Nakamoto：Bitcoin，第6节^{②③}

这里需要避免从安全支出跳到价值判断。消耗资源可以支持账本安全机制，却不直接证明账本中的资产具有同等经济价值，也不证明所记录的分配具有正当性。⁷确认服务对共同事业的作用，应当依据它提供了什么保障、付出了什么成本来评价。

工作量证明还要求持续关注未来维护条件。过去积累的工作提供历史基础，后续参与力量和资源投入则影响继续维护的能力。不能因为历史很长，就推定未来在任何条件下都能保持同样保障。奖励来源、设备结构和参与者行为的变化，需要进入长期评价。

对利益相关者资本治理而言，工作量证明提供了一种通过开放资源竞争维护历史的方式。它适合被作为具有特定条件的确认基础来分析，但协议中的计算工作不能被直接当作企业贡献的统一尺度。维护账本的工作与共同事业中的劳动、知识、关系和风险承担，需要分别表达。

二、权益证明：质押参与、确认权重与激励约束

权益证明通常把参与资格或确认影响，与按协议投入并受到约束的资源联系起来。参与者需要满足相应质押、激活和运行条件，才能进入特定确认角色。这里的“权益”首先是协议所识别的质押资源及其权重，不应自动解释为企业股权或对全部共同事业的治理资格。

持有资产与承担验证职责之间仍有距离。资产持有人可能自行运行验证服务，也可能委托他人操作，或者通过其他服务关系间接参与。谁提供质押资源、谁实际签署确认、谁控制退出和提取，需要分别识别。相同的账面持有量，可以对应不同的实际控制关系。

权益证明需要与具体的提议、投票和分叉选择程序结合。协议可以依据有效质押权重分配提议机会和确认影响，也可以为不同角色设置不同条件。拥有较多普通网络连接或创建更多地址，并不会当然扩大有效质押总量；但权重怎样计算、何时生效和如何变化，仍由具体规则决定。

以太坊的权益证明说明将区块提议、执行验证、确认消息和检查点最终性联系起来。其最终性机制需要按有效质押权重形成规定的支持，并经过相应检查点程序。这为理解质押资源怎样进入确认提供了技术参照，不能被简化为所有节点各投一票，也不能推广为所有权益证明网络都采用相同程序。Ethereum开发文档：权益证明〔4〕

权益证明并不天然等于某一种最终性。有的设计以链式选择为主要结构，有的结合明确的拜占庭容错确认，有的把链头选择与最终性分别安排。比较时，应当检查具体协议如何处理冲突、什么证据代表确认，以及安全和进展分别依赖什么条件。

质押使参与资源能够在一定范围内承担责任。若协议能够识别被禁止的矛盾签署，就可以按照规则对相应资源采取处罚。这样，部分安全成本从持续竞争的计算支出，转为资源占用、操作责任和可能发生的损失。验证服务仍需要计算、存储与网络维护，质押不会消除全部运行成本。

未及时履职与可被证明的严重违规，也可能对应不同处理。协议可以减少奖励、扣减资源或对特定行为执行罚没，但触发条件必须具体。处罚是否有效，还取决于证据可得、资源仍在约束范围内以及处理程序能够执行。一个抽象的质押数额，不能独立证明任何攻击都会得到充分约束。

激励设计希望使正确参与具有持续吸引力，但行为动机可能超出账内收益。若某些主体重视对外部业务的影响，愿意承担损失，或者控制了实际操作而不承担全部经济后果，就需要重新分析约束效果。奖励和罚没为守规行为提供支持，不能代替明确的故障上限与协议证明。

受托参与尤其需要检查风险与控制是否对应。质押资源的提供者可能承担损失，运营者却掌握签名与运行决策；平台也可能控制提取条件或收取服务费用。委托关系因此需要说明职责、报酬、故障责任及退出安排，避免把协议层的质押记录当作完整的受托管理制度。

确认力量也可能受到规模和服务结构影响。大型运营者如果具有技术、成本或渠道优势，可能吸引更多委托；奖励是否复投以及权重怎样调整，也可能影响后续分布。这些是需要持续观察的机制结果，不能仅凭权益证明的名称就断言它必然集中或必然分散。

退出与提取在这种安排中通常具有不同阶段。停止承担验证角色、等待尚存责任被处理，以及取得可自由使用的资源，未必同时发生。以太坊的提款说明也区分了验证者退出、相应排队和通过服务商参与时的其他条件。能够转让某种参与凭证，并不意味着底层验证者已经退出或责任已经解除。Ethereum：质押提款〔5〕

退出规则还与历史安全相关。若过去参与者的资源已经不再受到约束，仅核验旧密钥对一段替代历史的签名，可能不足以帮助长期离线或新加入的节点识别应该采用的历史。部分权益证明设计因此对同步起点提出额外要求。

以太坊用弱主观性检查点处理这类历史识别问题，新加入或需要重新建立可靠同步依据的节点，需要取得适当的近期可信起点，再继续验证。检查点来源与交叉核验因此构成安全条件的一部分。Ethereum开发文档：弱主观性〔6〕

这个条件说明，评价权益证明需要同时考察当前确认和历史接续。谁提供初始参照，哪些主体保持独立核验，退出责任延续多久，以及异常后采用何种恢复路径，都影响共同账本的长期可用性。

对于利益相关者资本治理，质押参与可以提供一种明确的技术责任安排，但资源锁定不能替代贡献评价。某人有能力承担较多质押，不表示其已经承担企业全部长期风险；获得协议确认权，也不表示其有权替其他利益相关者决定分配。采用权益证明时，需要持续保持这两层制度之间的边界。

三、许可型网络：身份准入与拜占庭容错协议

许可型网络通过准入安排确定哪些主体可以承担特定角色。读取账本、提交业务请求、执行程序、参与排序和修改配置，可以分别设置资格。它并不必然意味着全部数据只对内部开放，也不必然由单一组织控制；其具体含义取决于哪些活动需要许可，以及谁能够授予和撤销许可。

身份准入为确认制度提供了不同的基础。参与者可以被关联到现实中的组织和责任主体，维护职责也可以通过既定关系分配。系统因而不一定需要用开放计算竞争或公开质押，来解决所有参与资格问题。但身份已经明确，不表示参与者一定守规，也不表示其设备、人员和密钥不会出现问题。

因此，准入制度需要与故障模型分别选择。崩溃容错机制主要处理节点停机、失联等故障；拜占庭容错机制则进一步考虑部分参与者发送矛盾信息或任意偏离协议的情形。许可型网络可以采用前者，也可以采用后者。获得许可这一事实，不能自动把可能恶意或被控制的节点简化为只会停机的节点。

Hyperledger Fabric的文档分别介绍了采用Raft的崩溃容错排序服务和采用SmartBFT的拜占庭容错排序服务，并明确两者面对的故障范围不同。这表明，网络具有身份准入制度之后，仍需选择适当的确认协议。Hyperledger Fabric文档：排序服务及容错类型〔7〕

在一类具有明确最终性的拜占庭容错协议中，参与集合、权重和消息认证是已知的，确认者按规定轮次形成支持，并以相应锁定规则约束后续行为。达到确认条件后，守规参与者在安全假设成立时，不会再确认与之冲突的结果。第九章所讨论的确认集合交集，在这里获得具体用途。

这种保障仍然依赖足够的守规力量。若关键参与者失联，系统可能无法继续形成最终确认；若偏离协议的力量超过允许范围，安全保证也可能不再成立。协议中关于安全性的条件与关于继续推进的网络条件，应当分别说明。身份可识别有助于追责，却不会取消这些技术限制。Buchman、Kwon与Milosevic：The latest gossip on BFT consensus〔8〕

以身份或声誉作为资格基础的安排，有时也被归入权威证明的讨论。但身份来源、提议轮换和容错确认不是同一件事。仅有一个经批准的生产者名单，尚未完整说明名单成员相互冲突时如何处理，更没有说明名单本身由谁修改。比较这类系统，应当继续检查实际协议及管理权限。

准入管理因此具有直接的权力后果。谁可以成为确认者，申请需要满足什么条件，已有成员是否能够阻止新的独立主体进入，以及被拒绝者能否获得理由，都会影响长期权力分布。技术上的身份验证只能检查既定凭据，准入理由是否适当则需要制度判断。

资格变更同样需要共同可识别的程序。增加或移除确认者，会改变能够形成确认的集合和权重。如果一个管理者可以单独替换全部参与者，就可能取得超出表面节点分布的控制能力。成员调整应当与当前规则衔接，并让相关主体知道变更何时生效、依据何在。

证书和密钥管理也需要进入这一过程。撤销未来使用资格、替换操作密钥和核验过去签名，具有不同作用。某个身份凭据不再被接受，不代表此前的全部记录可以自动删除或否认。系统需要保留当时资格、规则版本和确认依据，以支持历史核验及后续责任处理。

对于共同控制，应当追踪独立性实际存在于何处。不同机构可以各自持有密钥并管理设备，也可以把全部运行交给同一家服务商；多个节点可能分布在不同地方，却由同一个管理账户控制。形式上的组织数量和实际可独立履职的能力，需要分别评价。

技术运行职责与业务决定职责仍需分开。排序服务可以维护共同顺序，却未必负责判断每项交易所依据的贡献是否真实，或者某项分配是否应当批准。即使排序和验证在同一组织内部完成，也应当说明其权限来源。加入网络，不能被解释为接受所有未来业务安排的概括授权。

许可型网络的维护可以由成员预算、服务费用或其他有效安排支持，不必以发行新代币为前提。其激励和约束可以结合协议记录、服务约定和组织监督。但这些机制需要实际的资源、证据和执行责任；一个能够识别名称的节点，并不因此成为可以无成本信赖的节点。

退出也包含多个过程。成员停止提供确认服务，需要更新参与集合并保持必要的运行能力；退出业务合作，可能需要处理尚未完成的承诺；停止访问某些材料，还需要按原有安排处理保存和披露责任。这些过程不能仅通过删除一个网络身份一并完成。

如果许可型网络主要由同一权力中心控制，并且其他成员可以接受这样的委托，采用数据库、签名日志或其他方案也可能满足需要。是否使用区块链，应当回到第六章的比较：它是否实际提供了有价值的共同验证、控制约束和责任延续，而不只是增加了分布式部署的外观。

许可型网络由此提供了一种把确认职责嵌入明确组织关系的路径。它可能便于安排保密、服务责任和成员更替，也需要持续防止准入权、配置权和日常操作权被无谓地集中。其制度质量取决于具体权限与责任，而非“许可”或“联盟”这一名称。

四、比较参与门槛、权力集中、最终性与退出条件

比较共识机制，应当让不同方案面对同一项治理需求。共同状态涉及什么资源，哪些主体需要独立核验，最担心哪类单方行为或协同故障，以及后续行动需要多稳定的确认，决定了比较的尺度。如果这些前提不同，单独比较吞吐量、设备数或名义费用，容易得到缺乏意义的排序。

参与门槛首先需要分层。使用系统的门槛，与独立验证的门槛不同；独立验证的门槛，又与获得提议或确认权的门槛不同。一个网络允许任何人读取，并不表示任何人都能以可承担的成本进入确认角色。评价应当说明门槛对应的是哪一层参与。

工作量证明的确认参与需要适当计算资源及持续运营能力，质押参与需要相应资源和运行条件，许可型确认则需要获得身份资格并履行服务要求。开放资源门槛可能排除资源不足者，资格审批也可能排除缺少组织渠道者。两种限制都需要结合实际影响评价，不能仅凭开放或许可的名称推定参与公平。

对利益相关者资本治理，还需要检查这些门槛是否不必要地限制了业务参与。一个主体无法运行确认节点，并不表示其贡献不应被记录，或者无权查看与自己有关的决定。底层确认可以专业化，应用层仍需要为贡献提交、知情、异议和适当参与提供路径。

权力集中则需要从实际能力分析。谁选择交易，谁决定采用的软件，谁掌握密钥与恢复入口，谁能够组织足够力量延迟确认，谁控制业务方日常依赖的查询和提交服务，都是需要检查的对象。某一环节较为分散，不能为其余环节作全面担保。

不同机制的集中路径可能不同。计算资源与矿池安排、质押资源与受托运营、身份准入与配置管理，分别构成需要观察的关系。共同的软件缺陷和基础设施依赖，也可能跨越这些分类形成风险。比较应当同时记录资源份额、实际控制和相关故障，而非仅用一个节点数代表全部状况。

最终性比较应当明确结论属于什么机制。概率性确认根据历史积累及相关模型表达风险变化；具有明确最终性规则的系统，则依据特定确认条件及安全假设表达结果。权益证明可以与不同最终性机制结合，许可型网络也需要具体协议支持。确认快慢必须连同保证范围一起理解。

退出条件需要同时观察行动自由和责任连续。停止生产区块，未必能够立即收回设备投入；停止验证，未必意味着质押资源立即可用；退出一个许可型网络，也可能保留尚未完成的业务责任。对长期合作，能够合理退出与不能任意逃避已经承担的责任，同样重要。

下表比较的是常见组合的制度侧重点，具体系统仍需要按其有效规则核验。

比较维度	工作量证明型确认	质押驱动的确​​认	身份准入与拜占庭容错确认
主要进入条件	计算资源、设备与持续运行能力	协议认可的质押资源及验证条件	有效准入身份、职责和节点能力
确认影响的主要来源	计算竞争及有效历史的累计工作	有效质押权重与相应确认程序	获准参与集合、权重及容错协议
需要观察的集中环节	设备、能源、矿池和候选构造	持仓、委托、运营和密钥控制	准入、成员变更、配置和服务控制
常见最终性表达	随后续工作积累形成概率性保障	依具体设计采用链式选择或明确最终性	在协议安全假设内形成明确确认
持续成本	计算、能源、设备和运行维护	资源占用、运行维护及违规风险	设施、通信、协调和组织监督
退出时需要处理	停止投入、设备与服务关系	退出程序、资源释放及尚存责任	集合调整、业务义务和记录交接

这些差异应当进入具体的选择理由。需要面向广泛未知主体开放确认，和需要若干具有明确责任的组织共同维护记录，可能对应不同路径。若现有安排可以通过较简单的技术提供充分保障，就没有必要仅为取得某个机制标签增加负担。若确需限制单方控制，则要检查候选方案是否真正改变了相关权限。

技术选择也不能通过任意替换权重来完成。将贡献评分直接作为确认权重，看起来可以使账本维护贴近共同创造，但评分来源、重复申报、串谋以及修改权限都会进入安全假设。既有协议在质押或其他资源条件下形成的保证，不能无条件转移到一套主观评价分数上。

本书主张，贡献评价与账本确认可以通过明确接口联系：共同账本保存评价依据和有权结果，评价制度另行规定适当权益；如果确实希望让某种贡献参与决定确认资格，就需要重新论证资格的可核验性、攻击成本和权力约束。制度目标值得追求，技术保证也必须有相应依据。

同样，采用多个机制并不自动叠加全部优点。业务网络、基础账本和外部凭证服务可以使用不同确认方式，但每一次跨系统采用都需要说明依赖的证据、最终性和故障处理。某个局部结果很稳定，不能保证其余环节同时完成，组合后的保障范围需要重新分析。

面向未来，可以研究使账本基础设施具有受约束的替换能力：当参与结构和维护条件变化时，经有效程序调整确认安排，同时保留已有权益与承诺的可核验延续。这是一项有待检验的制度设计方向。其难点在于新旧历史如何接续、谁有权决定迁移、异议如何处理，以及迁移是否引入新的控制集中。

因此，不同共识机制的价值，应当放在共同事业需要的保障、能够承担的成本和可以接受的权力结构中判断。确认制度提供稳定的共同状态，企业和其他合作组织则继续负责贡献认定、权益安排与实际履行。下一章将进入智能合约，讨论已经形成的制度规则怎样转化为可执行条件，以及共识确认与自动执行如何分工。

定稿补强：权益证明中的弱主观性与参与者引导

权益证明网络的新参与者并不总能仅凭从创世开始计算，就在所有可能历史之间得到唯一可信结论。检查点、客户端版本、验证者集合和社会协调可能参与新节点的引导。这种弱主观性不是对技术的否定，而是要求系统公开说明参与者还接受了哪些起点和更新来源。

采用权益证明时，应登记可信检查点的产生与发布主体、检查点新鲜度、客户端更新渠道、验证者集合变化和长程攻击处置。新节点、长期离线节点与灾难恢复节点应采用明确的引导程序，并能核验所接受起点的来源。若不同来源提供冲突检查点，系统应停止自动采用并进入预定的技术和治理程序。

因此，共识机制比较还要加入“新参与者如何开始信任”这一维度。开放参与不意味着完全没有外部引导；许可网络的身份准入也不意味着历史一定可靠。每种机制都应公开其最小信任基础。

本章注释

1. [SRC-011] Bitcoin Project：Bitcoin开发文档：工作量证明与分叉选择。[原文或官方页面](#)

- 本章引证：Bitcoin开发文档：工作量证明与分叉选择。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：比特币开发文档：区块链、Bitcoin开发文档：区块链与交易输出、Bitcoin开发文档：区块高度与分叉、Bitcoin开发文档：工作量证明与分叉选择。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-012] Bitcoin Project：Bitcoin开发文档：挖矿与矿池。[原文或官方页面](#)

- 本章引证：Bitcoin开发文档：挖矿与矿池。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Bitcoin开发文档：挖矿与矿池。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

3. [SRC-003] Satoshi Nakamoto：Bitcoin: A Peer-to-Peer Electronic Cash System。[原文或官方页面](#)

- 本章引证：Nakamoto：Bitcoin，第6节。
- 支持范围：用于支持所引理论、模型、算法或经验研究的原始论证，本书引用主题包括：比特币白皮书，第2节、比特币白皮书，第11节、Nakamoto：Bitcoin，第6节。
- 使用边界：原始研究支持其设定范围内的结论，不直接证明本书提出的治理制度已获得普遍实证验证。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

4. [SRC-031] Ethereum.org：Ethereum开发文档：权益证明。[原文或官方页面](#)

- 本章引证：Ethereum开发文档：权益证明。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：以太坊开发文档：权益证明、Ethereum开发文档：权益证明。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

5. [SRC-042] Ethereum.org：质押提款。[原文或官方页面](#)

- 本章引证：Ethereum：质押提款。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum：质押提款

- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
6. [SRC-034] Ethereum.org：Ethereum开发文档：弱主观性。[原文或官方页面](#)
- 本章引证：Ethereum开发文档：弱主观性。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum开发文档：弱主观性。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
7. [SRC-049] Hyperledger Fabric：Hyperledger Fabric文档：排序服务及容错类型。[原文或官方页面](#)
- 本章引证：Hyperledger Fabric文档：排序服务及容错类型。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Hyperledger Fabric文档：排序服务与交易流程、Hyperledger Fabric文档：排序服务及容错类型。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
8. [SRC-002] Ethan Buchman、Jae Kwon、Zarko Milosevic：The latest gossip on BFT consensus。[原文或官方页面](#)
- 本章引证：Buchman、Kwon与Milosevic：The latest gossip on BFT consensus。
 - 支持范围：用于支持所引理论、模型、算法或经验研究的原始论证，本书引用主题包括：Buchman、Kwon与Milosevic：The latest gossip on BFT consensus。
 - 使用边界：原始研究支持其设定范围内的结论，不直接证明本书提出的治理制度已获得普遍实证验证。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第十一章 智能合约：制度规则如何被执行

共同账本为多方提供了可以核验的状态，但共同创造还需要行动。已经有效批准的资源怎样分配，满足条件的权益怎样取得，已经撤销的权限怎样停止使用，都要求制度从记录进入执行。智能合约为其中能够明确表达的一部分规则，提供了按程序处理的能力。

这里讨论的智能合约，是部署在相应执行环境中、按照调用和协议规则处理数据与状态的程序。以太坊开发文档将其描述为位于特定地址的代码与状态，使用者通过交易调用其中的功能。它能够执行被写入程序的条件，但“合约”这一技术名称并不直接证明其构成完整的法律合同，或已经取得约束有关主体的全部依据。Ethereum开发文档：智能合约简介〔1〕

智能合约的制度价值，在于使某些已经明确的承诺减少对临时操作意愿的依赖。要实现这种价值，需要把条款转化为准确条件，为执行提供必要资源，并为裁量、错误和变化保留有权处理的路径。本章沿着这一过程，讨论技术怎样执行制度，以及执行能力本身怎样受到制度约束。

一、从制度条款到条件、权限与状态转换

一项自然语言条款，通常同时包含目标、判断标准和行动要求。程序需要的表达则更加具体：哪些数据作为输入，什么条件成立时允许执行，由谁调用，以及执行后哪些状态发生变化。制度条款进入智能合约，需要完成这两种表达之间的转换。

转换首先需要确定采用对象。倡议、讨论稿和已经生效的规则，不能因为都可以写成程序就取得相同地位。开发者应当能够识别自己实现的是哪个版本，哪些事项已经获得批准，哪些仍待决定。否则，代码中的默认值就可能把尚未解决的制度问题提前固化。

接下来需要明确主体和权限。谁能够提交材料，谁能够确认事实，谁有权批准分配，谁只能执行已经批准的结果，应当分别表达。将这些角色映射为地址、凭据或其他技术权限，还需要保留它们与现实授权的对应关系。程序中的一个管理角色，不应被默认为可以处理全部制度事项。

条件表达需要说明事实怎样进入系统。“贡献得到确认”可能要求有权审核者签署，也可能要求多方核验或异议期间届满。程序能够检查的是这些已经表达的条件，不能自行填补“确认”的含义。若制度需要专业判断，就应当把专业判断的形成程序和结果输入方式一并说明。

数量和时间也需要明确。计算基数、计量单位、精度、取整方式、适用期间及边界时点，都可能改变实际结果。对零值、缺失信息、过期授权和分母为零等情形的处理，也属于规则表达的一部分。技术人员可以指出可能后果，涉及权益的实质选择仍需要有权决定。

状态转换随后表达执行前后有什么不同。提交材料可以使事项进入待审核状态；有效批准可以形成待履行安排；满足支付条件并完成相应转移，才可能更新履行状态。每次转换都需要明确前置条件，防止某个入口跳过必要阶段。

本书将这一转换概括为条款与执行条件的对应关系。

制度条款需要说明的内容	程序需要表达的对象	转换时应当核对的依据
谁可以作出决定	角色、调用权限和授权范围	现实主体、委托关系及有效期间
什么情况下可以行动	前置状态、输入证据和判断条件	条款口径、事实确认及未完成条件
可以使用多少资源	额度、计算方法和可支配资源	预算、资源控制及其他既有负担
行动后产生什么结果	状态更新、资产操作和执行记录	权益内容、义务主体及履行标准
发生错误或争议怎么办	暂缓、复核、纠正和恢复路径	处理权限、证据要求及责任安排

资源条件需要特别检查。合约拥有某项资产的操作权限，与它已经具备足够可用资源，并不相同；记入应付数额，与完成实际支付也不相同。没有可支配资源时，程序可以准确保存尚未履行的义务，却不能通过改变显示状态使义务变成已经履行。

在利益相关者资本治理中，贡献确认也不自动产生全部权益。程序应当分别表达贡献记录、评价结果、资本安排和具体权利。取得收益请求权、获得资源使用权和进入治理程序，可能具有不同条件，不能因为采用同一个积分或凭证，就把它们合并为一种无边界的资格。

执行规则还需要保持一些持续成立的约束。已经完成的同一笔支付不得被重复执行，未获授权的主体不得改变分配对象，已承诺资源与后续可用额度需要相容。这些约束需要覆盖所有相关入口，而不只是正常操作路径。一个被忽略的管理功能或例外入口，也可能改变相同状态。

业务层面的防重复尤其重要。同一请求可以通过不同交易多次到达，交易序号不同也不意味着对应不同义务。合约需要根据明确的业务标识和状态检查，识别某项履行是否已经发生。否则，账本可以正确处理每一笔交易，业务却仍然出现重复支付或重复授予。

条款与代码的对应应当接受审查。审核者需要检查正常条件、边界情况、权限失效和异常输入下的行为，并核对程序结果是否符合已经采用的制度。形式化验证可以对明确写出的规范提供更严格的检查，但证明程序符合规范，不等于证明规范已经完整表达制度意图。Ethereum开发文档：智能合约的形式化验证〔2〕

这一区别要求保留不同层次的验收。制度审查关注规则的依据和后果，技术审查关注实现与明确规范是否一致，部署核验则需要检查实际使用的程序、初始参数和管理权限是否对应已经批准的版本。草案通过讨论、程序通过测试和实际执行安排已经生效，应当分别记录。

代码最终承载的是被准确表达并实际部署的规则。转换过程越清楚，参与者越容易判断程序正在执行什么，也越容易在结果偏离预期时找到原因。智能合约由此成为制度的一种执行形式，而制度仍需为这种形式提供完整的含义与依据。

二、共识确认与合约执行的分工

共识确认和合约执行相互依赖，但承担的工作不同。合约执行根据既定状态、输入和程序计算结果；共识机制则帮助参与者形成可以共同采用的记录与顺序，并按相应规则确认结果。前者回答程序怎样处理一项请求，后者回答多方怎样共同采用相容的处理历史。

这是一种职责分工，不能简单理解为所有系统都先完成共识，再执行程序。在一些架构中，提议者先执行候选交易，其他参与者进一步核验，结果才进入共同确认；另一些架构会先模拟执行和收集背书，再排序并验证。具体阶段取决于系统设计。

Hyperledger Fabric的交易流程说明了后一种安排：交易先经过提议与执行背书，随后进入排序，提交时还需要检查背书策略及有关状态是否已经变化。某次模拟执行成功，不代表它最后一定形成有效的状态更新。Hyperledger Fabric文档：交易流程〔3〕

无论采用何种路径，共同执行都需要明确输入。相同程序若面对不同的前置状态、规则版本或外部数据，可能得到不同结果。系统需要把相关环境条件纳入可共同核验的范围，使验证者能够检查结果来源，而不是仅接受某个执行者声称已经算对。

共识不会纠正程序中已经存在的制度错误。如果程序把批准额度写错，多个节点可以重复得到同样的错误业务结果；如果程序的权限设置过宽，按权限实施的操作也可能通过协议检查。因此，共同确认能够支持结果的一致性，却不能替代对程序及其制度依据的审查。

执行结果也需要与调用结果区分。请求被接收、交易被纳入、调用成功和预期业务完成，并非同一状态。合约可以成功记录一项申请，而申请仍需审核；一个程序调用也可以返回失败状态，而交易本身仍然存在于账本。使用者需要知道成功对应的是哪一步。

在以太坊一类执行环境中，发生相应异常可以撤销当前调用及其子调用中的状态修改，但子调用错误也可能被上层程序捕获并按其他路径继续处理。因此，不能笼统地认为一次局部失败必然撤销整个业务过程。Solidity文档对异常传播、捕获和低层调用的差异作了明确说明。Solidity文档：异常与状态回退〔4〕

这也限定了原子执行的范围。被同一有效事务边界覆盖的一组操作，可以按照相应语义整体成立或撤销；多笔交易、跨网络消息以及现实中的交付，不会自动获得相同保障。程序需要准确处理已经完成的部分和仍待完成的部分，不能把一个局部成功扩张为全部义务完成。

外部动作尤其需要等待适当的确认条件。某个系统观察到合约事件后立即安排不可轻易撤回的履行，如果相关记录随后发生重组，就可能面临记录变化与现实后果不一致。应当在制度中说明后续行动依据何种确认程度，以及出现异常时由谁协调处理。

执行记录本身也需要准确解释。一个事件可以说明程序发出了相应记录，却未必足以证明目标资产实际到账，或链下服务已经交付。核验应当结合实际状态、必要回执和有关证据。记录设计需要让参与者能够追踪结果，而不是只提供一个容易被误解的成功通知。

程序可执行，还需要请求进入相应执行环境。对于通常由交易驱动的链上合约，日期到达不会使它在没有调用的情况下自行醒来。定时服务、使用者或其他程序需要触发相应请求；费用、网络和调用权限也需要可用。“自动”描述的是触发后按规则处理的能力，并不消除触发和持续运行的责任。

这一区别对长期承诺具有实质影响。组织可以把定期释放、到期结算等条件写入程序，但仍需安排谁监测条件、谁提交请求、失败后谁继续处理。将这些工作交给外部服务时，也需要说明服务中断后的替代路径。部署完成之后的运行维护，仍然属于履约基础。

因此，应当分别检验执行正确性、共同确认和履行可达性。执行正确性关注计算是否符合规定，共同确认关注多方是否采用相容结果，履行可达性则关注必要条件具备时，有关主体是否确实能够完成行动。程序永远拒绝越权操作，并不意味着它不会把所有正当请求一起锁住。

对于利益相关者资本治理，三者需要形成连续关系。有效制度提供应当执行什么的依据，程序把可计算部分转化为状态变化，共识机制支持对有关历史的共同采用，组织再使剩余资源和现实责任进入履行。技术分工明确，才能使自动化真正缩短承诺与兑现之间的距离。

三、自动履行、人工裁量与例外处置

自动履行适合那些条件可以清楚表达、输入能够可靠取得、结果能够由系统控制的事项。它可以减少重复操作和执行时的任意拖延，使参与者更容易预期满足条件之后会发生什么。其适用范围应当由这些条件决定，而不能仅以减少人工为目标不断扩大。

制度中也存在需要理解情境的判断。交付是否达到约定质量，某项贡献应当如何归因，延误是否具有可以接受的原因，以及多种利益发生冲突时如何处理，都可能需要专业审查和说明理由。把这些判断压缩为一个数值，可以便于计算，却不保证保留了原制度需要考虑的内容。

因此，可以将执行事项区分为三种关系：条件已经明确且证据具备时按程序处理；需要裁量时交由有权主体作出判断，再把结果输入执行程序；证据不足或争议尚未解决时，保留明确的待处理状态。这种分工使自动化与裁量分别承担适当工作。

人工裁量也需要受到制度约束。谁可以判断，判断哪些事项，需要取得什么材料，是否存在利益冲突，以及结论怎样接受复核，都应当事先说明。技术可以把这些程序条件作为后续执行的前提，防止一条未经适当形成的人工指令直接触发重大变更。

裁量权限需要与事实材料和具体事项对应。审核者对某项履行作出认可，不意味着其可以调整整个分配规则；复核者纠正一项事实，不意味着其可以自行免除其他主体的义务。人工处理越可能改变权益，越需要明确判断范围与理由。

处理结果进入系统时，应当能够关联决定主体、适用规则、证据范围和时间。必要时还应当说明有效期限及后续复核条件。敏感原始材料可以按适当权限保存，但系统应当让受影响者知道决定依据在哪里、通过什么路径提出异议。

例外处置需要区分规则内的例外与规则本身的修改。既有制度已经授权在特定条件下调整履行时间，属于按规则处理；事后增加新的分配依据或改变基本责任，则可能属于制度修订。不能把所有变更都命名为例外，以绕过更严格的决定程序。

暂缓状态可以为调查提供必要空间，但应当限定范围。某一事项发生争议，不应在没有依据的情况下阻断全部无关履行。制度可以研究把待核部分、已确认部分与尚未到期部分分别管理，并说明哪些动作继续、哪些动作等待。暂缓的目的，是防止在关键条件不明时扩大后果。

暂缓也需要有处理责任和复核时点。谁继续收集材料，谁在什么期间作出回应，超期后由谁接手，都影响参与者能否实际获得解决。规定复核期限不必意味着到期后不问原因一律自动放行；它可以触发进一步审查或替代程序，使等待不至于无人负责。

履行资源不足，需要准确表达为未完成或部分完成。系统不能因为可用余额耗尽，就默认相应义务已经消灭；也不能在没有有效依据时自行降低已经成立的请求数额。后续怎样补足资源、调整安排或处理责任，应当进入相应程序。

面对技术错误，程序中的失败状态也不等于业务责任已经终结。调用因网络、费用或程序条件失败，可能只意味着需要在核对后再次处理；如果已经完成部分外部动作，则需要先识别哪些后果仍然存在。重试前应当检查既有记录，避免恢复过程造成重复履行。

纠错可以通过新增的有效操作改变当前状态，并保留原有历史。错误付款后的返还、错误授予后的调整，以及遗漏义务的补充履行，都需要相应权限和资源。确认曾经发生过某个错误，与系统现在能否将其实际后果纠正，仍是两件不同的事。

人工裁量还可能被自动辅助工具支持。软件可以整理材料、发现不一致并提示规则适用问题，但如果某项判断涉及尚未形式化的标准，工具输出不能仅因被写入链上就取得最终决定效力。组织需要说明谁对采用结果负责，以及什么条件下必须进一步审查。

本书据此提出，把裁量的边界本身纳入可执行程序。程序可以检查必要批准是否齐备、判断者是否具备资格、决定是否超出额度及期限，并为异议保留入口；具体判断则由有权主体在这些边界内作出。这样，技术不仅执行确定答案，也支持形成答案的程序。

这一设计仍需接受实际检验。裁量入口可能减少僵化执行，也可能成为绕过规则的通道；自动条件可能提高处理一致性，也可能遗漏重要情境。评价应当关注判断是否更可解释、问题是否得到处理，以及受影响者能否有效使用相关程序。

自动履行、人工裁量和例外处置共同构成制度的执行能力。它们分别处理可计算条件、需要判断的事项和正常路径无法覆盖的情况。将三者衔接起来，才能使共同承诺既具有稳定性，也具备应对现实变化的能力。

四、合约升级、紧急暂停与制度修订

智能合约需要在长期运行中面对错误修复、业务变化和制度更新。参与者既希望既有承诺不被任意改变，也希望严重缺陷能够得到处理。升级与暂停机制因此需要在最初设计时进入权力安排，明确哪些内容可以改变、谁能够启动，以及怎样维护已经成立的关系。

合约升级不必表现为直接改写原有地址中的程序。常见方式包括部署新合约并迁移有关状态，或者通过代理结构，让使用者继续与原入口交互，而实际调用另一份执行逻辑。以太坊的升级文档对这些结构作了区分。地址保持不变，不代表实际执行规则从未变化。Ethereum开发文档：智能合约升级〔5〕

参数变化也可能产生制度上的实质影响。即使程序代码没有改变，调整计算比例、资格名单、到期时间或资源使用上限，也可能改变参与者处境。因此，技术上被称为配置的操作，仍需要按其实际后果判断应当经过何种授权。

升级权限具有较强控制力。能够改变执行逻辑的主体，可能有能力调整资产操作、角色限制和状态解释。日常功能具有严格权限，并不意味着升级入口也受到同等约束。需要一并检查代理管理、角色授予、参数修改和外部依赖替换等能够改变实际行为的路径。

制度修订则回答这些技术变化凭什么可以发生。修复实现偏差、调整既有授权范围内的参数、改变权益规则和迁移长期安排，可能需要不同程序。开发者判断某项修改是修复，并不足以自动证明它不影响权益；其判断需要有明确的旧规则、新行为和影响说明支持。

本书主张，重要变化应当分别识别以下权限。

变化类型	主要作用	需要说明的授权与限制
紧急暂停	暂时限制特定操作，控制进一步影响	触发条件、适用范围、处置责任与复核时点
恢复运行	重新开放被限制的操作	故障处理依据、验证结果及恢复权限
参数调整	在现有逻辑内改变具体执行条件	可调整范围、生效期间及权益影响
逻辑升级	改变后续调用采用的程序行为	有效批准、版本对应和状态兼容要求
制度修订或迁移	改变规则依据或执行载体	修改权限、新旧关系衔接及异议处理

紧急暂停的技术能力应当准确表达。OpenZeppelin的暂停模块要求把相应检查实际接入需要控制的功能；仅引入模块，并不会使所有功能自动受到暂停限制。暂停能阻止什么，取决于具体执行路径，而非界面上是否存在一个暂停按钮。OpenZeppelin文档：Pausable〔6〕

暂停通常也不会撤销已经完成的交易，更不会自动冻结其他系统中的全部行动。在链上执行的暂停请求，本身仍需被网络处理，不能保证一定先于其他竞争请求生效。组织需要根据实际覆盖范围制定处置安排，避免把暂停能力当作可以消除任何后果的保证。

暂停权与恢复权可以分别设置。发现风险时迅速限制特定操作，和确认处理充分后恢复运行，需要的信息与判断可能不同。但权限分开之后，也需要避免无人能够完成恢复，或者任何一方可以无限期阻断处理。运行责任、替代路径和复核安排应当同时明确。

暂停的范围尤其需要与风险对应。可以研究限制新增承诺、限制某类资产操作或只暂缓争议部分，而保留必要查询和申诉渠道。是否继续允许领取、撤回或其他动作，应当结合漏洞与义务关系判断，不能预设所有情况下全面冻结或全面开放都适当。

对常规升级，延迟执行可以提供检查变化的时间。OpenZeppelin的时间锁安排，将已排定的操作置于最低等待期间之后执行，为使用者审查提供机会。但时间经过不会自动使修改取得正当性；参与者是否能够理解变化、提出异议或实际退出，还取决于具体制度与资源条件。OpenZeppelin文档：延迟操作与时间锁〔7〕

延迟机制还需要覆盖真正能够改变结果的权限。如果管理者可以通过另一入口直接升级、替换管理者或绕过延迟，表面等待期就可能失去预期作用。相反，所有关键角色都失去操作能力时，严格的权限结构也可能阻断必要维护。因此，共同控制应当同时考虑防止滥用与持续履职。

新旧版本之间最重要的是状态和责任的衔接。已经取得的权益、尚未完成的义务、正在处理的申报以及已提出的异议，需要分别确定适用规则。不能仅因新算法上线，就默认旧规则下已经形成的全部关系失效；也不能让新旧系统同时把同一项未结义务重复当作可履行余额。

状态迁移需要核对主体对应、数量、单位、状态含义和处理位置。旧系统何时停止有关操作，新系统从哪个依据继续，迁移失败时如何处理，都应当明确。即使采用保持原状态的代理升级，也需要检查新逻辑是否按同样含义读取已有数据，避免记录仍在而解释发生无意变化。

验证需要围绕这些实质后果展开。权限变化是否符合批准，既有权益是否按安排延续，边界情况下是否发生重复处理或永久阻断，以及实际部署是否对应审查版本，都是重要检查对象。一次技术测试通过，不能替代制度批准；一项制度批准，也不能证明实际部署没有偏差。

升级完成后的结果还需要可以追踪。参与者应当能够识别当前规则和程序版本、变更依据、生效位置及尚待处理事项。界面更新、部署完成和迁移核对结束属于不同进展，准确表达这些状态，有助于继续核验共同承诺。

智能合约的长期可靠性，由执行规则和约束执行权力的规则共同支持。它可以使确定条件下的行动更加稳定，也需要让裁量、暂停和修订始终具有清楚依据。下一章将转向现实连接，进一步讨论事实、证据和履行结果怎样进入链上制度，使程序所处理的状态能够与共同创造的实际过程衔接。

定稿补强：升级不变量与应急权限

规则经过有效治理程序批准，并不保证技术升级一定正确。合约升级至少要保持六类不变量：权利和义务的语义不被无意改变，接口对既有调用保持明确兼容，存储布局与状态迁移可验证，权限不会在迁移中扩大，账实余额能够前后勾稽，历史证据和版本关系可以追溯。任何不能保持的不变量都应在提案中列为显式变更，而不能隐藏在部署细节里。

升级流程应包含代码或配置审查、测试、迁移演练、时间锁、受影响主体通知、部署人和批准人分离、迁移前后快照、失败停止条件和撤销证明。所谓回滚也要说明边界：程序版本可以恢复，已经发生的外部付款、现实交付或第三人权利未必能够自动回到原状。

紧急暂停是限制损失的工具，不是无限期治理授权。其触发证据、作用范围、最长时间、续期门槛、事后追认、补偿和恢复后的权限撤销，应与升级规则一起公开。

本章注释

1. [SRC-038] Ethereum.org：Ethereum开发文档：智能合约简介。[原文或官方页面](#)
 - 本章引证：Ethereum开发文档：智能合约简介。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：以太坊智能合约文档、Ethereum开发文档：智能合约简介。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
2. [SRC-039] Ethereum.org：Ethereum开发文档：智能合约的形式化验证。[原文或官方页面](#)
 - 本章引证：Ethereum开发文档：智能合约的形式化验证。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum开发文档：智能合约的形式化验证。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
3. [SRC-050] Hyperledger Fabric：Hyperledger Fabric文档：交易流程。[原文或官方页面](#)
 - 本章引证：Hyperledger Fabric文档：交易流程。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Hyperledger Fabric文档：交易流程。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
4. [SRC-021] Solidity Documentation：Solidity文档：异常与状态回退。[原文或官方页面](#)
 - 本章引证：Solidity文档：异常与状态回退。
 - 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：Solidity文档：异常与状态回退。
 - 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
 - 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。
5. [SRC-040] Ethereum.org：Ethereum开发文档：智能合约升级。[原文或官方页面](#)
 - 本章引证：Ethereum开发文档：智能合约升级。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum开发文档：智能合约升级。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。

◦ 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

6. [SRC-019] OpenZeppelin：OpenZeppelin文档：Pausable。[原文或官方页面](#)

- 本章引证：OpenZeppelin文档：Pausable。
- 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：OpenZeppelin文档：Pausable。
- 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
- 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。

7. [SRC-016] OpenZeppelin：OpenZeppelin文档：延迟操作与时间锁。[原文或官方页面](#)

- 本章引证：OpenZeppelin文档：延迟操作与时间锁。
- 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：OpenZeppelin文档：延迟操作与时间锁、OpenZeppelin：访问控制与角色权限、OpenZeppelin：角色与访问控制。
- 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
- 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第十二章 现实连接：链上制度如何对应链下事实

链上的规则可以准确处理输入，却不能自行观察全部现实。交付是否完成，服务是否达到约定要求，某项材料由谁形成，以及一项长期能力是否仍然存在，都需要从共同创造的实际过程取得依据。制度技术进入现实，必须建立从事实到证据、从证据到判断、从判断到状态的联系。

这种联系不只是数据传输。信息由谁采集，采用什么口径，经过哪些核验，原始材料怎样保存，以及谁能够在必要时提出反证，都会影响链上结果是否值得依赖。链上执行越能直接触发权益变化，输入过程就越需要明确的责任与审查条件。

本章讨论这种连接的四个方面：外部信息怎样成为程序输入，实物与服务怎样获得适当核验，证据怎样在链下保存并与链上状态关联，以及参与者如何在不过度披露的条件下证明必要事实。它们共同决定，技术维护的状态能否持续对应现实中的对象、行动与责任。

一、预言机、业务证据与信息输入责任

预言机是连接链下信息与链上程序的一类机制。它可以从业务系统、设备、信息服务或人工确认中取得材料，再按规定方式把结果交给合约使用。以太坊开发文档将预言机描述为使外部信息可供链上合约使用的应用及相应组件。其作用是建立信息接口，名称中的“预言”并不意味着预测未来或天然掌握真相。Ethereum开发文档：预言机〔1〕

需要这种接口，是因为共同执行要求输入能够被确定地采用。如果不同节点在执行同一请求时，各自读取随时变化的外部页面，就可能得到不同结果。预言机把特定来源、时间和处理方式下的信息表达为共同可使用的输入，使节点能够据此执行同一规则。

输入得到统一，首先改善的是执行依据的一致性。原始信息是否准确，仍然取决于来源和形成过程。一个经过有效签名的数据值，可以证明有关密钥对该内容作出了签署，却不能单凭签名证明设备测量正确、填报者没有遗漏，或者材料已经得到适当解释。

因此，需要区分信息来源、采集方式、处理过程与提交结果。来源说明原始信息从何处取得，采集方式说明它怎样被观察或记录，处理过程说明采用了哪些筛选、换算和汇总，提交结果则是合约实际接收的内容。每一步都可能引入变化，也各自需要能够说明的责任。

业务证据为这种说明提供基础。它可以包括原始交付材料、双方确认、设备记录、验收意见和有关过程文件。但一项材料能够支持什么结论，需要结合其形成目的判断。为安排工作而生成的日志，未必足以独立证明全部工作质量；一份付款记录，也未必能够说明付款所对应的义务已经完整履行。

结构化输入应当保留必要语境。事项标识、来源主体、发生时间、采集时间、计量单位、适用期间和规则版本，可能共同影响一个数值的含义。不同时间不能随意混用，不同口径也不能因为数值形式相同就直接合并。程序接收到的简洁结果，需要有可以返回其依据的路径。

新鲜程度也是输入有效性的条件。某项信息在形成时真实，不表示今天仍然适合用于执行。权限、资源状态和履行进展都可能变化，制度应当明确更新频率、最长适用期间和过期后的处理。网络没有取得新数据时，不能在没有明确依据的情况下，把旧值持续呈现为当前有效值。

多来源机制可以支持交叉检查，但独立性需要核实。多个提交者若读取同一个底层来源，实际并没有形成同等数量的独立观察。汇总和多数选择可以处理某些错误，却也可能共同接受同源偏差。来源数量、运营者数量和独立证据数量应当分别表达。

汇总规则本身也具有制度意义。选择哪类来源，排除哪些异常值，怎样赋予权重，以及差异超过什么程度时暂停采用，都会影响最终输入。修改这些规则可能改变资产操作或权益结果，因而需要按照其实际影响确定授权，不能一概作为普通数据维护处理。

本书将输入过程中的主要责任作如下区分。

环节	主要责任	需要保留的核验依据
原始观察与采集	按约定范围取得材料，说明局限与异常	来源、对象、时间、方法及原始记录
整理与转换	保持含义，准确完成换算和关联	处理规则、版本及前后对应关系
审核与判断	在授权范围内核实事实并说明结论	审核资格、证据范围及判断理由
提交与更新	将确定结果按规定条件交给系统	签署、提交状态、有效期间及更正记录
采用与执行	检查输入是否满足当前使用条件	来源权限、时效、用途和异常处理规则

责任可以由同一主体承担，也可以分工，但不应因分工而留下空白。技术服务商准确转发信息，与业务审核者对事实作出确认，属于不同工作。出现错误时，需要回到具体环节，识别是原始观察不足、转换失误、判断偏差，还是采用了已经失效的数据。

输入失败也需要有明确状态。未收到信息、材料相互矛盾和已经核实不符合条件，不能统一处理为同一种否定结果。系统可以等待补充、请求复核或限制相关操作，但应当说明当前缺少什么，以及谁继续负责处理。

纠正输入时，需要同时检查已经发生的后果。更新一个数据值，不会自动返还此前支付的资源，也不会使已经执行的外部动作自然恢复。新的记录应当关联原有事项，并由有权程序决定是否调整后续状态、补充履行或处理责任。

预言机由此成为一种受到制度约束的信息入口。它使外部信息能够进入共同计算，而业务证据和输入责任使这些信息具有可审查的来源。两者结合，才能避免把稳定传输误认为已经完成事实判断。

二、实物、服务与履约结果的核验

现实对象进入链上制度，首先需要解决指向关系。一个记录标识究竟对应哪件物品、哪批资源、哪项服务或哪个履行阶段，应当能够识别。指向关系不清，后续记录即使保持完整，也可能始终没有指向各方实际关心的对象。

实物标识可以通过编号、标签、封装或其他方式建立，但标识与对象的绑定仍需维护。标签可能被复制或转移，对象也可能在保管和交接中被替换。能够读取同一标识，只说明读取结果一致；它是否仍然附着于同一对象，需要相应检查。

对象还可能发生拆分、合并、加工或损耗。制度应当说明这些变化怎样进入记录，以及原有标识与后续对象如何关联。把不断变化的现实对象固定为一个永远不变的链上名称，可能掩盖数量、性质和可用状态的变化。

核验需要沿着保管与交接过程展开。谁在什么期间实际控制对象，交接时检查了什么，数量与质量差异怎样记录，以及接收者认可的范围是什么，都可能影响后续责任。某次扫码或登记不能自动替代这些具体过程。

设备能够扩大观察范围，但仍有自己的边界。设备身份认证可以帮助识别数据来自哪个设备，无法单凭这一点保证安装位置正确、测量对象没有变化或设备保持适当状态。采集范围、校验、维护和异常处理，应当与设备记录一起进入核验设计。

抽样和全面检查也应当分别表达。抽样可以在适当设计下为一定判断提供依据，却不意味着逐件核实了所有对象。制度需要说明样本怎样取得、结论适用什么范围，以及出现异常后是否扩大检查。证据的强度应当与所声称的结论相匹配。

服务核验通常具有另一类困难。活动持续了多长时间、提交了多少材料和发生了多少次交互，可以提供过程信息，但未必直接说明服务质量。需要区分投入、交付、被接受、实际使用和使用结果，使不同阶段分别获得适当证据。

这种区分对共同创造尤其重要。工作成果已经交付，使用者可能尚未采用；成果被采用之后，其效果也可能受到其他投入和环境变化影响。有关贡献可以得到认可，但对长期价值的归因仍需说明方法，不能把一份即时验收记录扩张为对全部未来结果的确定证明。

验收本身也需要有明确权限和范围。接收材料的人不一定有权确认质量，负责技术核验的人也不一定有权调整报酬或免除义务。制度应当说明确认者正在认可什么，以及哪些条件尚未完成。签名越容易触发后续执行，这些范围越需要清楚。

利益冲突会影响判断条件。交付者自报、交易对方确认和独立复核，各有可以提供的证据，也各有局限。增加确认人数有时能够改善检查，但若所有确认者都依赖同一利益安排，也需要保留其他复核路径。程序应当支持对不利材料和相反意见的认真处理。

核验不应预设所有事项都只能得到完全通过或完全失败的结论。部分完成、符合某些要求、存在待补事项和结论有争议，都可能更准确。把这些状态表达清楚，有助于组织安排部分履行、补充工作和进一步审查，而不是被一个过度简化的开关限制。

履行结果还需要与义务内容对应。链上资产转移可以核验一定范围内的转移状态，实物交付和服务完成则需要相应外部材料。付款完成、收货完成、质量验收与责任终结，各自可能具有不同条件。任何一个技术回执都不应被赋予超过其证明范围的含义。

同一现实事项也可能形成多条记录。不同部门、不同协作者和不同系统可能各自记录其所见。链上标识可以帮助关联，但重复事项的识别仍需要业务口径。既要防止同一义务被重复履行，也要避免把多人分别作出的贡献误判为同一条应当删除的记录。

没有找到记录，也不必然说明行为没有发生。可能是采集范围有限、材料遗失或某个主体没有履行记录责任。判断缺少材料的后果时，需要结合事先的记录义务、现实取证条件和其他证据，不能让控制信息入口的一方仅凭记录缺失否定他人的全部主张。

本书主张，让核验结论同时表达对象、范围、依据与尚存不确定性。链上可以保存简洁的状态，链下则保留必要材料及复核路径。这样，实物和服务无需被假定为完全数字化，也能够与共同账本建立可以持续检查的联系。

三、链下存储、链上凭证与数据可用性

现实协作产生的材料，往往比共同账本需要处理的状态丰富得多。原始文件、检测数据、工作记录和交付材料可能持续增长，其中还包含个人信息、商业秘密以及与共同确认无关的内容。制度技术需要决定哪些信息必须共同验证，哪些材料应由适当主体保管，哪些内容只在争议或审查时提供。

一种可以采用的分工，是在链下保存较完整的业务材料，在链上记录材料标识、完整性校验值、必要的签名、版本关系以及确认状态。共同账本负责固定某些可共同核验的联系，存储系统负责让相应材料在需要时能够取得。两者通过明确的引用规则衔接，才能支持持续复核。

这种安排首先需要区分完整性、可取得性与可理解性。完整性回答取回的材料是否与此前承诺的内容相符；可取得性回答有权访问的人能否在所需时间取得材料；可理解性回答材料是否具有足够的格式说明、业务背景和解释条件。三个问题分别得到满足，记录才可能成为持续可用的证据。

哈希值不能替代原始材料。核验者通常需要取得相应内容，再按约定的方法计算和比较，才能检查内容是否匹配。如果原始材料已经丢失，一个留在链上的哈希值通常无法将其恢复。它可以继续标识此前承诺的内容，却不能独自承担展示事实、解释过程和支持复核的全部任务。

文件的读取地址与内容承诺也应当分别处理。同一个地址可能在不同时间返回不同内容；同一份内容也可能被保存在多个地址。制度需要规定如何根据版本和校验值识别正确材料，如何迁移读取位置，以及如何发现引用失效。否则，链上记录虽然仍然存在，其指向的依据却可能已经发生变化。

链上凭证还需要表达出具者究竟证明什么。出具者可能确认材料已经接收，也可能确认审查已经完成，或者确认某一资格在特定期限内有效。这些声明具有不同含义。可验证凭证可以支持对出具来源和内容完整性的密码学检查，但接收者仍须判断是否信任该出具者对有关事项作出的声明，以及声明是否满足本次业务要求。凭证的这种作用并不以全部内容上链为前提。W3C：可验证凭证数据模型 2.0〔2〕

保存责任不能被“分布式存储”几个字代替。以 IPFS 为例，内容寻址有助于按照内容标识取回数据，但网络中的缓存可能被清理；固定保存可以使相应节点保留内容，持续保存仍需要实际运行的节点和资源投入。采用某种存储协议，本身并不构成永久保存承诺。IPFS：持久化、固定保存与垃圾回收〔3〕

因此，组织应当把保存期限、保管主体、备份安排、费用来源和迁移条件写入实际制度。不同材料不必具有相同期限，但期限应与所支持的业务、复核和争议处理需要相协调。委托外部机构保存时，也需要安排服务终止后的交接；负责人员离开时，则需要确保资料和必要权限能够有序移交。

区块链协议所讨论的数据可用性，有其特定技术对象：参与者需要能够获得验证区块等操作所必需的数据。相关机制着眼于使验证所需数据可获得，不能据此推断全部业务档案已经获得长期保存保障。Ethereum：数据可用性〔4〕

这里存在两个不同层次的责任。网络可能已经满足协议规定的的数据可用性条件，而一份链下验收材料仍无人保存；业务机构也可能保存了完整档案，而某个网络参与者无法取得验证所需的数据。技术选型应当明确各层保障的对象和时间范围，避免用其中一层的承诺遮蔽另一层的缺口。

材料仍在服务器上，也不等于材料能够用于复核。加密密钥丢失、权限配置错误、文件格式无法读取或必要说明缺失，都可能使保存流于形式。有效保管应当包含必要的恢复与读取检查，并保留证明材料对应哪个事项、哪个版本和哪次确认的联系。

可取得性还必须说明取得者的范围。公开验证某个链上状态，不意味着所有参与者都应当下载支撑该状态的全部私人材料。对于不同事项，可以分别提供原始材料、经授权的查阅、有限字段或满足条件的证明。数据可用性的组织含义，应当是适当主体能够为适当目的取得必要内容，而不能简单等同于无差别公开。

错误材料需要纠正时，原记录与后续状态之间也应当存在清楚的关系。新材料可以补充原材料，新的判断可以撤销先前确认，凭证可以到期或被撤销。历史上曾经存在某项声明，与该声明目前仍可作为执行依据，是两件不同的事。系统必须让采用者能够查询必要的当前状态，而不能只验证一份旧凭证的签名仍然正确。

长期保存也不意味着无限期保留一切。收集范围、保存期限与删除安排需要相互协调。对于可以公开复制的链上内容，不能承诺依靠删除某个本地副本就让所有副本消失；这更要求组织在记录之前慎重确定公开内容。撤销访问权限通常只能约束后续访问，不能保证收回他人已经取得的信息。

利益相关者资本的形成具有跨期性，支持权利主张的材料也就可能跨越人员、系统与服务商的更替。只有某一时点上传成功，远不足以支撑这种连续性。本书据此主张，记录保存应当作为持续履行的组织义务：定期检查材料能否取得、能否正确解释、能否与当前主张对应，并为必要的更换保管主体保留条件。

如果形成权利主张的人始终无法接触支持自身主张的必要依据，共同记录便可能形成新的信息依附。链上可见性与链下访问安排应当共同服务于当事人的知情、核验和申诉能力。制度技术的价值，也体现在参与者能否在长期合作中持续使用证据，而不仅是某个系统曾经成功接收过数据。

四、隐私保护、选择性披露与零知识证明

共同治理需要证据，也需要保护参与者不被过度观察。员工、客户、供应商和合作伙伴可能需要证明资格、履行义务或提出贡献主张，但这些需要并不自动授权组织收集其全部活动。若参与共同创造必须以持续公开个人生活和商业关系为代价，记录能力的增强便可能转化为对参与者的控制。

隐私设计应当从需要作出的判断开始。一个确认程序究竟需要知道什么，哪些信息会改变判断结果，哪些主体承担判断职责，这些问题先于具体技术。业务核验者、分配执行者、争议处理者和一般参与者可能需要不同范围的信息。把这些需要区分开，才有可能减少无关数据的流转。

加密、选择性披露与零知识证明可以支持不同程度的信息保护，但各自解决的问题并不相同。加密主要限制谁能够读取内容；选择性披露允许在支持相应能力的凭证机制中出示必要属性；零知识证明则可以使验证者检查某个明确命题是否得到满足，而无需取得被保护的秘密输入。实际制度可以组合使用这些方法。

技术安排	主要支持的能力	仍需另行解决的问题
加密与访问控制	限制原始内容的读取范围	密钥保管、授权变更及获准读取后的使用责任
选择性披露	出示必要属性并保留相应可验证性	凭证来源、属性关联与披露范围是否合适
零知识证明	核验约定条件，同时保护秘密输入	条件是否完整、输入依据是否可信及证明使用范围

选择性披露的制度意义，是让一次核验只取得此次必要的信息。凭证包含的全部内容不必总是整体提交。但这种能力需要相应的凭证和密码学机制支持，不能通过任意删除普通签名文件中的字段自动获得。还需要防止从不同凭证中拼接属性，制造原本不存在的资格或关系。W3C：可验证凭证中的选择性披露与隐私考虑〔2〕

零知识证明进一步允许把核验对象从某些原始属性转向明确条件。证明者持有秘密材料，双方知道需要检验的关系，验证者接收证明并检查该关系是否满足。制度可以要求证明某项数值达到门槛，而不披露具体数值；也可以在适当构造下，证明持有合格出具者签发的有效资格，而不公开资格材料中的所有信息。

这类证明通常以完备性、可靠性和零知识性描述其目标：符合条件的诚实证明能够通过；不符合条件的主张难以伪造为有效证明；验证过程不会泄露超出约定公开信息及命题成立所必需的秘密信息。具体保障取决于证明系统的安全假设及正确实现。Ethereum：零知识证明〔5〕

这里最关键的制度问题，是究竟证明了什么。若证明只表明某组输入经某个公式计算得到某个结果，它并不自动证明输入来自真实履约，也不证明公式体现了正当分配原则。证明可以严密地验证一个狭窄命题，组织仍需要判断这个命题是否足以支持相应行动。

因此，需要将可信来源与必要条件纳入核验关系。依赖资格凭证时，可能需要检查出具者是否被认可、签名是否有效、资格是否处于有效期限，以及适用的撤销状态。需要确认由特定持有人行使资格时，还必须有相应的持有或授权绑定。缺少这些条件，一个数学上有效的证明仍可能被用于不适当的业务判断。

同样，证明应当与使用场景衔接。针对一次申请产生的证明，是否能够被再次使用，是否能够被转交他人，以及是否只对某个事项有效，都需要明确定义。防止重复申领时可以采用限定用途的唯一标记，但其范围应当经过设计，避免将本来可以分离的活动变成可长期关联的个人轨迹。持有一个凭证，也不自动证明其背后是全系统唯一的自然人。

零知识性并不意味着整个应用不泄露信息。公开命题本身可能具有敏感性；地址、访问时间、交易频率和重复出现的标识也可能使活动相互关联。某次证明隐藏了原始材料，仍需检查公开输入和周边操作暴露了什么。使用外部服务生成证明时，还应明确该服务是否需要接触秘密材料，不能把链上看不到内容误认为任何第三方都没有看过。

哈希也不能直接承担全面的保密功能。对可能取值很少的信息，观察者可能通过枚举候选值并比较哈希进行猜测。需要隐藏又允许日后核验的信息，应当选用适当的密码学承诺或其他保护机制，并处理随机量和密钥的保管问题。把个人信息换成一串字符，不足以单独证明隐私已经得到保护。

隐私保护与责任追溯可以在明确权限下共同设计。一般核验可以只接收必要证明，发生争议时则由具有相应职责的主体依据既定程序查阅必要材料。查阅范围、理由、记录和后续使用应当受约束。保护隐私不要求所有材料立即销毁，追究责任也不要求所有人随时掌握全部材料。

对于利益相关者资本治理，这种分工尤其重要。贡献的确认可能需要工作证据，分配执行可能只需要已经成立的权益数额，治理参与可能只需要有效资格及相应权限。三个环节不必都获得全部原始活动记录。与此同时，贡献被确认、资本安排成立、收益请求形成和治理权可以行使，仍然应当分别满足各自制度条件，不能由一个“已通过”的证明统一替代。

技术复杂性本身也会形成参与门槛。生成证明所需的设备、费用和操作能力，可能影响不同主体能否实际行使权利。制度需要提供适当协助与复核路径，检查错误拒绝、材料补充和系统失效如何处理。因技术困难无法生成证明，与不具备实际资格，应当保留可区分的处置方式。

面向未来，本书提出一个需要实践检验的制度设计方向：让共同治理更多围绕“足够支持本次行动的可核验命题”组织信息流动。不同主体在各自职责范围内验证必要条件，减少为每一次合作重新集中收集完整档案的需要。它的成效应当由信息暴露是否减少、核验是否可靠、参与是否便利以及争议是否仍能处理来检验，而不能仅凭采用了先进密码学就宣告成功。

这种方向仍然需要清楚的社会基础。谁有权出具材料、什么条件构成有效资格、什么主张应当获得救济，都来自组织和社会对关系的安排。密码学可以帮助准确执行其中一部分信息规则，也可以使越权取数更困难，却不能自行决定应当赋予谁怎样的权利。

至此，制度进入技术系统的基本联系已经展开：密码学支持授权与证据检查，分布式账本和共识机制形成共同状态，智能合约执行明确规则，现实连接则为这些规则提供具有来源、责任和使用边界的信息。任何环节的有效性，都需要其他环节提供相应条件。

接下来，问题将转向共同创造本身。组织需要识别参与者及其关系，记录承诺与行动，形成可复核的贡献判断，并依据适当制度连接资本与权益。技术已经提供了建立这些联系的工具；怎样让联系准确、公平并能够长期维持，将成为下一篇的中心。

定稿补强：三类可用性、预言机威胁与隐私责任

“数据可用”需要分成三个问题。协议数据可用性关心验证者是否能取得重建或验证状态所需的数据；证据可取回性关心授权主体能否在保留期内取得支持某项事实和决定的材料；业务连续性关心组织能否在故障、迁移或服务中断时继续履责。三者的对象、负责人、恢复目标和缺失后果应分别记录。

预言机和其他跨域输入应接受独立威胁建模。需要检查来源之间是否真正独立，数据是否具有明确时间戳和新鲜度，聚合阈值能否抵抗操纵，来源停机或分歧时系统如何降级，以及自动执行是否允许人工复核。多个接口若最终依赖同一数据库或同一运营者，数量增加并没有消除同源风险。

隐私保护也不能仅由加密或零知识证明概括。实施方案应说明处理目的、必要字段、责任角色、访问与更正、保留和删除替代、跨境或第三方处理、泄露处置及主体救济。链上只保存必要凭证和状态，将可更正、可删除或高度敏感的原始材料放在具有明确责任的链下系统，是一种常见方向；是否充分仍取决于适用法域和具体数据流。

本章工具与图表

本章的制度关系可结合[附录六](#)、[附录九](#)、[附录十二](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

图12-1 交易、共识、合约与链下事实的责任边界

状态正确不等于事实真实；自动执行也不免除输入、授权与救济责任



《区块链——利益相关者资本论的底层技术》V1.0 · 可编辑SVG

图12-1 交易、共识、合约与链下事实的责任边界

图12-1 交易、共识、合约与链下事实的责任边界。状态正确不等于事实真实；自动执行也不免除输入、授权与救济责任

本章注释

1. [SRC-037] Ethereum.org：Ethereum开发文档：预言机。[原文或官方页面](#)

- 本章引证：Ethereum开发文档：预言机。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum开发文档：预言机。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-076] 万维网联盟（W3C）：Verifiable Credentials Data Model v2.0。[原文或官方页面](#)

- 本章引证：W3C：可验证凭证数据模型 2.0；W3C：可验证凭证中的选择性披露与隐私考虑。
- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：W3C：可验证凭证数据模型 2.0、W3C：可验证凭证中的选择性披露与隐私考虑、W3C：可验证凭证的参与角色与验证边界、W3C：可验证凭证的验证与业务判断、W3C：可验证凭证与数据最小化。
- 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

3. [SRC-015] IPFS Documentation：持久化、固定保存与垃圾回收。[原文或官方页面](#)

- 本章引证：IPFS：持久化、固定保存与垃圾回收。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：IPFS：持久化、固定保存与垃圾回收。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

4. [SRC-035] Ethereum.org：数据可用性。[原文或官方页面](#)

- 本章引证：Ethereum：数据可用性。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum：数据可用性。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
5. [SRC-043] Ethereum.org：零知识证明。[原文或官方页面](#)

- 本章引证：Ethereum：零知识证明。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum：零知识证明。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第三篇 贡献确认：共同 创造如何成为可核验的记 录

第十三章 利益相关者身份与关系建模

共同创造首先发生在人与组织之间。技术系统可以记录一次提交、一次签名或一次转移，但在据此确认贡献之前，仍然需要回答：行动涉及谁，行动者以什么身份参与，代表自己还是代表他人，以及这次行动处于怎样的协作关系之中。如果这些问题没有得到处理，完整的记录也可能把贡献归给错误的主体，把组织行为归给经办人，或者把一个账户拥有的操作能力误认为其背后的制度权利。

上一章讨论现实事实怎样形成能够核验的输入。本章进一步讨论这些事实怎样与参与者及其关系对应。身份建模为记录提供明确的主体指向，关系建模则说明主体之间在特定事项、期间和规则下怎样连接。二者共同为承诺、贡献确认、资本形成和责任追溯提供基础。

本书主张，利益相关者身份应当围绕共同创造中的具体关系建立。模型既要保持主体的连续性，也要容纳角色和授权的变化；既要能够发现冒用与重复主张，也要允许合理的多重身份和隐私保护。它的目标，是让参与者能够被准确地承认，让行动能够被适当地归属。

一、自然人、组织与代理关系

主体是制度安排中被识别、承接行动和权利义务的对象。在利益相关者资本治理中，自然人与组织是两类基础主体。自然人可以投入劳动、知识和其他资源，也可以代表组织工作；组织可以安排协作、承担承诺并持续管理共同形成的能力。模型需要表达这两类主体的联系，同时保留各自的边界。

数字标识承担的是指向功能。姓名、组织名称、内部编号和链上地址都可以帮助识别对象，但其含义不同。名称可能重复或发生变化，地址可能由多人共同控制，也可能在不同期间由不同人员操作。把一个地址直接设置为现实主体的全部身份，会使控制方式的变化被错误地理解为主体本身的变化。

在技术标准中，这种区分也有明确表达。W3C 的去中心化标识符规范区分标识所指向的主体与控制该标识相关文档的控制者，两者可以相同，也可以不同。控制者能够管理有关验证方法，并不能仅凭这一点说明其就是被标识的自然人或组织。W3C：去中心化标识符的主体与控制者〔1〕

因此，一个适当的模型至少需要区分现实主体、系统标识、操作账户和验证密钥。主体可以关联多个账户，账户可以按用途配置不同密钥，密钥也可以被更换。每项关联都需要有建立依据、适用范围和变更记录。保持这些层次的可区分性，才能使账户迁移与密钥恢复不必重新制造一个“新人”，也不致悄然转移原有身份所关联的主张。

主体识别的充分程度，应当由需要处理的关系决定。公开提交一般意见，可能只需要一个能够持续联系的标识；代表组织确认重大义务，则需要核实组织指向、代表资格和授权范围。所有参与都要求同等强度的身份材料，会增加不必要的负担；对重要行动仅核验账户控制，又可能留下实质性缺口。

组织身份尤其不能停留在名称层面。需要明确记录指向的是哪个组织、哪个内部单位或哪个协作集合，并说明其与承诺承担者的联系。部门、项目组和临时联盟可以成为业务记录对象，但不能因为系统给它们分配了编号，就预设它们具有相同的独立承担能力。涉及法律主体资格与对外责任时，还需要依据组织文件及适用制度另行判断。

内部层级也不应被自动解释为外部代表权。一个人属于某个部门，部门属于某个组织，只能先说明隶属关系。是否能够代表组织接受交付、修改约定或处分资源，还要有相应授权。系统可以沿层级查找授权依据，却不能把每一条组织结构上的连接都当作权限传递。

代理关系由此成为身份模型的独立部分。它说明谁授权谁，在什么事项、期限和条件下，以谁的名义行动。有效的代理记录应当能够回答授权从何而来、允许哪些操作、有哪些限额、是否需要共同批准，以及代理人是否可以进一步委托他人。这些内容使“代表组织”成为可检查的制度关系。

模型对象	主要回答的问题	不宜直接推导的结论
主体	记录和主张指向谁	主体必然控制某一特定账户
账户与密钥关联	当前请求通过什么控制方式发起	控制者拥有全部相关权益
组织隶属关系	谁属于哪个组织或单位	成员具有全部对外代表权限
代理授权关系	谁能够代表谁完成哪些行动	代理人取得被代理人的资产或贡献
事项与期间	关系在什么范围和时间内适用	一次成立便永久、普遍有效

代理还需要保持行动者与被代表者的双重指向。经办人提交材料，是一次实际操作；该材料是否构成组织的正式声明，需要结合代理关系确认。贡献由谁作出、谁负责验收、谁代为上传，也应分别记录。代为上传不意味着取得贡献，代为收取不意味着成为最终受益者。

多级代理应当能够向上追溯到被认可的授权依据。本书建议，后续委托的权限不得超过上一级在相应范围内可以授予的权限，并明确期限、再委托限制和撤销的影响。技术上能够生成一份签名授权，只说明授权内容被签署；是否有权签发这份授权，仍须回到授权链及其制度依据。

共享账户容易使这种联系模糊。多人使用同一套密钥时，一次签名通常不足以区分实际操作人。组织可以在适当范围内采用个人操作凭证与组织账户相结合的安排，记录经办、审批和最终提交的不同环节。多人签署也应当说明各自确认的内容，不能把签名数量直接当作责任已经合理分配的证明。

自动化程序同样应当进入代理与控制模型。程序可以在授权范围内提交材料、执行任务或生成记录，但其运行标识需要关联部署者、授权者和必要的监督责任。为程序分配身份，不等于赋予其独立法律人格、资本所有权或最终裁决权。有关人与智能体共同创造的进一步安排，将在后续章节专门讨论。

主体的连续性也不意味着关联关系永远不变。人员更替、组织更名和系统迁移，需要区分哪些只是标识变化，哪些涉及实际承接主体变化。模型应当保留有依据的前后联系，避免通过改名逃避追溯，也避免因名称相似就合并本来不同的主体。此处需要维护的连续性，是经过核验的制度联系。

身份与代理建模由此为共同创造建立了最初的归属秩序。系统不仅识别“谁进行了操作”，还能够检查“这次操作应当按谁的行动理解”。这种区分越清楚，后续贡献确认和责任判断就越少依赖含混的账户标签。

二、员工、客户、供应商与合作伙伴的角色

主体识别解决指向问题，角色则说明主体如何参与具体协作。员工、客户、供应商与合作伙伴，是观察共同创造的不同关系入口。它们不是对人的永久分类，也不是价值高低的等级。一个主体可以在不同事项中承担不同角色，各种角色所支持的主张需要分别说明。

角色具有相对性。员工身份需要指向相应组织和任职关系，客户身份需要指向一定交易或使用关系，供应商身份需要指向相应供给安排，合作伙伴身份则需要指向明确的共同活动。只在个人档案中写上一个角色名称，无法充分解释这个角色对谁、在何时、针对什么事项有效。

因此，关系应当成为可以单独核验的记录对象。它至少需要关联参与各方、关系类型、适用事项、成立依据、有效期间和当前状态。角色从这些关系中取得含义，再依据适用规则影响参与方式。这比给每个人固定分配一个覆盖全部活动的标签，更能表达共同创造的实际结构。

员工角色通常连接持续性的工作安排、职责分工与组织能力积累。岗位可以说明期待承担的工作，却不能单独证明实际贡献已经发生。工时、交付、被组织吸收的知识和协同形成的能力，需要结合实际事件分别确认。担任某个职务也不意味着可以将团队全部成果归于个人。

员工同时具有不同性质的主张和义务。日常工作职责、报酬安排、对工作记录的知情与异议，以及参与某项资本计划的资格，各有不同依据。制度设计应当使这些关系能够被分别表达，避免用一项贡献评价替代全部安排。进入一项额外的协作激励机制，也不应被系统设置成核验其他既有主张的唯一通道。

客户角色连接需求表达、交易、使用与反馈。客户可能参与产品改进、应用扩展或长期合作，但购买行为与具体贡献仍需分别识别。付款可以支持交易关系的确认，不能仅凭付款规模推定客户已经作出了相同比例的创新贡献，或者自动取得企业治理权。

客户关系中的行动者还可能不同。提出需求、实际使用、签订约定和支付费用的主体未必一致。模型若将这些角色统一归给付款账户，可能遗漏实际使用者的反馈，也可能把代表组织采购的个人误认为交易关系中的最终主体。角色分解的目的，是使不同事实能够找到恰当的对应者。

供应商角色连接资源供给、交付质量、履约持续性和供应协同。供给可能形成可长期利用的能力，但收到订单、完成交付、帮助改进流程以及承担额外风险，是需要分别记录的事项。供应商取得约定对价，与其是否因额外贡献进入长期资本安排，仍然需要不同的确认条件。

供应关系还可能包含分包与协同交付。签约主体、实际作业者和关键资源提供者可能处于不同层次。模型需要保留这些联系，以便适当解释贡献与责任；但记录了某个下游参与者，也不意味着其自动取得对所有上游主体的直接请求权。关系的可见性为制度判断提供材料，不能取代判断本身。

合作伙伴角色最容易因名称宽泛而失去边界。共同研发、联合交付、渠道协作与资源共享都可能被称为合作，但其投入方式、决策范围和责任结构并不相同。有效建模应当返回具体安排，说明各方共同做什么、分别承担什么、哪些事项需要共同决定，以及合作在什么条件下结束。

角色	需要明确的协作关系	贡献确认时需要进一步查明的事项
员工	任职、职责与具体工作安排	实际行动、交付及组织吸收情况
客户	购买、使用、需求与反馈关系	超出关系标签的具体参与及其作用
供应商	供给、交付及持续履约安排	交付结果、协同改进与承担的风险
合作伙伴	共同任务、资源安排与决策约定	各方投入、共同成果及分别承担的责任

这些角色并未穷尽所有利益相关者。资本提供者、社区成员及其他受到组织活动影响的主体，也可能具有需要承认的关系和主张。身份模型应当允许依据治理范围扩展角色，并解释准入和代表方式，不能因为某类主体不在最初的四个选项之中，就预先否定其提出利益主张的可能。

关系成立的依据也可以不同。有些关系由双方约定形成，有些由有权组织程序确认，有些仍处于一方提出、另一方有异议的状态。系统应当保留依据和确认状态。自称合作伙伴不能直接获得对方资源的操作权限；对方暂不确认，也不应导致提出关系主张及请求复核的记录被删除。

模型还需要区分参与角色与审查角色。作出贡献的人可以提交说明，但能否确认自己的结果，需要单独规定。一个人在某项工作中负责交付，在另一项工作中可以负责审核；对同一事项是否存在应当回避的关系，必须结合具体对象判断。仅靠统一的职位高低，难以完成这种检查。

利益相关者资本治理关注长期共同创造，因此角色建模也需要容纳关系的沉淀和结束。一次交易的结束未必终结全部支持义务，任职关系的结束也未必消除已经发生的贡献记录。模型应当让当前参与状态与历史行动保持联系，同时由各自制度决定后续权益如何处理。

本书据此提出，角色的作用是组织贡献确认的入口和解释条件。角色说明一个主体为什么进入某个协作过程，实际事件说明其作出了什么，资本与权益制度再说明这些结果将产生怎样的安排。三个环节相互连接，才能使利益相关者被承认，而不被一个标签替代。

三、身份凭证、访问权限与角色变更

身份和关系进入系统后，需要通过可供检查的材料表达。身份凭证可以支持对主体指向、任职关系、业务资格或代理授权的核验。它不是对一个主体全部情况的完整证明，而是某个出具者在一定范围内作出的声明。凭证能够支持哪些行动，取决于声明内容、出具资格以及采用它的规则。

W3C 的可验证凭证模型区分出具者、持有者、凭证所描述的主体和验证者，持有者不一定是凭证主体。凭证验证可以检查来源和完整性等条件，但不会自动完成对其中事实的判断。这意味着，取得一份凭证副本与有权以其中所描述的身份行动，仍然是不同问题。W3C：可验证凭证的参与角色与验证边界〔2〕

关系凭证应当准确限定其声明。某组织证明一个人在某段时间任职，不等于证明此人可以无限额处分组织资源；业务平台确认某供应商完成登记，也不等于确认其全部交付合格。接收凭证的系统需要按本次用途解释声明，避免从一个窄范围事实扩张出过宽的权限。

身份核验、登录认证和行动授权也应当分别处理。身份核验检查所声称的主体及相关证据；认证检查当前请求者是否控制与账户绑定的认证手段；授权决定该请求在当前条件下是否可以执行。NIST 的数字身份指南区分身份核验、账户与认证手段管理，并将有关身份信息作为接收服务作出授权决定的依据之一。NIST：数字身份指南 SP 800-63-4〔3〕

据此，验证通过应当说明通过的是哪项检查。“签名正确”“资格有效”和“允许执行”不宜显示成含义相同的状态。一个请求可以由真实主体发起，使用有效密钥签署，却因超出业务范围或缺少共同批准而不能执行。保留这些区别，既有助于限制越权，也有助于向参与者解释拒绝的具体原因。

访问权限需要落实为对一定对象进行一定操作的条件。查阅材料、提交记录、确认交付、调整参数和执行支付，是不同的操作；同一种操作针对不同项目、期间和资源，也可能需要不同授权。只设置“普通成员”和“管理员”，往往无法表达共同治理中实际存在的职责分工。

角色可以提供一组基本权限，具体使用仍可结合对象、事项状态、有效期限和其他属性进行判断。NIST 对基于属性的访问控制的描述，就是依据主体、对象、请求操作及必要环境条件的属性，结合规则作出授权决定。这提供了将粗略身份标签细化为具体行动条件的一种技术方法。NIST：基于属性的访问控制指南〔4〕

本书在这一技术思路上强调，权限规则应当能够返回其制度来源。一个人被允许审核某类贡献，应当能够查明是谁授予、依据什么职责安排以及是否存在回避条件。系统维护人员可以负责录入和配置，但能够修改权限表，不应成为其自行决定全部治理资格的依据。

角色的叠加尤其需要限制自动扩权。一个人同时担任提交者和审核者时，可以拥有两类功能入口，但是否能够审核自己的事项，应由独立规则判断。多个角色的权限不能简单取并集后不再检查限制条件。禁止事项、共同批准要求和利益冲突约束，应当在具体请求中继续有效。

身份与角色还具有不同的生命周期。主体识别完成后，某项任职可以尚未生效；任职已经结束后，主体仍然存在；一个业务资格暂停期间，其他无关关系也可能继续有效。模型应当支持分别变更这些状态，避免一次账户冻结不加区分地中断全部协作和必要查询。

角色变更需要记录决定依据、生效时间、实际录入时间、受影响的权限和通知情况。生效时间与系统获知时间可能不同，追溯时不能仅凭当前页面覆盖过去。对于执行中的任务，还需要明确变更从哪个检查点影响请求：提交时有效的权限，是否还须在最终批准或执行时再次核验，应按事项性质事先规定。

权限撤销也不是修改一处记录就自然完成。业务系统、链上合约、缓存和已经建立的会话，可能在不同时间获知变化。制度需要规定同步责任、可接受的延迟，以及状态无法确认时的处置。短期凭证、重新认证或关键操作前查询当前授权，可以作为不同场景下的实现选择。

撤销当前资格，与否定历史行动仍须分开。曾在有效任职期间作出的合格操作，不应仅因今天离职便自动改写为越权；若发现凭证曾被冒用或资格自始存在错误，则需要按证据确定受影响的期间和事项。旧签名需要结合当时的授权、密钥状态和证据解释，不能只查当前状态就作出全部结论。

同样，停止工作权限不等于取消既有权益。离职、合作结束或供应资格到期，可能要求立即关闭新增业务操作，但已经发生的贡献、尚未结算的款项、有效期内形成的主张以及必要的申诉访问，应当依据各自安排处理。账户生命周期不应代替贡献和权益的生命周期。

密钥恢复则是另一类变更。若主体不变，只是丢失了原有认证手段，恢复程序需要重新建立该主体与新手段的可靠联系，限制旧手段，并检查关联权限是否仍然成立。不能因为新密钥获得控制，就把恢复过程解释为一次资本或权利转让；也不能允许协助恢复的人因此取得被恢复主体的全部身份能力。

跨组织使用凭证时，技术上的可读取与制度上的可采用需要进一步衔接。接收组织应当明确认可哪些出具者、认可其证明哪些事项，以及本组织采用的有效性和权限条件。相同的“合作伙伴”名称，在不同组织可能具有不同含义。可携带凭证可以减少重复取证，却不保证角色和权利原样迁移。

在此基础上，区块链可以承担需要多方共同检查的授权或状态记录，敏感身份材料则可以保留在适当的链下系统中。具体选择应当服务于共同验证和责任安排。身份系统是否有效，最终要看每次行动能否得到适当授权，变更能否及时反映，以及参与者是否仍有可靠的纠错和恢复路径。

四、多重身份、虚假身份与责任追溯

一个主体拥有多个标识，并不必然意味着身份虚假。不同账户可以用于区分个人行动与组织代理，隔离不同业务，或者减少无关活动被关联。利益相关者身份模型需要容纳这种现实，同时防止同一主体借助多个标识重复取得本来受到限制的资格。

因此，需要区分三个问题：标识是否指向所声称的主体，主体是否具有所声称的关系，以及同一项规则下的资格是否被重复计算。冒用他人材料主要破坏主体对应关系，虚报任职主要破坏关系真实性，多账户重复申领则可能利用资格计算的缺口。它们需要不同证据和处理方式。

女巫攻击揭示了其中一种典型结构：同一实际控制者呈现多个身份，使系统把这些身份误当作独立参与者，从而削弱依靠多方参与建立的保障。Douceur 的相关研究讨论了这种攻击对点对点系统冗余和身份确认的影响。John R. Douceur: The Sybil Attack [5]

在利益相关者资本治理中，这种结构可能表现为重复取得成员资格、用多个账户相互确认贡献，或制造看似独立的支持意见。防止这些问题，首先需要明确规则究竟按什么单位计数。一个自然人、一个组织、一段有效关系和一项独立贡献，是不同的计数对象，不能统一用地址数量替代。

“一人一份资格”需要在规定范围内检查自然人的重复登记；“一组织一个席位”需要识别组织及相关控制关系；“同一贡献不得重复申领”则需要检查贡献事件和请求依据。一个组织中有多名真实员工，并不意味着他们在每项组织决策中都构成相互独立的组织代表；多人共同完成一项任务，也不意味着只允许保留其中一人的贡献。

真实性、唯一性与独立性因而需要分别论证。两个账户可能属于不同的真实自然人，但其在某项审核中存在共同利益或受同一方指示。身份核实可以提高冒名的难度，却不能据此证明所有参与者没有串谋。参与关系、授权关系和必要的利益冲突声明，仍然是治理判断的重要材料。

核验强度应当与资格的重要性和潜在影响相称。接入更多材料、采用现场检查或提高操作认证强度，都可能增加某些攻击的难度，但也会增加成本和错误拒绝。缴纳保证金或持有某类资产可以约束部分行为成本，却不能单凭资源投入证明主体唯一，更不能证明其已经对共同创作作出相应贡献。

隐私保护要求唯一性检查具有清楚范围。为了防止某项资格重复使用，并不当然需要公开一个人全部账户及其他合作关系。系统可以在适当机制下检查限定范围内的重复性，同时只向有关审核者披露必要联系。上一章讨论的选择性披露与零知识证明可以提供部分支持，其前提仍是初始资格与持有人联系已经可靠建立。

合理化名也应当与逃避责任区别对待。在允许使用化名的协作中，持续可联系的标识、有效授权和必要的受控核验，可以共同支持参与。治理需要的是与具体事项相称的可追溯性，不应将公开全部身份资料作为任何活动的默认条件。披露更多信息未必能消除阴谋，却可能扩大参与者承担的信息风险。

身份关联错误同样需要认真处理。姓名相同、共用网络、设备相似或行为接近，可以成为进一步核查的线索，但不宜单独作为合并主体或判定欺诈的依据。将两个人错误合并，可能取消其中一人的资格；把同一主体错误拆分，又可能造成重复计数。关联和解除关联都应当有证据、权限与复核记录。

责任追溯需要沿着行动过程展开。记录应当能够连接主体、当时的角色、代理依据、所使用的密钥、请求内容、适用规则和处理结果，并在必要时返回支持这些联系的业务证据。只有一个交易编号，通常不足以说明行为发生的完整制度条件。

追溯也需要区分操作、批准、控制与后果。经办人发起请求，审核者作出批准，系统执行动作，组织取得结果，各环节可能由不同主体承担。判断责任需要结合职责、授权、实际行为与因果联系。有效签名是重要证据，但在密钥被盗、共享控制或自动化运行等情况下，仍须查明其具体背景。

记录保存者与身份确认者也处于责任链之中。错误绑定主体、迟延撤销授权、未保留必要变更依据，可能影响对行为的判断。不能一方面由组织控制身份登记和权限维护，另一方面在发生问题时仅凭账户名称把所有后果推给账户所标记的人。责任模型应当覆盖这些基础服务的实际职责。

对可疑身份采取措施时，本书主张使措施与证据和影响范围相称。需要控制新增风险的，可以按授权程序限制有关操作，同时保留通知、补充材料与申诉途径。暂时无法核实不应直接写成已经证实欺诈；纠正身份关系也不应顺带删除尚待审查的历史贡献或未决主张。

更深一层的问题，是谁能够决定一个主体在共同制度中是否“存在”。如果唯一的身份服务商可以不说明理由地拒绝登记、撤销凭证或阻断恢复，它就可能实质控制参与、申诉和退出。身份基础设施自身也需要治理，包括准入依据、决定权限、复核安排以及必要的替代验证与迁移条件。

面向未来，本书提出一个需要检验的方向：在特定协作范围内保持主体和责任的连续性，同时允许不同关系使用适当分离的标识。其成立条件包括可靠的授权衔接、限定范围的重复检查、必要的历史证据和可实际使用的恢复程序。若这种安排增加了冒用、错误排除或追溯困难，就需要修订关联与披露规则，而不能仅凭“去中心化身份”的名称判断制度已经改善。

利益相关者身份与关系建模由此构成贡献确认的第一层制度基础。它使系统能够说明谁进入了协作、以何种关系参与、在什么范围内行动，以及变化发生后哪些联系继续有效。识别准确并不保证贡献已经发生，却能让贡献记录从一开始就具有可以检查的归属。

下一章将进一步把这种关系放入行动过程：参与者承诺了什么，实际完成了什么，哪些投入形成交付，交付又怎样被使用并产生结果。主体与关系提供指向和解释条件，承诺、任务与贡献事件则使共同创造获得可以逐步核验的具体内容。

定稿补强：分级身份与合规触发

身份设计应同时避免识别不足和过度收集。一般协作、访问内部材料、取得不可转让资格、接收可转让价值、高额支付、跨境活动和受监管职能，可以采用不同的身份强度。系统不应为了所有低风险活动收集同样多的数据，也不能在高影响价值流转时只依赖一个无法追责的地址。

每个身份等级应写明证明目的、签发者、验证者、有效期、撤销、最少披露字段和升级触发器。涉及反洗钱、制裁、税务、消费者或其他监管要求时，应由相应责任主体根据法域确认，不由DID、可验证凭证或账户格式自动完成。身份凭证表达的是声明及其验证关系，不能替代对声明内容和使用目的的判断。

本章注释

1. [SRC-074] 万维网联盟（W3C）：[Decentralized Identifiers（DIDs）v1.0](#)。[原文或官方页面](#)
 - 本章引证：W3C：去中心化标识符的主体与控制者。

- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：W3C：去中心化标识符的主体与控制者。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
2. [SRC-076] 万维网联盟（W3C）：[Verifiable Credentials Data Model v2.0](#)。[原文或官方页面](#)
- 本章引证：W3C：可验证凭证的参与角色与验证边界。
 - 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：W3C：可验证凭证数据模型 2.0、W3C：可验证凭证中的选择性披露与隐私考虑、W3C：可验证凭证的参与角色与验证边界、W3C：可验证凭证的验证与业务判断、W3C：可验证凭证与数据最小化。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
3. [SRC-066] 美国国家标准与技术研究院（NIST）：[数字身份指南 SP 800-63-4](#)。[原文或官方页面](#)
- 本章引证：NIST：数字身份指南 SP 800-63-4。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：NIST：数字身份指南 SP 800-63-4。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
4. [SRC-009] 美国国家标准与技术研究院（NIST）：[基于属性的访问控制指南](#)。[原文或官方页面](#)
- 本章引证：NIST：基于属性的访问控制指南。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：NIST：基于属性的访问控制指南。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
5. [SRC-058] John R. Douceur / Microsoft Research：[John R. Douceur：The Sybil Attack](#)。[原文或官方页面](#)
- 本章引证：John R. Douceur：The Sybil Attack。
 - 支持范围：用于支持所引理论、模型、算法或经验研究的原始论证，本书引用主题包括：John R. Douceur：The Sybil Attack。
 - 使用边界：原始研究支持其设定范围内的结论，不直接证明本书提出的治理制度已获得普遍实证验证。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第十四章 承诺、任务与贡献事件

共同创造需要参与者，也需要能够承接行动的组织安排。身份与关系说明谁进入协作、代表谁以及可以做什么；承诺与任务进一步说明各方准备完成什么、需要哪些配合，以及怎样判断履行进展。实际行动发生之后，组织才有材料讨论贡献，而不能仅凭身份、意愿或任务名称，提前认定贡献已经成立。

从承诺走向贡献，并不是把一项计划的状态从“未完成”改成“已完成”那么简单。资源可能已经投入，交付仍未形成；交付可能已经通过验收，尚未进入实际使用；使用已经发生，长期效果仍然需要观察。如果系统只保留一个综合分数，就会把这些不同事实压缩在一起，使参与者难以理解确认依据，也难以对错误提出有针对性的异议。

本章把承诺、任务与贡献事件作为三个相互联系的对象。承诺表达面向未来的安排，任务组织履行过程，贡献事件则记录与贡献判断有关的实际行动及其联系。这里使用“贡献事件”这一名称，不预先表示贡献已经获得确认；记录所处的证据和确认状态，必须另行表达。

一、事前约定与贡献条件

事前约定的首要作用，是使参与者能够在行动之前理解组织将如何对待其投入。共同目标越抽象，越需要说明具体行动怎样与目标相连。否则，一方可能认为自己在履行明确义务，另一方却把同一行动理解为没有承诺回报的自愿尝试，分歧直到投入已经发生才显现出来。

承诺应当具有明确的相对方和事项。谁作出承诺，向谁作出，准备提供什么，以及需要什么条件配合，都会影响后续履行。承诺可以涉及劳动、资源、交付、使用、审核或支付，不宜只记录执行者必须做什么，而遗漏组织应当提供的条件和反馈。

意向、提议与已经成立的约定，需要保留不同状态。一个人提出愿意承担工作，不等于组织已经接受相应安排；管理者发布任务，也需要根据其权限和适用程序确定效力。系统应当能够查明哪些事项已经得到有权确认，哪些仍然等待协商。技术上的“创建成功”不能替代制度上的成立条件。

任务是对承诺履行的组织化表达。它可以把一个较大的目标分解为可协作的范围、阶段和交付要求，并明确依赖关系、责任人及协调机制。但任务分解并不意味着每个细小动作都要单独评价。分解的尺度应当足以支持交接和核验，同时避免把工作切成大量只为计数而存在的片段。

贡献条件则说明什么行动可以进入贡献判断，以及需要满足哪些要求。这些要求可能涉及真实发生、与共同目标有关、处于适当授权范围、达到约定质量或能够提供必要证据。不同贡献类型可以采用不同条件，但条件应当具有可理解性，不能只用“表现优秀”“价值突出”等词语代替全部判断依据。

这里需要区分进入记录、确认贡献和形成权益的条件。一个实际行动可以被记录，却尚不足以证明其构成所主张的贡献；贡献得到确认，也可能仍需满足组织吸收、持续使用或风险承担等条件，才进入某项资本安排。收益权和治理权的形成又有各自依据，不能由任务完成标记直接推导。

事前约定还应说明哪些结果可以由行动者控制，哪些依赖他人和环境。对可控制的交付质量作出承诺，与保证全部经营结果，是不同性质的要求。如果任务需要组织提供材料、权限或配套资源，这些依赖应当同时记录。配合条件未满足时，不能只在执行者一侧留下未完成的结论。

对于探索性活动，事前完全规定成果可能并不现实。组织可以约定研究范围、资源边界、阶段汇报和停止条件，并说明可接受的不确定性。没有达到最初期待的结果，不足以单独判断参与者没有履行约定；反过来，投入了时间也不自动证明探索方法适当或形成了有用知识。

持续维护、协调支持和风险预防同样需要适当的任务表达。这些活动的作用可能体现为运行条件得以维持，未必表现为一个显眼的新成果。制度若只认可新增交付数量，就可能遗漏维持共同能力所必需的工作。事前可以约定责任范围、观察期间和必要材料，为此类贡献保留可审查的入口。

证据要求也是约定的一部分。谁负责采集，何时形成记录，由谁保管，哪些信息可以向谁披露，应当尽量在行动前明确。证明负担需要考虑各方实际掌握材料的条件，不能要求执行者提供只有组织控制的资料，又不给予其获取或请求核验的途径。

确认职责与时限也应当同步安排。执行者按期提交后，接收方需要说明何时检查、何时反馈以及出现分歧怎样处理。逾期没有回应，应当触发约定的提醒、升级或其他处理；未经明确规则，不能任意把沉默视为全部认可，也不应允许沉默无限期阻断参与者的主张。

约定中的回报需要表达承诺的具体程度。确定的履约对价、满足条件后进入评议的资格，以及依赖未来可分配资源的安排，应当分别说明。把“有机会参加”写成“必然取得”，会使技术记录固定一项原本并未成立的预期；把已经承诺的事项事后改称一般激励，也会破坏合作的可预期性。

规则变化不可避免，但变更需要有明确程序。新增任务、扩大范围、改变质量口径或调整确认条件，都可能影响原有投入。系统应当保存原约定、变更内容、授权依据和生效范围，让参与者能够判断某次行动适用哪个版本。新规则是否影响已经发生的行动，需要经过相应制度处理，不能由配置更新悄然决定。

现实中也会发生未经完整事前安排的必要行动。紧急处置、临时协助和制度尚未覆盖的共同创造，不宜因缺少任务编号就被排除在记录之外。可以允许提出补充说明并进入专门审查，同时保留“事前未约定”的事实。补充确认不能把事后材料伪装成原本存在的承诺，也不能保证所有自发行动都获得请求的回报。

由此，事前约定既形成可检查的行动边界，也为无法完全预见的情况保留处理程序。它使参与者知道什么可以期待、什么仍待判断、什么变化需要重新讨论。制度技术可以固定这些安排及其版本，为执行提供依据；承诺是否合理、是否得到适当接受，仍需要组织治理作出判断。

二、投入、交付、使用与结果的分别记录

共同创造中的不同阶段，回答的是不同问题。投入说明哪些资源已经进入活动，交付说明形成了什么并向谁提供，使用说明交付怎样进入后续活动，结果说明在特定范围和期间观察到了什么变化。它们可以相互关联，却不应被当作同一个事实的不同名称。

投入首先需要区分承诺可用、实际提供和实际消耗。某项资源被列入预算，不说明资源已经到位；资源到位，也不说明已经投入相应任务。记录应当说明资源类型、数量或范围、提供主体、发生期间及用途。涉及共享资源时，还需要保留分配口径，避免同一资源在多个任务中都被按全部投入计算。

资源投入可以包括时间、资金、知识使用条件、设备能力和必要的协作支持，但这些项目不必立即折算为同一金额。工时可以描述投入长度，资金可以描述支付规模，设备占用可以描述使用条件。它们为贡献判断提供不同信息，不能只因都能计数，就直接相加为一个总贡献值。

交付记录需要指向具体对象或可核验的服务阶段，并保留版本、数量、质量要求和接收范围。材料已经上传，只能先说明完成了一次提交；接收方已经收到，不等于其确认全部符合要求。提交、接收、验收和要求补正，可以围绕同一交付分别形成关联记录。

交付还应当区分原始成果、修订成果和后续维护。对同一对象的修订可能只是修正原有缺陷，也可能形成新增能力，需要结合任务范围判断。改变文件名称或重新上传，不应自动形成一次新的实质交付；真正新增的工作，也不应因为仍然关联同一对象就被抹去。

使用记录说明某项交付是否进入后续协作。谁使用、用于什么活动、采用哪个版本以及持续多久，都会影响解释。获得访问权限与实际使用不同，下载材料与完成应用也不同。涉及服务和组织能力时，使用还可能体现为持续采用某种流程、方法或协作安排，而不只是读取一个数字文件。

来源追溯技术提供了组织这些联系的参考。W3C 的 PROV 数据模型区分实体、活动和承担有关责任的参与者，并表达生成、使用、衍生和代理等关系。这样的结构有助于描述某个成果从何而来、进入了哪些后续活动，但具体业务事实仍需相应证据支持。W3C：PROV 数据模型〔1〕

结果记录则需要明确观察对象、期间和口径。产出增加、质量改善、协作时间缩短或能力得以维持，都需要说明怎样观察和比较。变化发生在交付之后，不足以单独证明变化全部由该交付造成。其他人的投入、原有积累和环境变化，也可能共同影响结果。

记录层次	需要回答的问题	不宜直接推导的结论
投入	哪些资源实际进入了什么活动	投入规模就是贡献价值
交付	形成了什么，交给谁，符合哪些要求	提交成功就是完整履行
使用	谁在什么活动中实际采用了交付	获准访问就是已经产生作用
结果	在何种范围和期间观察到什么变化	全部变化均由某一主体造成

这四类记录并不构成每项工作都必须逐级通过的单一通道。有的约定以合格交付作为履行条件，有的还要求支持使用，有的则关注一定期间的结果。判断任务是否完成，应当返回具体约定；长期效果尚未显现，不能自动成为拒绝已满足条件的阶段性确认的理由。

使用机会也未必由交付者控制。成果符合要求后，组织可能因优先次序、资源不足或方向调整而暂不采用。系统需要保留“不使用”的实际原因，而不能把所有未使用都解释为交付无效。与之相应，组织也不应为了满足记录指标而制造没有业务必要的形式使用。

延迟结果需要明确观察安排。任务结束后，可以继续形成与原交付关联的使用和结果记录，并说明哪些结论暂时未知。未知、尚未观察和已经观察到没有达到目标，应当分别表达。用空白值或零分混合这些状态，会使长期贡献受到不适当的即时评价。

失败与不利结果也应当被如实记录。探索没有达到期待目标，可能仍形成经过验证的知识，也可能暴露方法和履行中的缺陷；维持了运行，可能来自有效维护，也可能只是没有遇到风险。不能把失败自动美化为贡献，也不能仅因没有新增可见产出就否定全部作用。判断需要结合承诺、实际行动和可支持的结论。

对共同能力的记录尤其需要谨慎。能力可以通过持续活动和相关结果获得支持，但组织拥有某项能力，不意味着可以把成员的全部个人知识登记为组织所有。记录需要说明组织实际能够持续利用的条件，以及这些条件依赖哪些关系。能力形成与权利归属仍然应当分别表达。

分别记录还能够减少同一事实在多个阶段被累加计价的风险。投入、交付、使用与结果可以是同一创造过程的不同证据，不能先把投入记作全部贡献，再把交付和结果各按全部价值加一次。是否认可不同阶段的独立作用，应由计量和分配制度明确，而不是由记录条数自然决定。

因此，本书建议保留多维事实，再按具体目的进行评价。任务管理可以关注进度，履约确认可以关注条件，资本形成可以关注持续使用与组织吸收。不同目的读取相互关联的材料，但不必强迫所有事实一开始就变成同一种分数。这样才能为后续价值判断留下充分而清楚的依据。

三、贡献事件的结构与生命周期

贡献事件把持续发生的协作转化为可以指认、关联和复核的记录单元。它可以描述资源已经投入、交付已经提交、成果开始被使用，或者某个期间的效果已经得到观察。事件的划分应当服务于事实表达和责任判断，其粒度可以不同，不必把所有活动都压缩为某个瞬间发生的点击。

在建模时，首先需要区分现实发生的事项、关于事项的记录以及依据记录提出的主张。同一现实事项可以产生多份观察记录；一份记录也可以支持不同范围的判断。记录标题写着“贡献”，并不意味着其中陈述已被核实；记录中列明某个主体，也不意味着其已经取得全部所请求的权益。

任务与事件之间通常存在一对多或多对多的联系。一个任务可以产生多次交付和补正事件，一次协作活动也可能同时服务于多个任务。系统需要保存这些联系，并说明各个任务实际采用了什么。把任务编号当作唯一的事件编号，会混淆同一任务中的不同动作；为每个任务复制全部事件，又容易制造重复记录。

本书提出如下最小结构，用于表达贡献事件的制度含义。它是一种面向本书问题的模型建议，具体实现可以根据业务增减字段，不要求所有类型使用完全相同的表单。

信息组	主要内容	对制度判断的作用
事件指向	事件标识、类型、来源及相关事项	区分记录对象并寻找关联记录
参与主体	行动者、被代表者、接收者及各自角色	解释行动归属与协作关系
约定依据	承诺、任务、适用条件及规则版本	查明行动应当按什么标准理解
行动与对象	实际动作、交付对象、版本、数量及范围	限定记录所声称的事实
时间信息	发生时间或期间、记录时间、提交时间	区分现实先后与系统获知先后
证据联系	材料引用、出具来源、完整性信息及访问条件	支持核验并说明证据取得路径
处理状态	待核验、已有结论、异议及修订联系	表达当前可以采用的判断范围
下游联系	已关联的评价、资本或权益处理记录	追踪采用情况，避免自动混同与重复处理

事件标识首先解决识别问题，不能独自证明真实或唯一。不同系统可能给同一现实事项分配不同标识；同一个标识也可能因录入错误而被用于不同内容。除了编号，仍然需要对象、来源和业务联系支持判断。标识的作用是稳定引用，实际事项的对应关系需要核验。

时间信息尤其需要分别表达。行动可以持续一段时间，也可以在发生后很久才被记录。补录历史活动时，应当保留实际发生期间和补录时间，并说明时间依据。链上收录时间可以帮助判断记录何时进入相应账本，不能直接作为链下工作在同一时刻发生的证明。

主体与授权应当关联到有关行动所适用的期间。一个人提交记录时可能已不在原岗位，但其历史行动仍可能发生在有效任职期间。系统需要能够查阅当时的角色及授权依据，而不是以当前身份状态替代全部历史。代录人员与实际贡献者也应在事件结构中分别指明。

证据联系应当保留材料所支持的范围。可以在链下保存必要材料，在共同记录中保存引用、版本和完整性信息，并根据用途控制访问。事件不必向所有参与者公开全部工作细节，但有权核验者应当能够取得必要依据。没有有效获取路径的证据编号，难以支撑持续复核

贡献事件的生命周期，主要指记录及其判断如何被处理，不是现实事实可以被程序任意改写。初始记录可以处于草拟状态，正式提交后进入待核验状态；核验过程中可以补充材料，结论形成后可以表达全部认可、部分认可或不予认可的范围。有异议时，再通过有权程序形成新的处理记录。

这些状态不应被写成必须单向通过的一条流水线。某一部分已经确认，另一部分可以继续等待材料；一个判断受到质疑，也不必使所有无关事实失效。记录可以包含分项结论和明确的适用范围，使后续系统知道哪些内容可以采用、哪些内容需要等待，而不被一个“通过”按钮遮蔽。

业务状态、确认状态和权益状态还应当各自维护。工作可能已经停止，事实核验仍在继续；贡献已经确认，资本形成条件可能尚未满足；某项收益处理完成后，后续效果仍可能继续被观察。三个过程通过明确的关联规则相互通知，不能用其中一个状态替代其他过程。

历史纠正可以采用保留原记录、追加更正及其关联的方式。事件溯源是一种利用事件序列表达状态变化的技术模式，其更正通常通过新增补偿事件记录，而不是覆盖原事件。这种模式可以在不采用区块链的系统中实现；区块链是否必要，仍取决于是否需要多方共同验证和维护有关记录。Microsoft：事件溯源模式〔2〕

用于贡献治理时，更正记录还需要说明由谁决定、为何更正、影响哪些内容，以及后续采用者怎样获知变化。补充一项遗漏事实，与撤销一项错误确认，具有不同含义。当前有效状态应当能够反映最新的有权决定，同时保留理解原判断所必需的历史联系。

记录状态的变化也不会自动消除已经发生的外部后果。如果此前确认已经进入计量、资本登记或支付安排，更正需要通知相关环节，并分别处理其影响。追加一条补偿记录可以表达应当调整的事项，但实际资源是否收回、主张是否改变，还要看有关授权、程序和履行条件。

系统还需要说明什么情况下可以结束处理。任务取消可以停止未来工作，却不应自动撤销已经完成的部分；主张人撤回某次申请，不必意味着其曾经提交的事实全部为假；材料暂时不足，也不应被标记为已经证实虚报。不同终止原因需要保留各自含义及后续可采取的行动。

结构版本同样需要管理。业务发展后新增字段、调整事件类型或改变口径，应当保留旧记录的解释方式。不能用新版本默认值填补旧记录缺失的信息，再让系统把推定值当作历史事实。跨系统交换时，还应说明相同事件名称是否具有一致含义。

事件结构的质量，最终体现为参与者能否从当前结论返回主体、行动、约定、证据和修订过程。链上记录获得技术确认，只说明其在相应协议下得到收录或形成有关状态，不代表所有业务争议已经结束。共同账本可以固定程序留下的轨迹，贡献结论则继续接受制度规定的复核与修订。

四、多方共同贡献与重复记录识别

共同创造往往由多方相互补充而成。资源提供、问题识别、实际执行、协调配合和成果采用，可能由不同主体承担。若系统要求每项成果只能归于一个人，就会把共同过程压缩为最后提交者的记录；若允许所有参与者各自申报全部成果，又可能重复确认同一总量。

适当的结构应当同时保留共同事项与个人或组织的具体行动。共同事项记录协作目标、整体交付及有关结果，参与者的事件记录则说明各自实际作出了什么。不同事件可以关联同一成果，并表明它们是提供条件、生成、修改、审核或使用等不同关系。

这种关联首先用于解释共同创造的过程，不立即等同于分配比例。一个主体提供必要条件，不说明全部结果由其单独创造；一个主体完成最后交付，也不说明其可以排除此前参与者。来源联系可以支持后续归因判断，但本身不是对经济价值份额的精确证明。

共同成果也未必能够无损拆分。有些作用只有在多人协作时才成立，单独观察某项行动无法表达其全部意义。在证据不足以支持精细比例时，可以先确认共同事项与参与范围，保留尚待评议的部分。本书不主张为满足自动计算而提前制造看似精确的个人份额。

重复识别需要先说明正在排除哪一种重复。消息被重复传送、同一事实被不同主体记录、同一成果被拆成相似条目，以及同一权益请求被重复提交，是不同层次的问题。只有把层次分开，才能在避免重复处理的同时，保留必要证据与合理主张。

消息重复通常发生在技术传输和重试过程中。CloudEvents 规范要求以事件来源与事件标识的组合区分事件，重发同一事件时可以保留同一标识，接收者据此识别重复。这为跨系统传递提供了一种约定，但依赖发送方正确维护标识，不能单靠它发现所有业务上的重复事项。CloudEvents：事件标识与来源规则〔3〕

接收系统还需要使同一有效请求的重复到达不重复产生业务后果。技术上通常称为幂等处理，其核心是在约定范围内让重复请求得到一致的处理结果。用于贡献治理时，需要明确这个范围对应哪项操作和哪个处理周期，不能让一次消息重试再次增加已确认数量或再次触发支付。

这种保障应当延伸到实际执行环节。系统记录了“已经处理”，但外部执行失败，与外部执行成功却未收到回执，是不同情况。有关环节需要通过明确的操作标识识别处理状态和对账恢复确定结果。只在消息入口去重，不能保证所有下游动作自然只发生一次。

事实的多份记录则具有另一种意义。交付者的说明、接收者的回执和核验者的意见，可能都指向同一次交付。它们可以作为关联证据保留，而不各自被计算为新的交付。识别出指向同一事实，应当建立对应关系，并保留来源差异，不宜直接删除其中的记录。

多份记录之间也可能存在冲突。数量、时间或质量描述不同，需要查明各自观察范围和依据。较早上链的记录不因时间在先就自动更真实，较多账户重复同一说法也不自动形成更多独立证据。重复识别可以把有关材料放到一起，却不能替代下一章将讨论的证据审查。

对内容相似的记录，需要进一步判断其业务含义。相同文件可能在不同期间被实际使用，形成不同的使用事件；文件字节不同，也可能只是同一交付的格式转换。哈希可以帮助检查内容是否一致，但不能单独决定贡献是否重复。对象、版本、任务、行动类型和实际使用关系需要共同参与判断。

持续性工作还需要处理时间范围的重叠。按日、按阶段和按月分别记录的工作，可能存在包含关系。系统可以把阶段性汇总关联到原始事件，并说明汇总范围，使统计时选择适当层级。若同时把全部明细和全部汇总相加，就会重复计算同一活动。

共同任务与个人任务也需要同样的层级约束。整体完成数量和参与者的工作记录可以并存，分别服务于履约管理和贡献判断。它们不必被强制变成可以简单相加的同一单位。需要汇总时，应明确采用哪些记录、排除哪些重叠，以及共同作用如何保留。

重复主张则必须结合具体权利安排判断。同一事实可能支持履约对价、署名认可或另有依据的长期激励，这些主张是否可以并存，需要看各自规则。防止重复获得同一项权益，不意味着凡已获得一种回报就排除其他主张；也不意味着可以换一个名称绕过明确的重复领取限制。

跨组织协作需要进一步限定互认范围。同一事件可以被多个组织引用，各自承担不同的确认和结算职责。若涉及共享的限额或只能处理一次的需求，就需要共同标识、已处理状态或适当的对账安排。一个组织内部的去重规则，无法自动约束其他组织独立维护的记录。

自动识别可以帮助寻找编号重复、时间重叠、内容相似和异常关联，但识别结果应当表达证据强度。系统高度怀疑两条记录对应同一事项时，可以提示核查；证据不足时，应保留不同主张及说明。错误合并会使真实贡献消失，因此解除错误关联与补回遗漏，也应当属于模型支持的正常操作。

面向未来，本书提出一个需要检验的制度设计方向：在保持个人与组织行动可辨认的同时，以共享的事项、成果和使用关系连接分散记录。其目标是减少重复取证和重复计量，让共同作用能够被持续追踪。若这种结构把难以形式化的协调工作排除在外，或让掌握登记入口的一方垄断贡献解释，就需要调整记录尺度和确认程序。

承诺、任务与贡献事件由此把共同创造连接为可以讨论和检查的过程。约定提供预期与条件，任务组织行动，事件保存实际发生的事项及其联系。记录越清楚，越能够容纳多人共同作用、延迟结果和必要修订，而不必把复杂协作提前压缩为一项确定价值。

但记录结构本身仍不能完成贡献确认。证据来自哪里、能够证明什么、谁有权确认，以及异议怎样改变结论，需要进一步建立明确程序。下一章将围绕这些问题，讨论贡献证据与确认程序，使可记录的行动逐步成为具有适当依据的共同判断。

定稿补强：人员贡献中的劳动与知识产权边界

员工、承包人、研究者和合作伙伴的贡献记录，不能用来改写其不可放弃的法定权利或既有合同义务。工资、最低报酬、工时、社会保障、职务成果、作者或发明人权利、商业秘密和许可范围，需要先依据关系类型和适用法域确定。贡献权益可以作为另行安排，不能当然替代应付报酬或法定义务。

记录人员贡献时，应保留关系类型、工作任务、既有报酬、知识产权归属或许可、数据使用范围、退出后持续权利和争议渠道。组织以后把成果识别为资本，不能倒推贡献者已经放弃原有权利；贡献者获得某项权益，也不能被解释为其自动承担无限经营风险。

本章工具与图表

本章的制度关系可结合[附录三](#)、[附录四](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

图14-1 从承诺、贡献到权益与回报

每个箭头都是独立判断关口，不允许用一条记录跨越全部制度门槛



《区块链——利益相关者资本论的底层技术》V1.0 · 可编辑SVG

图14-1 从承诺、贡献到权益与回报

图14-1 从承诺、贡献到权益与回报。每个箭头都是独立判断关口，不允许用一条记录跨越全部制度门槛

本章注释

1. [SRC-075] 万维网联盟（W3C）： PROV Data Model。 [原文或官方页面](#)

- 本章引证：W3C： PROV 数据模型。
- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：W3C： PROV 数据模型、W3C： PROV 数据模型中的衍生关系。
- 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-057] Microsoft： Microsoft： 事件溯源模式。 [原文或官方页面](#)

- 本章引证：Microsoft： 事件溯源模式。
- 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：Microsoft： 事件溯源模式。
- 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
- 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。

3. [SRC-047] Cloud Native Computing Foundation / CloudEvents： CloudEvents： 事件标识与来源规则。 [原文或官方页面](#)

- 本章引证：CloudEvents： 事件标识与来源规则。
- 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：CloudEvents： 事件标识与来源规则。
- 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
- 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第十五章 贡献证据与确认程序

共同创造被记录下来之后，组织仍然需要决定哪些主张可以得到承认。一次提交说明有人作出了陈述，一组材料提供了检查线索，一次签名可以固定某个主体表达的内容，但它们不会自行组成一个充分的贡献结论。确认程序的任务，是让材料与主张建立可以解释的联系，并使有权判断者对采用和排除证据的理由负责。

这种程序影响利益相关者能否被准确承认。证明要求过于宽松，虚报和重复认可可能损害共同资源；证明要求脱离现实取证条件，又可能排除真实但不易量化的劳动、知识和协作。有效制度需要同时处理错误认可与错误排除，而不能只追求记录完整、审批迅速或争议数量减少。

上一章建立了承诺、任务与贡献事件的联系。本章进一步讨论证据怎样支持具体主张，谁参与确认，分歧怎样进入复核，以及程序本身如何抵御操纵。这里的确认，是在明确范围内形成可以被组织采用的判断；它不直接等同于资本已经形成，也不预先决定收益和治理权的配置。

一、证据来源、证明范围与质量分级

证据首先需要对应一个清楚的待证问题。某项行动是否发生，是否由所声称的主体完成，是否满足交付条件，是否被实际使用，以及是否对一定结果产生作用，是不同的命题。若把它们合并为“是否有贡献”，审核者就容易凭整体印象作出结论，参与者也难以知道究竟哪一部分得到认可。

贡献主张因此应当说明主体、行动、对象、期间和所请求确认的范围。证据审查再逐项回答哪些材料支持这些内容，哪些材料与之冲突，哪些问题仍然没有依据。先限定命题，再组织证据，可以避免材料很多却无法回答核心问题，也能避免把证明范围较窄的材料赋予过大的含义。

证据来源可以包括参与者的过程记录、接收者的交付回执、业务系统日志、设备采集数据以及独立检查形成的材料。来源不同，观察范围和形成条件也不同。直接参与者可能掌握细节，却存在自身利益；外部检查者可能相对独立，却只能观察有限时点。来源身份只是判断质量的一个因素。

原始材料、整理结果与后续解释也应当区分。汇总表可能从大量记录中抽取数据，评价报告可能进一步采用筛选和推断。审查需要了解这种转换是否保留了原有含义，遗漏了什么，以及能否返回必要的依据。排版完整、语言专业或图表精细，不会单独提高材料对事实的证明力。

密码学检查有明确而有限的作用。W3C 的可验证凭证模型说明，凭证的可验证性不意味着其中主张真实；验证者仍需依据业务规则判断是否采用有关声明。对贡献证据也是如此：签名和完整性检查有助于核实来源及内容变化，却不能替代对行动、履约和作用的审查。W3C：可验证凭证的验证与业务判断〔1〕

质量判断可以从相关性、来源可靠性、内容完整性、覆盖范围、时效和可复核性等维度展开。相关性要求材料真正回答待证问题；可靠性关注形成条件和来源；完整性关注重要部分是否遗漏或改变；覆盖范围说明检查触及了多少对象和期间。这些维度需要结合，不能由一个强项自动弥补所有缺口。

证据数量与证据质量也不能混同。PCAOB 的审计证据标准区分数量上的充分性与相关性、可靠性所构成的适当性，并指出增加同类材料不能弥补其质量缺陷。本书借鉴的是这一方法区分，不将财务审计标准直接设为所有贡献确认的统一规则。PCAOB：AS 1105《审计证据》〔2〕

多份材料是否提供了新的支持，需要检查它们的独立程度。不同账户转发同一份报告，可能只有一个原始来源；同一系统生成的多种图表，也可能共享同一个错误输入。相互印证应当增加对事实的认识，而不只是增加表达同一结论的次数。

质量分级应当以特定命题及其证据组合为单位，而不宜给某个人或某类文件永久贴上高低标签。本书提出以下分级摘要，作为组织设计时可以调整的表达式。它不是统一行业标准，也不对应预设的真实性概率；采用哪一级作为某项行动的依据，需要另行规定。

支持程度	对特定命题的证据状态	确认程序中的主要用途
线索性	有可供调查的信息，来源或关键联系尚待核实	登记主张并确定补充核查方向
有限支持	部分事实得到支持，关键范围或条件仍有缺口	形成分项判断并说明尚待解决的问题
充分支持	在约定范围和判断标准下，必要事实已有足够依据，实质冲突得到处理	支持相应范围内的确认决定
强化支持	在充分支持基础上，关键环节得到额外检查或更广范围的检验	服务于后果较大或持续依赖程度较高的事项

分级摘要必须同时附带适用命题、检查范围和限制条件。一份材料对“已经收到交付”可以提供充分支持，对“产生了长期经营价值”却可能仍只是线索。对后一个命题提高要求，不应顺带取消前一个已经得到支持的事实；对前一个命题的认可，也不应自动扩张为后一个结论。

等级不应由确认人数或出具者头衔机械决定。关键在于实际检查了什么，以及检查方式是否能够发现所关心的错误。一次范围明确、方法适当的直接核验，可能比多轮未接触原始材料的签字更有意义。独立复核可以增强某些判断，却不是让所有材料自动升级的仪式。

重要反证需要进入同一审查范围。支持性材料很多，并不能使一项足以改变结论的矛盾消失。审核者应当说明矛盾指向的是主体归属、数量、质量还是结果解释，并决定是否补充核查或限制结论。质量分级应当随着新的实质材料更新，而不能成为阻止进一步提问的标签。

材料缺失的后果也需要结合记录责任判断。若组织控制关键数据并负有保管义务，不能只因参与者无法自行提供该数据就否定主张。制度可以要求保管者说明缺失原因，并寻找其他核验路径。缺少记录既不动自动证明行动发生，也不自动证明行动没有发生。

不同类型的贡献还需要不同证据组合。持续协调、隐性知识传递或风险预防，可能依赖期间记录、相关主体说明和实际运行资料共同支持。不能因为它们没有单一文件或即时财务结果，就预先认定证据质量低；但对其作用的解释仍需要限定范围，保留不确定性。

证据质量的制度意义，最终是让组织知道自己凭什么作出判断，以及判断可以被依赖到什么程度。它服务于有依据的承认，不是把全部共同创造压成一个“可信分”。当证据足以支持某项事实时，后续仍需另行讨论贡献计量、资本形成与权益安排。

二、自报、互证、业务验证与独立复核

不同确认方式承担不同工作。自报让参与者表达行动及其主张，互证补充协作各方的观察，业务验证检查材料与实际过程是否对应，独立复核则检验初始判断及其依据。四种方式可以组合，但不应被设置为所有事项必须逐级经过的固定阶梯。

自报具有不可替代的信息入口作用。参与者通常最先知道自己做了什么、遇到哪些条件限制，以及哪些工作没有进入现有系统。允许自报，能够使组织看到常规记录未覆盖的行动。自报的存在说明主张被正式提出，不表示该主张已经获得共同认可。

有效自报应当区分直接观察、根据材料得出的判断和个人估计。参与者可以引用已有事件，说明自己的具体作用，列出可核验依据及已知限制。无法确定的数量或影响应当明确标注，不能通过表单强迫填入一个看似准确的数值，再把系统要求造成的推测当作已经证实的事实。

自报责任也需要与组织提供的条件相配合。参与者应当对如实说明负责，组织则应当提供可理解的要求、必要的记录支持和补正机会。表达能力、数字工具熟练程度或是否擅长制作材料，不应成为真实贡献能否被看见的决定性条件。

互证能够增加不同位置的观察。接收者可以说明收到什么，共同执行者可以说明分工与配合，实际使用者可以说明采用情况。每个确认者都需要限定自己的所见及依据。只负责接收的人不宜被要求确认全部质量，未接触后续使用的人也不应被默认认可长期效果。

互证还应当允许部分认可和明确保留意见。确认者可以承认某项行动发生，同时对数量或作用提出不同判断。若界面只提供整体同意与整体拒绝，参与者可能为了不阻断合作而认可自己没有核验的内容。分项确认能够使协作关系与事实判断获得更准确的表达。

业务验证把主张放回实际运行过程。验证者可以比对任务范围、交付对象、接收记录、使用情况和有关结果，检查不同材料之间的联系是否成立。这里关注的是业务条件是否满足，而不只是记录字段是否齐全，或者几个系统显示的数字是否相同。

业务系统也可能共享同一输入，因此对账一致不总是增加独立支持。验证应当在需要时返回原始形成环节，检查对象、口径和例外情况。自动规则可以发现遗漏、重复和范围冲突，但对复杂质量、归因和合理例外的判断，需要保留相应人工职责。

独立复核则需要与原始提交和初次判断保持适当距离。独立性不仅涉及是否来自组织外部，也涉及任命、报酬、利益关系和报告路径。复核者如果必须依赖被复核者挑选材料，或者其回报直接取决于认可数量，形式上的外部身份也难以提供充分保障。

复核还需要能力与范围相匹配。具备一般管理资格，不意味着能够判断所有专业交付；具有技术能力，也不意味着可以自行决定分配原则。组织应当明确复核者检查的是事实、方法、程序还是特定结果，并为必要的专业协助和回避安排提供条件。

本书建议根据错误后果、材料复杂程度和既有控制条件选择确认组合。范围明确且后果有限的事项，可以采用较简洁的核验；影响较大、关联复杂或存在实质矛盾的事项，需要更深入的检查。具体门槛应当由组织依据自身活动确定，不能从采用区块链这一事实直接推导。

抽查可以帮助发现常规流程中的缺陷，但需要说明抽取对象和结论范围。针对异常事项的检查有助于处理具体风险，适当的随机抽查则可能发现现有规则没有识别的问题。少量检查通过，不能被写成全部事项都已逐项核验；样本覆盖的期间和类型也应当可查。

确认流程还需要明确谁负责使事项得到处理。受理时可以登记主张范围和材料缺口，进入判断前核实权限与利益冲突，作出结论时说明采用的证据和适用规则。材料需要补充，应当说明原因及下一步责任，避免把事项长期留在没有解释的等待状态。

结果表达应当围绕确认对象展开。可以分别说明哪些事实得到认可、认可范围多大、哪些内容不予认可、哪些仍待核验，以及结论适用哪个规则版本。决定作出者、时间、依据和复核入口应当与结果一起保留。只有一个批准标记，难以支持后续计量和必要纠错。

存在意见分歧时，组织可以依据既定权限和程序形成可执行决定，但程序性表决不能把所有不同判断变成虚假。决定应当解释怎样处理关键反对理由。技术共识可以固定决定记录，治理程序可以确定采用哪个结论，二者都不意味着事实因多数赞成而自然改变。

确认工作本身也需要资源和评价。若组织不安排审核时间、专业能力和资料访问，只要求尽快完成审批，制度就容易退化为形式签字。确认者的工作质量，应当结合理由是否充分、范围是否恰当以及复核发现的问题判断，而不能仅以通过率或处理数量衡量。

通过这样的分工，自报提供主张入口，互证增加观察位置，业务验证检查现实联系，独立复核约束初次判断。它们共同形成一种能够说明理由的确认秩序，使利益相关者获得承认时有依据，受到否定时也有可以回应的具体问题。

三、异议、申诉与确认结果修订

确认程序必须允许自己的判断受到检查。贡献涉及多人协作、不同观察位置和延迟显现的结果，初次决定难以预先穷尽全部材料。异议与申诉为程序提供纠正路径，也使参与者能够在不退出共同关系的情况下表达分歧。它们应当作为制度的正常组成部分。

本书在程序设计上作如下区分：异议是对材料、事实、归属或判断依据提出具体问题；申诉是对已经作出的决定，依照规定请求再次审查。组织可以采用不同名称，但需要让参与者清楚何时可以提出问题、向谁提出，以及提出之后将发生什么。

可以提出异议的主体，不宜只限于最初申报者。共同参与者可能发现归属遗漏，接收者可能发现确认范围超过实际验收，承担后续义务的一方也可能掌握相反证据。程序应当说明哪些主体具有相应的参与资格，同时为其他线索提供适当入口，避免无关请求无限阻断处理。

有效入口应当能够对应具体事项和理由。参与者可以指出哪项事实有误、哪份材料遗漏、哪些规则使用不当，或者哪个确认者存在利益冲突。组织不应要求其在申请受理之前就完整证明最终结论必然错误，否则申诉程序可能把本应由复核完成的工作全部推给申请人。

受理与认可也需要区分。收到异议后，程序可以先检查是否属于处理范围、是否存在明确问题以及需要哪些补充材料。进入复核并不意味着原决定已经被推翻，不予受理也应当说明理由和可以采取的下一步。系统的状态应当表达这些区别，而不能只显示申请失败。

参与者需要取得足以回应决定的必要信息，包括所适用的规则、关键事实判断及不予认可的理由。涉及他人隐私或商业秘密时，可以采用限定查阅、适当遮盖或由有权复核者查验等方式。保护材料不应使当事人连针对自己的主要不利主张都无法理解。

对新出现且可能影响结果的不利材料，应当给予有关主体适当说明机会。回应可以澄清观察范围、补充遗漏背景或指出材料错误，并不要求双方在所有价值判断上达成一致。程序需要保留不同意见及处理理由，使决定建立在可以回应的依据之上。

复核者的安排应当减少原判断的自我保护。原确认者可以解释其理由，但不宜独自掌握是否允许复核及最终处理的全部权限。根据事项性质，可以由未参与原决定的人员、跨职责小组或外部专业人员承担审查，并检查其能力、利益关系和资料取得条件。

程序也需要规定合理期限、延期理由和超期后的处理责任。期限应当从明确的通知或材料可得条件起算，避免当事人尚未获知决定就失去回应机会。对于后来才发现的重要材料、明显程序缺陷或其他规定情形，可以设置例外受理条件，兼顾结论稳定与必要纠错。

申诉期间如何执行，应当单独决定。并非每项异议都需要暂停全部安排，也不能让所有决定在复核完成前无条件产生难以调整的后果。本书建议结合争议范围、执行可逆性、潜在损害和现有证据，分别处理无争议部分与争议部分，并由有权主体说明继续执行或暂缓的依据。

暂缓措施本身应当具有范围、期限和复查安排。为了核实一部分数量而冻结全部无关主张，可能扩大争议造成的损害；对可能重复执行的争议请求完全不作控制，又可能使后续纠正更加困难。措施的目的在于保留适当处理的条件，不应提前充当对申请者的处罚。

修订决定需要明确属于哪一种变化。事实纠正、贡献归属调整、确认范围收缩、适用规则纠正和程序性重新审查，具有不同后果。新决定应当关联原决定，说明变化依据、生效范围和仍然保留的部分，使采用者能够理解当前可以依赖的结论。

历史记录与当前结论也应当分别呈现。原决定可以保留为曾经作出判断的证据，但不能继续被默认显示为现行结果。链上可以追加修订及关联信息，链下系统则需要更新当前状态和必要提示。数据仍可追溯，与错误结论继续有效，属于不同问题。

修订还需要追踪下游采用情况。贡献结论可能已经进入计量、资本记录或收益处理，相关系统应当收到变化，并依据各自规则重新检查。本书不将贡献修订直接写成资产自动收回；已经发生的支付、已形成的请求及其他主体的依赖，需要按照适用安排分别处理。

发现系统性错误时，纠正范围也不宜停留在最先申诉的人。相同规则、相同来源或同一审核方法可能影响一组事项。组织应当检查是否需要扩展复核，并通知相关主体。纠错机制若只补偿最善于提出异议的人，可能保留同类错误造成的不平等。

异议成本也会影响程序能否实际使用。过高费用、复杂材料要求、必须依赖原审核者提供帮助，以及对提出问题者的不利对待，都可能使形式存在的程序难以发挥作用。制度应当提供必要说明和协助，并限制因善意申诉而发生的报复。未获支持的申诉，不应仅凭结果就被认定为恶意。

结论的稳定性仍然需要维护。对已经处理且没有新理由的重复请求，可以依据明确规则不再重复全面审查，但应说明前次处理及适用依据。重新开启的条件、内部处理的终点和可能的后续争议途径应当清楚，避免一方面无限悬置，另一方面用“最终结果”掩盖未经处理的重大问题。

由此，申诉与修订形成对确认权的持续约束。可信的程序不以从不改变结论证明自身正确，而是能够说明为何维持、为何修订，以及变化怎样传递到后续安排。可修订性只有与理由、权限和稳定规则结合，才能改善共同创造中的预期。

四、防止串谋、虚报与评价操纵

贡献确认一旦影响资源和机会，就需要考虑参与者如何利用规则。风险不仅来自申报人虚构事实，也可能来自确认者相互照顾、管理者压低他人贡献，或者规则制定者改变口径以有利于特定群体。治理需要观察从材料形成到最终采用的整个过程。

串谋、虚报与评价操纵具有不同结构。串谋是有关主体协调行动，利用表面独立的身份或职责影响判断；虚报涉及对行动、数量、归属或结果作出不实陈述；评价操纵则可能在事实表面真实的情况下，通过选择指标、样本、期间或比较范围改变呈现效果。三者可以交织，也需要分别核查。

防范应当同时包括事前约束与事后发现。GAO《绿皮书》将内部控制用于组织运行、报告与合规目标，并提供预防性、发现性控制及相关数据来源的设计参考。本书借鉴这种分层思路，将贡献确认的预防、检查和纠正相互连接，不将该公共部门框架直接视为本书模型的效力依据。GAO：内部控制《绿皮书》〔3〕

事前约束首先涉及职责与利益关系。提交、确认、例外批准和执行，不宜在重要事项上由同一主体不受检查地全部控制。确实难以分工的小型组织，可以设置有记录的事后复核或其他制约，并说明其局限。职责分离的实际效果取决于相互检查是否存在，不能只看系统中设置了多少角色。

互证安排尤其需要防止把熟悉关系变成互相放行。长期合作可以增加对事实的了解，也可能形成相互依赖。组织应当检查重要确认是否长期集中在固定关系内，必要时改变复核安排，并要求说明影响独立判断的关系。发现密切联系是进一步核查的理由，不足以单独证明参与者串谋。

审核者的选择和报酬也会影响判断条件。若报酬只随认可金额增长，或者只奖励否决数量，就可能形成偏向。本书建议依据核查工作、专业要求和判断质量安排审核资源，同时通过抽查、回避和适当轮换限制长期依附。轮换并不能替代能力要求，也不能保证来自同一利益网络的人真正相互独立。

虚报可以发生在不同阶段：把承诺写成已投入，把提交写成已验收，把访问记录写成实际使用，或者把整体结果全部归于个人。前几章对主体、阶段和事件的区分，为发现这些问题提供了检查位置。核验者应当寻找关键状态之间缺少的依据，而不是只检查表单是否填满。

评价操纵还可能表现为拆分工作以增加条目，选择有利期间，隐去不利结果，或仅展示容易取得高分的活动。单条记录即使真实，整体呈现仍可能误导。确认程序需要检查申报范围和应当报告的事项，比较所选材料与实际业务总体的关系，避免只在被筛选后的材料中寻找一致性。

但是，防止遗漏不能转化为无限收集。需要收集哪些反向材料，应当与待证问题及原有记录义务相关。组织不应以防止操纵为由持续获取参与者全部活动。资料覆盖范围、保存责任和访问权限仍然需要受到约束，异常调查也应当说明具体目的和期限。

异常分析可以发现值得关注的模式，包括反复出现的相互高评、集中发生的异常调整或与业务规模不相称的申报。此类模式只能提供调查线索。真实的专业分工、紧密合作和季节性活动也可能形成相似表现，自动筛查应当保留解释与复核路径。

AI可以辅助整理材料、比对陈述和提示冲突，但其生成的摘要或风险判断需要返回原始依据。被标为异常，不等于已经证实虚报；未被标出，也不等于已经完成核验。用于关键决定时，组织需要明确人工职责，并检查系统是否持续误判某些角色、表达方式或贡献类型。

规则本身也应当接受操纵检验。公开条件有助于参与者形成预期，但若组织只奖励某个易计数指标，参与者可能逐渐把注意力转向指标而忽略共同目标。对此，需要检查指标是否仍能支持所声称的贡献，而不是把所有对规则的适应都认定为个人欺诈。制度造成的偏向应当通过适当修订处理。

规则修订不能成为事后否定履约的便利工具。发现旧指标容易被利用，可以调整未来安排；对过去事项则需要区分明确违反原规则、故意不实陈述和按照当时规则完成的行动。把不满意的制度后果一律归为参与者违规，会使贡献确认失去稳定依据。

发现问题后的处置应当区分材料错误、合理分歧、疏忽失职和故意操纵。它们可能都需要纠正记录，但责任和后续措施不必相同。限制资格、要求返还或采取其他处理，需要有适用规则、明确权限和相应证据，并保留说明与复核机会。技术触发不应替代这些条件。

提供线索者与被调查者都需要适当程序保障。线索可以在受控范围内核查，避免未确认指控扩散；有关主体应当能够回应关键问题。对提出善意问题的保护，与对恶意捏造事实的处理可以并存，但不能用后者威胁正常异议。调查者自身的利益关系和行为也需要监督。

确认制度的有效性应当通过多项结果检查：错误认可是否被发现，真实贡献是否被错误排除，申诉是否带来必要修订，处理成本是否可承受，以及长期难以表达的贡献是否持续被遗漏。投诉减少或通过率提高，都不能单独证明制度改善；它们也可能来自参与者不再愿意提出主张。

面向未来，本书提出一个需要实践检验的方向：让确认程序形成关于自身判断质量的记录。复核发现了什么缺口，哪些证据组合经常被误用，哪些主体反复承担不相称的证明负担，都可以成为修订依据。但不能用一个自动生成的审核者排名决定全部权力，应当保留理由审查、情境解释和正式授权。

贡献确认由此具有双重责任：对参与者的主张作出有依据的判断，也使判断权本身受到检查。区块链能够帮助保存提交、确认和修订的共同轨迹；证据制度、职责安排和异议程序则决定这些轨迹是否支持适当承认。技术记录与社会判断的联系，需要在这种相互约束中持续维护。

当贡献事实在一定范围内得到确认，组织才有较清楚的基础进一步讨论计量与评价。证据充分不意味着贡献价值已经精确确定，程序正当也不意味着所有贡献都能用同一尺度比较。下一章将转向贡献计量与价值判断，讨论事实怎样进入评价，以及评价应当保留哪些边界。

定稿补强：独立申诉与利益冲突回避

申诉程序只有在复核者能够相对独立地重新审视事实、规则和程序时，才具有纠错意义。原评价者可以说明理由，但不应独自作出终局复核。高影响事项应设置回避规则、复核席位、材料访问、举证责任、时限、暂缓执行和再审条件。

复核记录应保存原决定、申诉请求、补充证据、适用规则版本、回避情况和新结论。改判并不等于删除原记录；系统应以新的有效决定调整当前状态，并追踪受影响的资本判断、权益登记和分配。申诉长期积压、同类案件改判率异常或某评价者持续偏离，应当成为制度审查的信号。

本章注释

1. [SRC-076] 万维网联盟（W3C）：Verifiable Credentials Data Model v2.0。原文或官方页面

- 本章引证：W3C：可验证凭证的验证与业务判断。
- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：W3C：可验证凭证数据模型 2.0、W3C：可验证凭证中的选择性披露与隐私考虑、W3C：可验证凭证的参与角色与验证边界、W3C：可验证凭证的验证与业务判断、W3C：可验证凭证与数据最小化。
- 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-067] 美国公众公司会计监督委员会（PCAOB）：AS 1105《审计证据》。原文或官方页面

- 本章引证：PCAOB：AS 1105《审计证据》。
- 支持范围：用于确认财务、审计、内部控制或公司治理中的规范口径，本书引用主题包括：PCAOB：AS 1105《审计证据》。
- 使用边界：规范口径需要结合适用主体、报告目的和具体交易事实，不宜机械移用于链上权益。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：官方来源存在访问限制，已保留人工复核标记，核验日：2026-10-08。

3. [SRC-045] 美国政府问责局（GAO）：内部控制《绿皮书》。原文或官方页面

- 本章引证：GAO：内部控制《绿皮书》。
- 支持范围：用于确认财务、审计、内部控制或公司治理中的规范口径，本书引用主题包括：GAO：内部控制《绿皮书》。
- 使用边界：规范口径需要结合适用主体、报告目的和具体交易事实，不宜机械移用于链上权益。

- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：官方来源存在访问限制，已保留人工复核标记，核验日：2026-10-08。
-

第十六章 贡献计量与价值判断

贡献得到确认之后，组织仍然面临一个更困难的问题：怎样理解不同贡献的大小、作用与相互关系。确认解决的是在什么范围内可以承认某项行动及其结果，计量则需要选择描述和比较的尺度。两者相互关联，却不能因为事实已经得到核验，就认为贡献价值已经随之确定。

共同创造包含可以直接计数的交付，也包含持续维护、知识积累和关系协同。它们形成作用的时间不同，依赖条件不同，能够支持的比较也不同。若制度预先要求所有贡献都进入同一张排名表，模型可能优先照顾容易记录的活动，而使真正重要但难以压缩为单一数字的作用逐渐被忽略。

本章讨论计量应当如何服务于价值判断。重点不是寻找一条能够算出全部贡献真实价值的公式，而是说明事实如何成为指标，指标如何进入评价，以及评价如何在明确条件下支持组织决定。区块链可以帮助共同核验输入、规则和计算结果；尺度是否适当、判断是否合理，仍需要受到制度审查。

一、贡献事实、评价分数与经济价值的区别

贡献事实首先描述发生了什么。行动主体、投入范围、交付数量、使用期间及观察结果，可以在证据支持的范围内得到确认。其中有些事实天然具有数量形式，有些需要分类或文字说明。已经确认一项事实，并不意味着它已经具有可与其他事实直接相加的价值单位。

评价分数则是依据特定规则对事实进行转换的结果。选择哪些指标、采用怎样的尺度、怎样处理缺失和重叠，以及各指标占多大权重，都会影响分数。因此，分数不仅包含对现实的描述，也包含组织对于何种作用更值得关注的判断。

分数的含义应当与评价目的共同说明。衡量履约进展、比较阶段性表现、识别能力积累和安排某项激励，可能需要不同指标。为进度管理设计的评分，不宜未经论证就用于长期资本安排；用于识别服务质量的问题指标，也不一定适合直接决定个人收益。

经济价值进一步涉及有关活动和成果在特定条件下能够支持的经济作用。降低资源消耗、提高可用产出、维持协作能力或扩大未来选择，可能具有经济意义，但这些作用需要结合对象、期间、替代条件和实现可能性判断。它不能由某个内部积分的名称直接确定。

已经实现的经济结果与对未来作用的估计也需要区分。成本变化可以被观察，但仍须检查比较口径；未来收益可以被估计，却依赖尚未发生的使用和环境条件。组织应当说明评价针对哪一类对象，避免把一项预测写成已经获得的资源。

成本、价格与经济价值提供的信息并不相同。投入成本说明消耗了什么，交易价格反映一定条件下的交换结果，经济价值判断则需要考察资源和成果的实际作用。成本高可能来自复杂任务，也可能来自低效；价格高可能受到稀缺、议价和交易条件影响。任何一个数值都不宜独自承担全部贡献判断。

层次	主要回答的问题	需要保留的依据
贡献事实	谁做了什么，在何种范围内得到确认	事件、证据、确认范围与修订记录
评价分数	按什么目的和尺度，怎样描述或比较贡献	指标定义、转换方法、权重与规则版本
经济价值	在什么条件和期间产生或可能产生何种经济作用	使用条件、结果资料、比较基准及估计假设
权益安排	谁可以向谁提出何种请求或参与何种决定	制度依据、资格、义务主体与实现条件

共同创造还使价值归因具有复杂性。一项结果可能同时依赖当前劳动、既有知识、组织设施、客户采用和外部条件。把全部结果分配给最容易观察的最后环节，会遗漏其他作用；把每个必要条件都记为全部结果的创造者，又会重复计算。贡献关系可以帮助解释共同过程，但不动自动提供唯一的价值拆分比例。

对于个别主体的作用，比较“有其参与”和“没有其参与”可能提供分析思路，但后一种状态通常不能被直接观察。可以采用有依据的比较或模型估计，同时说明可替代性、其他投入变化和组织调整等假设。不能把在一个既定模型中计算出的差额，写成脱离条件的个人真实价值。

评价尺度还决定哪些数学运算有意义。顺序等级可以表达相对高低，却未必支持倍数比较；某人分数是另一人的两倍，不必然意味着其贡献作用也是两倍。若用于加总或比例分配，需要解释尺度是否支持这些运算，而不能只因软件能够计算就认为结果具有相应含义。

对不同单位进行标准化，可以让它们进入某种共同评价，但标准化不会消除制度选择。参照最高值、平均水平或预设目标，会得到不同解释；比较对象改变时，相对分数也可能改变。没有发生事实变化的主体，可能因参照组变化而得到新分数，这种变化应当被明确说明。

当差异很小而证据或方法的不确定性较大时，精确排名可能超出资料支持的程度。组织可以采用区间、等级或多维比较，并明确哪些对象尚不具备直接比较条件。适当地保留并列和不可比较，比用更多小数位制造确定次序更有解释力。

分数与分配比例之间也需要单独的制度连接。一个评分可以成为分配时的参考，却不能单凭分数生成可分配资源。即使组织约定按某种分数安排一部分资源，也仍需明确分配范围、资格、约束和兑现条件。这说明分数承担了制度选定的用途，不说明它已经成为货币价值的客观单位。

分配问题还可能包含贡献之外的原则。既有承诺、实际承担的义务、风险安排和对特定利益的保护，都可能影响决定。若这些因素需要发挥作用，应当明确写入相应规则，而不必事后修改贡献事实或偷偷调整分数，以使结果看起来完全出自贡献计量。

因此，本书坚持将事实、分数、经济作用与权益安排分别表达。事实提供基础，评价选择尺度，价值判断分析作用，制度决定可以产生怎样的权利义务。四者的联系需要被论证和授权，不能由一个不断累加的积分账户全部代替。

二、不同贡献类型的计量边界

计量从识别贡献类型开始，但分类不应仅按参与者身份划分。员工可以贡献知识，客户可以参与问题识别，供应商可以形成协同改进，合作伙伴也可能承担持续维护。角色说明参与关系，贡献类型说明实际作用；两者应当关联，而不宜互相替代。

时间与劳动投入可以记录持续期间、任务范围、投入强度和完成情况，但工时本身不能完全表达工作质量。时间较长可能源于任务困难，也可能源于返工；时间较短可能来自熟练能力，也可能意味着必要工作被省略。比较需要考虑任务条件，不能直接将工作时长排列成贡献高低。

标准化交付可以在对象和质量口径一致时进行数量比较，但可比性需要核实。交付单位是否相同、验收范围是否一致、是否包含维护和后续支持，都可能影响数量含义。把复杂交付拆成更多条目，并不会自然增加其实质作用；重复提交和必要修订也应当按原有任务条件解释。

知识与创新的作用可能体现为解决问题、形成方法、帮助后续工作或保留新的选择。材料数量、文字长度和被调用次数可以提供部分观察，却不足以独立说明知识质量。计量需要追踪必要的使用联系和后续作用，同时承认这些作用可能延迟显现，并依赖他人的补充投入。

知识可以被重复使用，但重复使用不等于重复发生同样规模的原始创造。原始成果、后续适配、持续维护和新的应用，应当分别记录。是否给予持续使用相应认可，可以由制度规定；这种安排不能通过把同一原始工作在每次使用时重新登记一遍来隐蔽实现。

资源提供需要区分资源数量、可用期间、使用限制和实际承担的风险。相同数量的资金、设备或数据使用条件，在不同期限和约束下具有不同作用。资源的名义规模不能单独决定贡献评价，更不能使资源提供者自动取得全部协作成果的归属。

客户参与和关系协同也不宜只按联系数量衡量。问题是否得到澄清、协作条件是否改善、关系能否持续以及是否发生实际采用，都可能比新增名单更有意义。关系具有多方共同维持的性质，组织不能把某个人认识的全部对象直接登记为其可转让资产，也不能把客户整体交易额全部归于某一次引介。

维护、协调和支持性工作经常表现为其他活动能够顺利进行。它们可以结合职责范围、服务覆盖、响应情况和运行结果评价，但不宜只按问题发生后的处理次数奖励。预防减少了故障，可能同时减少可见的处理记录；如果分数只奖励故障后的动作，就可能忽略预防作用。

风险承担与风险降低也要分别理解。承担经约定的资源损失可能性，与通过适当行动减少风险，是不同贡献方向。风险越大不意味着贡献越大，主动制造不必要风险也不能成为获得更高评价的依据。没有发生损失，只能作为观察结果，仍需检查有关防范行动和判断条件。

探索中的失败可以支持不同结论。已经排除的路径、验证过的限制或形成的新知识，可能具有后续作用；无效重复和未履行约定则需要另行处理。不能按成功结果一概抹去合理探索，也不能按投入规模一概肯定所有失败。事前目标、不确定性安排和实际证据应当共同进入评价。

贡献类型	可以采用的观察维度	主要计量边界
劳动与交付	实际投入、合格交付、完成范围	时间和条目数量不能替代质量与任务条件
知识与创新	问题解决、采用、适配和后续作用	新颖程度、使用次数与经济作用不能直接等同
资源与条件提供	规模、期限、可用性和限制条件	名义数量不能覆盖全部机会、约束和风险
关系与协同	协作改善、实际采用和关系持续	联系数量不等于稳定能力，作用通常由多方共同形成
WISERUNION · V1.0 维护与风险管理	覆盖、运行、预防与处置依据	无事故不等于无贡献，也不自动证明预防有效

这些维度提供的是可选择的观察位置，不是已经验证的通用评分表。每类活动需要结合组织目的决定取用哪些维度，并检查信息是否可靠取得。指标过多会增加负担和重叠，指标过少又可能遗漏关键作用，选择需要依据实际解释能力不断检验。

不同贡献类型之间，可能只适合进行有限比较。可以先在较可比的任务和作用范围内评价，再由明确程序处理跨类型的资源安排；也可以保留多维结果，不强制产生一个总分。组织需要作出决策，并不意味着现实中必然存在一把适用于所有贡献的共同尺子。

参与机会也会影响观察结果。任务分配、资料权限、客户接触和资源支持不同，会影响谁有机会形成可见产出。评价可以解释这些条件，不能把机会差异全部写成个人能力差异；但解释条件也不能凭空补记没有发生的贡献。事实记录与对条件的裁量仍应当分开。

对没有数据、不适用和经核验没有发生，需要采用不同状态。缺少使用信息不应直接填为没有使用，不适用的指标也不应机械记零。若估算缺失值，需要说明估算依据及其影响，并保留真实记录与估计部分的区别，防止估计在多轮处理后被误认为原始事实。

本书据此主张，贡献计量应当允许数量、分类、区间和理由说明共同存在。能够准确计数的部分可以充分使用计算，依赖复杂判断的部分应当保留解释条件。承认计量边界，不会取消比较和决策，而是使比较知道自己适用到哪里。

三、权重、时间因素与不确定性的处理

权重说明在一套评价规则中，不同维度怎样共同影响结果。它可以反映组织对质量、及时性、持续作用或协同条件的关注，但需要说明服务于哪个目的。权重一旦影响参与机会或资源安排，就成为具有分配后果的制度参数，不能仅被当作技术人员可以自由调整的配置。

权重的依据可以来自组织目标、专业判断、参与者协商或经验研究，但这些依据不能互相冒充。数据可以帮助理解某个指标与观察结果的关系，却不自动决定该指标在制度上应当多重重要。由统计结构生成的权重，也需要检查其是否符合评价目的，不能因为由算法产生就免于说明。

等权重同样是一种选择。把各维度平均对待，并不意味着没有价值判断；如果某个作用被拆成多个相近指标，它可能在平均加权中获得更大实际影响。因此，需要检查指标之间的重叠和包含关系，避免通过增加名称相似的项目，重复强调同一种作用。

在适用条件明确时，可以用简单的加权模型表达综合评价：先按规定方法将各指标转换到适当尺度，再将转换值与相应权重相乘并求和。若采用非负且总和为一的权重，结果可以被解释为这套尺度下的加权平均。这只是一个可选的评价模型，不是贡献经济价值的定义。

这种相加方式隐含了不同维度可以按一定比例相互补偿的安排。较高数量可能补偿较低质量，较高及时性也可能抵消其他不足。若某些质量条件、授权要求或必要义务不允许被抵消，就应当作为独立条件检查，而不能仅给它们较低分数后继续与其他项目相加。

综合评价还可能遗漏共同作用。两个环节各自具备能力，并不必然意味着相互协作有效；某项贡献的作用也可能只有在另一条件成立时出现。模型可以为此保留共同评价或明确的条件关系，但增加复杂参数之前，需要有足够依据支持其含义，避免用复杂性代替认识。

权重应当经过适当的讨论、授权和版本管理。受到影响的各类参与者需要能够理解主要选择及其后果，提出没有被覆盖的作用。治理程序可以形成一套供当前使用的规则，同时保留分歧；多数接受不意味着权重已经成为自然规律。

时间处理需要先区分行动发生期间、效果观察期间和评价结算期间。一项行动可能在较早期间完成，后续才被采用并显示作用。评价不能把尚未成熟的结果与已经充分观察的结果直接比较，也不能让延迟录入改变实际行动的归属期间。

不同贡献的持续方式也可能不同。某些作用集中于一次交付，某些需要持续维护，某些知识则可以在较长时间内被使用。采用统一的时间衰减系数，可能无法表达这些差异。是否衰减、衰减什么以及依据何在，应当与具体评价目的和使用条件联系。

历史事实不会因为时间经过而不再发生过。当前作用可能下降，某一时期的评价权重可以依规则变化，但这些变化不应自动抹去历史贡献，也不应单独取消已经形成的权益。贡献记录、当前评价和权利存续的时间条件，需要分别维护。

持续使用还需要避免跨期重复累加。每个期间可以记录新的使用和维护事实，但不能在每个期间都把同一原始投入当作重新发生。若制度希望对持续作用安排阶段性认可，应当明确使用期间及相应依据，让原始贡献与后续贡献各有可解释的联系。

不确定性则需要分清来源。原始数量可能存在测量误差，贡献归因可能依赖不完整模型，未来作用可能受尚未发生的条件影响。对权重是否合理价值分歧，则属于另一类问题，不能简单当作统计误差，通过求平均就认为已经解决。

计量学中的不确定性表达提供了一项方法启发：输出的不确定性需要考虑输入及其在模型中的关系。JCGM 的测量不确定性指南对此作了系统说明。本书仅借鉴明确输入、模型和不确定性联系的思路，不把社会贡献直接当作具有统一物理量纲的测量对象。JCGM：《测量不确定度表示指南》第一部分 [2]

贡献评价可以根据资料条件表达区间、情景和暂时无法判断的部分。区间应当说明来自数据误差、合理参数变化还是不同未来情景。没有相应统计模型和依据时，不宜把主观设定的上下限称为某个概率水平的置信区间；增加计算位数也不会减少原有不确定性。

证据支持程度与贡献大小还应当分别呈现。证据薄弱需要补充核查或限制判断范围，却不意味着实际贡献必然较小。把证据等级直接乘为折扣系数，可能使难以留痕的活动长期处于不利位置。如果组织确需在证据未完备时作出暂定安排，应当说明它是处置规则，并保留补正后的调整路径。

敏感性分析可以帮助识别哪些选择真正左右结论。可以在有理由的范围内改变权重、观察期间或缺失数据处理方式，检查排序和等级是否大幅变化。综合指标手册将敏感性与稳健性检查作为评价方法影响的重要环节；本书将其用于提示计量结论对既定选择的依赖。OECD / 欧盟联合研究中心：综合指标的敏感性与稳健性〔1〕

若很小的合理调整就使结论反转，应当限制对精确名次的依赖，考虑区间、分组或进一步审议。反之，在若干合理设定下保持稳定，也只说明结论对这些设定较稳健，不证明原始数据必然真实，更不证明所有可能的制度选择都支持同一结果。

处理权重、时间和不确定性的目的，是让评价结果携带自己的适用条件。参与者应当能够看出哪些差异来自事实，哪些来自尺度选择，哪些仍取决于未来观察。这样的计量才可能支持稳定协作，而不把暂时判断固化为无法解释的确定值。

四、自动计算与人工裁量的衔接

自动计算能够按明确规则处理大量记录，完成单位换算、范围汇总、重复排除和规定公式的运算。它使同一条件得到一致处理，也能保存计算依据。但计算执行正确，只证明系统按给定输入和规则得到相应结果，不证明输入已经充分，也不证明规则适合当前事项。

自动化范围应当从可明确表达的条件开始。输入来源是否符合要求、确认状态是否有效、记录是否处于所选期间、适用版本是否一致，以及必需字段是否齐备，都可以形成检查规则。条件不满足时，系统应当说明缺口，不能为了得到一个完整分数而自行补出事实。

对计算结果的复核，需要能够取得适当的输入快照、规则版本、参数和处理说明。事实修订、规则改变与计算错误应当分别标明，避免每次分数变化都被理解为贡献发生变化。涉及不同单位、取整、精度或边界值时，也应当保持明确约定，防止实现细节改变实质结果。

区块链可以在需要共同验证时记录输入承诺、规则标识及结果，并为有权核验者保留重算或验证条件。完整的敏感材料不必因此全部公开。无论计算在链上还是链下，独立复核都需要足够依据；只有一个无法检查的总分被写入账本，并不会使计量方法更加可信。

人工裁量承担的是规则无法充分覆盖、证据需要解释或多个合理原则发生冲突时的判断。跨类型比较、共同成果中难以拆分的作用、特殊条件对结果的影响，可能都需要这种判断。裁量的存在应当被明确承认，同时规定谁可以作出、针对什么事项以及必须说明哪些理由。

裁量不应表现为在没有记录的情况下直接改写分数。可以保留原始计算结果，由有权人员形成调整建议，说明适用条款、补充材料、调整范围和理由，再依程序形成决定。原始结果、调整意见和最终采用值分别存在，才能使参与者了解差异来自哪里。

对同类情况，需要检查裁量是否保持合理一致。相似事项得到不同处理时，应当能够说明重要条件的差异；不同事项得到相同分数时，也需要留意统一规则是否抹去了实质区别。制度可以逐步整理经审议的解释口径，但不宜把每一次例外都自动推广为新规则。

裁量权限本身也需要受到约束。评价者的利益关系、专业能力和参与范围应当明确，重大调整可以采用额外复核。受到影响的参与者应当获得必要理由及异议入口。让人签字并不自动增加正当性，只有其真正承担检查、解释和责任，人工参与才具有实质意义。

AI 辅助评价还需要区分资料整理、分类建议和实质判断。模型可以帮助发现遗漏、关联事件或比较文字说明，但对复杂贡献给出的评分仍需说明依据与限制。历史评分可以成为分析材料，却不能因来自过去的人工决定，就被默认当作无偏的真实价值标签。

NIST 的 AI 风险管理框架讨论了复杂人类现象被数学模型表达时可能丢失必要语境，并强调区分人与 AI 在决策和监督中的职责。本书据此重视人机分工的明确性，不假定增加人工参与或采用 AI 本身就能自动消除偏差。NIST：《AI 风险管理框架 1.0》附录 C〔3〕

对用于评价的 AI 输出，应当保留必要的输入范围、模型版本、生成结果及人工采用情况。重复提出相同问题，不一定天然得到完全相同的输出，因此不能把模型的一次回答直接当作可稳定重算的制度公式。若将其纳入正式流程，需要说明哪些输出可以采用，以及出现不同结果如何处理。

人工复核也不应只是认可系统建议的最后一步。复核者需要有时间和材料检查关键依据，有权限要求补充说明或不采用建议，并能够说明自己的决定。系统可以展示分数由哪些事实和规则构成，减少对单一排名的依赖，使复核围绕具体问题进行。

自动结果与人工判断发生冲突时，应当区分冲突来源。若是程序没有正确执行规则，应当修复计算并检查影响范围；若是规则遗漏重要情形，应当依据现有例外程序处理，并考虑后续修订；若是对事实仍有争议，则应返回贡献确认程序。三类问题不宜都通过临时修改参数解决。

计量结果进入资本和权益安排之前，还需要进行相应制度检查。哪些主体符合条件，哪些记录尚有争议，哪些资源已经确定可以分配，以及哪项规则授权采用该评价，不能被一个计算成功的状态覆盖。事实确认、评价完成与权益执行应当通过明确接口衔接。

规则升级应当保留生效范围与迁移安排。系统可以使用历史材料比较新旧模型的影响，检查哪些贡献类型或主体受到显著变化，但回溯试算并不自动授权重写已经处理的权益。正式修改需要经过相应审议，并说明对当前期间、未决事项和未来活动分别如何适用。

实施前后的检验也应当同时关注计算和制度效果。计算能否准确执行既定规则，属于实现问题；规则是否系统性遗漏某类作用、是否诱导无效活动、参与者是否能够理解和质疑结果，则属于制度问题。仿真和有限试行可以提供线索，不能单独证明真实组织中的长期效果。

面向未来，本书提出一个需要检验的方向：让评价系统同时展示事实依据、不同合理设定下的结果以及需要裁量的问题，由有权程序决定当前采用的安排。技术可以扩大组织理解选择后果的能力，而不必将价值判断集成为一个不可讨论的总分。如果这种设计增加了理解负担或使责任模糊，就需要收缩模型复杂性和自动化范围。

至此，贡献确认这一篇形成了从主体与关系，到承诺与事件，再到证据、确认和评价的联系。每一步都增加了组织可以采用的信息，也提出新的判断条件。共同记录提供连续性，计量模型提供有限尺度，程序则使这些尺度能够被解释、质疑和修订。

经过评价的贡献仍然不是自动成立的资本。贡献能否被持续使用、被组织吸收并进入具有明确风险与权利义务的安排，还需要进一步论证。下一篇将转向资本形成与权益配置，从资本形成条件和账户体系开始，讨论共同创造怎样成为能够长期维持的制度关系。

定稿补强：评价者问责与数值用途

人工裁量需要理由，而不是只留下一个分数。评价者应记录判断依据、证据范围、不确定性、利益关系和适用权重；组织通过双评抽样、跨组一致性、偏差监测、申诉改判率和定期校准检查裁量质量。出现系统性偏差时，应调整规则、培训或权限，而不是仅修改单个结果。

每个数值还必须注明用途。贡献数量、评价分数、内部管理值、交易价格、经济估计与会计金额具有不同目的和条件，不能因数字形式相同而互换。建议统一记录计量目的、单位、基准日、方法、假设、区间或不确定性、批准人和禁止用途。模型输出应保留版本和敏感性，避免把复杂判断包装成虚假精确。

本章注释

- [SRC-064] 经济合作与发展组织（OECD）：[OECD／欧盟联合研究中心：综合指标的敏感性与稳健性](#)。[原文或官方页面](#)
 - 本章引证：OECD / 欧盟联合研究中心：《综合指标构建手册》；OECD / 欧盟联合研究中心：综合指标的敏感性与稳健性。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：OECD / 欧盟联合研究中心：《综合指标构建手册》、OECD / 欧盟联合研究中心：综合指标的敏感性与稳健性。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-022] 测量指南联合委员会（JCGM）：[Guide to the Expression of Uncertainty in Measurement, Part 1](#)。[原文或官方页面](#)
 - 本章引证：JCGM：《测量不确定度表示指南》第一部分。
 - 支持范围：用于支持所引理论、模型、算法或经验研究的原始论证，本书引用主题包括：JCGM：《测量不确定度表示指南》第一部分。
 - 使用边界：原始研究支持其设定范围内的结论，不直接证明本书提出的治理制度已获得普遍实证验证。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-063] 美国国家标准与技术研究院（NIST）：[《AI 风险管理框架 1.0》附录 C](#)。[原文或官方页面](#)
 - 本章引证：NIST：《AI 风险管理框架 1.0》附录 C。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：NIST：《AI 风险管理框架 1.0》附录 C。

- 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本 and 责任的独立判断。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第四篇 资本与权益：从 贡献记录到制度化权利

共同创造经过记录、核验和评价之后，组织已经能够说明参与者做了什么，以及怎样理解这些行动。但资本形成提出了进一步的问题：这些行动留下了什么，可以被谁在什么条件下继续运用，又由谁承担维持这种可用性的责任。过去的贡献与未来的创造条件，只有通过真实积累及相应制度安排才能连接起来。

第四章已经界定利益相关者资本，并区分可记录、可计量与可资本化。本章不再重述定义，而是处理其中最关键的转化关口：哪些经确认贡献被组织吸收为可以跨期运用的资源、能力与合作关系，以及这种状态如何被账户体系持续管理。

资本形成既需要辨认实际积累，也需要安排使用、维护、风险与权益。账户体系则把这些不同对象分别表达，使参与者能够追溯来源、检查当前条件并理解自己的主张。它的作用，是帮助制度准确承认和持续管理资本，而不是通过登记创造原本不存在的能力或资源。

一、贡献转化为资本的制度条件

贡献是已经发生的行动，资本形成关注这些行动是否留下可以延续的创造条件。完成一次任务，可能消耗了当期资源，也可能同时形成方法、设施、知识和合作能力。两种结果可以并存。判断资本形成，需要从行动完成之后的实际状态出发，不能仅按历史投入或评价分数的总量推算。

首先需要识别资本对象。所形成的是哪项资源、哪种能力或哪一组合作关系，支持什么后续活动，依赖哪些条件，应当可以说明。对于能力和关系，可以不要求其像实物一样独立存放，但需要有能够检查的作用范围和存续依据，不能只用“信任”“生态”或“影响力”等名称代替具体内容。

对象还应当与形成过程建立联系。哪些贡献提供了来源，哪些后续工作完成了整合，哪些既有条件共同参与形成，决定了资本不能被简单归给最后登记者。来源联系帮助解释积累怎样产生，但它并不自动给出各方拥有多少份额；归属及权益仍需依据相应安排确认。

持续可用性是另一项条件。某项成果必须具备进入后续创造的实际条件，而不只是存在于档案中。适当的使用权限、必要的配套资源、能够操作的人和可以维持的协作安排，都可能影响可用性。成果保存完整，却无人能够理解或无权采用时，组织需要如实说明这一限制。

资本形成还需要组织承接。承接不是在表单上增加一次批准，而是使有关成果进入职责、流程、资源安排和后续任务。谁负责保存与维护，谁可以提出使用请求，发生变化时由谁检查，都应当明确。缺少承接责任的成果，可能具有潜在作用，却尚未形成稳定的组织条件。

制度认可在其中承担界定和协调作用。有权程序需要依据事实确认对象范围、使用条件和维护安排，并说明哪些方面已经成立、哪些仍待观察。这种决定可以使各方形成共同预期，但决定本身不能替代真实积累。反过来，尚未登记的实际能力，也不能仅因系统缺少记录就被认为不存在。

本书将资本形成的主要条件归纳如下。它们是本书提出的治理分析框架，不是对所有资本或会计资产的一套通用确认标准。

条件	需要回答的问题	应当保留的依据
形成来源	哪些投入与行动形成了当前积累	贡献事件、确认结果及形成过程
对象与作用	实际形成什么，支持哪些后续活动	对象说明、能力表现与适用范围
使用条件	谁能够在什么条件下持续运用	权限、协议、人员及配套资源
组织承接	谁负责使用、维护和更新	职责、资源安排及协作程序
风险安排	可用性下降或结果不及预期时怎样处理	风险范围、承担依据及处置权限
制度认可	哪些条件已确认，结论何时及如何调整	授权、规则版本、决定与复核路径

权益安排需要与这些条件衔接，但并不总是最后才出现。事前承诺可以先规定参与者在满足条件后享有什么，从而支持其投入；形成过程中的确认再判断条件是否实现。贡献、资本与权益之间存在反馈关系，不能机械理解为必须等全部资本形成后才开始讨论参与者的主张。

有些权益也不以资本形成为前提。已经满足条件的履约对价，可以有独立依据；某项工作没有留下长期能力，并不足以单独否定相应报酬。将部分贡献纳入长期资本安排，应当明确其与既有约定的关系，不能仅把已应履行的义务改写成等待未来结果的资格。

共同资本的使用也不要要求把全部所有权集中到一个主体。个人可以保有专业知识，合作方可以保有设备或方法，各方通过明确安排形成可以持续调动的条件。资本分析需要说明这种分布结构及其稳定程度，同时尊重参与者自主选择，不能把能够合作解释为组织可以占有他人的全部能力。

本书所说的资本形成，与会计上的资产确认具有不同范围。IAS 38 对无形资产的识别、确认和计量设有专门条件，包括可辨认性及有关未来经济利益和成本计量的要求。治理上认为某种能力具有长期作用，不足以单独支持将有关金额计入财务报表。IFRS 基金会：IAS 38《无形资产》〔1〕

因此，治理记录、会计处理和法律权利需要分别确定依据。某项能力未被确认为会计资产，不意味着其组织作用不存在；某项治理记录被称为资本，也不意味着它已经成为注册资本、股权或其他特定法律权益。不同制度可以使用相关证据，同时分别承担对结论的解释责任。

资本形成还可能只有部分条件得到满足。对象已经形成，使用条件尚未落实；组织已经采用，长期维护能力仍需建立。系统应当表达这些具体缺口，允许有依据的阶段性判断。把所有对象统一登记为“已资本化”，会掩盖它们实际能够支持的行动差异。

不进入资本安排，也不应成为对贡献者的整体否定。有些贡献主要服务于当期需要，有些长期作用难以辨认，有些则因组织方向改变没有得到承接。这些原因需要分别记录。参与者是否获得相应认可和回报，应当返回其贡献事实与适用安排，而不是仅由资本登记结果决定。

由此，贡献转化为资本的制度条件，既包括使积累实际可用的安排，也包括对来源、维护和后果的承认。区块链可以帮助多方共同核验其中可明确表达的状态与决定；真正的资本形成，则仍要体现为下一轮共同创造能够使用的基础。

二、持续使用、组织吸收与风险承担

持续使用说明积累并未停留在过去，而是能够进入新的行动。但持续不等于始终高频使用。备用设施、经验证的方法和必要的协作能力，可能在需要时才发挥作用。判断应当区分正在使用、具备实际调用条件、暂时闲置和已经失效，不能只凭调用次数确定全部状态。

对正在使用的对象，需要说明使用主体、用途、期间和必要效果。对备用能力，则需要检查其是否仍能在约定条件下启用，配套人员、权限和资源是否存在。未来可能有用是一种预期，已经具备调用条件则需要相应依据，两者不宜混合登记。

组织吸收进一步涉及理解、整合和接续。取得一份成果，只是获得材料；将它纳入实际流程，形成可以重复执行的工作方式，并使必要人员能够使用，才使成果更可能成为组织能力。吸收过程本身也可能包含培训、适配和协调等新的贡献，应当留下相应记录。

制度需要辨认能力存续的实际依赖。有些方法已经形成稳定流程，有些仍依赖少数人员的隐性经验；有些关系具有可接续的合作程序，有些则主要依靠个人信任维持。依赖本身并不使资本无效，但会影响维护方式、可用范围和变化后的处置。

来源追溯可以帮助表达成果怎样被使用、改造和衍生。W3C 的 PROV 数据模型提供了生成、使用和衍生等关系，同时指出使用与生成之间的联系本身不足以证明特定衍生关系成立。本书据此强调，应当检查实际整合过程，不能只因两个记录先后相连就断言已经形成新增能力。W3C：PROV 数据模型中的衍生关系〔2〕

吸收也不必意味着原贡献者可以被完全替代。复杂知识与关系可能需要持续协作才能发挥作用。组织可以通过合理授权、接续安排和长期合作维护这些条件，同时承认其依赖。将所有个人作用都要求转化为可无条件转让的组织资产，既可能失真，也可能破坏原有合作基础。

使用与吸收还会不断改变资本对象。原有方法经过适配形成新版本，独立资源与其他资源组合形成新能力，长期协作形成新的配合方式。记录应当区分原有积累、维护性工作和新增作用，避免把每次调用都算作重新形成全部资本，也避免把后续贡献全部归于最初来源。

维护需要实际资源。数据更新、知识接续、设备保养、权限续接和关系协调，都可能是保持可用性的必要工作。如果组织只记录形成时的成果，却没有人承担维护费用和行动，资本状态就可能逐渐偏离现实。维护责任应当进入预算、职责及后续贡献确认。

风险承担则说明在资本形成和使用存在不确定性时，各方处于怎样的位置。资源可能损耗，成果可能不被采用，合作可能中断，投入也可能无法产生预期作用。这些风险应当按实际承担范围说明，不能只写一句“共同承担”就认为责任已经清楚。

风险的种类和承担主体可能不同。组织可以承担设施和运营成本，参与者可能承担经约定的机会成本或延迟回报风险，合作方也可能承担特定履约责任。是否承担、承担多少、在何种条件下结束，需要有明确依据。参与共同创造本身，不应被解释为对任何损失都作出了无限承诺。

承认风险也不意味着可以把全部经营不确定性转移给较弱的一方。风险安排需要结合信息取得、决策权限和实际控制能力。如果主体无法影响有关决定，却被要求承担全部结果，其安排就需要接受进一步的制度审查。已有义务是否可以调整，仍需根据适用依据处理。

承担风险、预防风险和造成损失又是不同事项。经约定承担结果不确定性，可以是长期安排的一部分；通过适当工作降低风险，可以构成另一种贡献；因失职或越权造成损害，则需要另行判断责任。三者不能仅凭最终是否发生亏损来区分，也不应都变成同一种账户扣减。

资本对象的风险状态与权益的实现条件需要分别记录。有的回报取决于未来可分配资源，有的主张已经满足约定条件。资本使用不及预期，可以影响某些依赖未来结果的安排，却不动自动消除所有已经成立的义务。风险揭示应当帮助各方理解具体联系，而不成为概括免责的替代品。

持续使用与风险承担还可能分布在多个组织之间。一个组织使用成果，另一个组织维护关键资源，个人或伙伴承担部分接续工作。这种结构需要明确各方的权限、成本与信息责任，特别是在服务停止、关系结束或对象需要替换时，谁负责协调后续安排。

合作持续的质量也值得检查。关系长期存在，可能因为各方认可其价值，也可能因为退出困难或信息不对称。资本治理应当观察参与者能否理解条件、提出异议并在合理安排下调整合作，不能把无法退出形成的表面稳定直接计为优质关系资本。

本书据此提出，资本存续应当由使用、吸收和维护的现实联系支持，风险则由明确的制度安排承接。积累是否值得继续投入，需要结合其作用和持续成本判断；维持全部历史对象并不是资本治理的目标。及时识别失去用途的积累，同样有助于为新的共同创造释放条件。

三、贡献账户、资本记录与权益账户的分工

账户体系需要忠实表达制度对象。贡献账户回答谁作出了什么，资本记录回答形成了哪些可以延续的创造条件，权益账户回答哪些主体依据什么可以提出怎样的主张。三者可以使用同一事项的证据，但承担不同任务，不能因为在一个系统中显示就合并为同一种余额。

这里的账户，是按主体、对象和事项组织记录的逻辑结构，并不必然对应银行账户、链上钱包或财务会计科目。可以采用不同技术实现，也可以在同一系统中分别维护。是否需要共享账本，应当依据跨主体核验和治理需求判断，而不是因为存在账户就默认必须发行通证。

贡献账户应当保留主体及其参与关系、有关事件、证据联系、确认范围和评价版本。未核验、已确认、受到异议和已修订的事项，需要分别表达。账户可以按期间或类型提供汇总，但汇总应当能够返回原始事项，不能让一个总分遮蔽不同事实及其状态。

贡献账户中的数量也未必具有共同单位。工时、合格交付、知识采用和协作说明可以并存，是否折算为某种评价分数，应当依据上一章讨论的规则。账户的首要责任是保持来源和判断清楚，而不是保证所有内容都能累加成一个可兑现数字。

资本记录应当围绕对象及其持续条件建立。记录可以包括对象类型、形成来源、适用用途、使用主体、依赖关系、维护责任、风险安排、当前状态和复查期限。涉及估计数量或价值时，需要标明计量口径、日期及不确定性，不能将估计值作为对象全部含义的替代。

一个资本对象可以关联多人贡献，一项贡献也可能参与形成多个对象。这种多对多联系需要说明实际形成关系和重叠范围。共同使用同一项资源，并不意味着资源在每个使用者名下都形成了一份独立可加总的资本；多个主体共同维持的能力，也不必被强行拆成可独立处分的部分。

资本记录还需要区分对象状态与参与者关联。某个主体提供了形成来源，不等于其始终负责维护；负责日常管理，也不等于拥有对象的全部权益。通过分别记录形成、使用、管理和维护关系，系统才能解释人员变化后哪些条件继续存在。

权益账户则依据已经成立的制度安排，记录主体的具体权利或有条件资格。需要说明权益类型、对应事项、义务主体、数量或范围、成立条件、履行状态和适用限制。所有权、收益权、治理权与使用权不宜合并为同一个不可解释的权益值。

有条件的参与资格、已经成立但尚未履行的请求和已经履行的权益，也应当分别表达。一项预期安排尚未满足条件时，可以记录其依据与条件，但不宜显示成可以立即提取的余额。权益是否得到实际履行，需要相应执行和对账信息支持。

记录类别	核心对象	主要变更依据	与其他记录的联系
贡献账户	行动、证据、确认与评价	新事件、确认决定、评价版本及纠错	为资本来源和特定权益条件提供依据
资本记录	跨期可用的资源、能力与关系	形成、采用、维护、依赖变化及状态决定	关联来源贡献，并说明相关权益的对象或条件
权益账户	主体的权利、资格与履行状态	有效约定、条件实现、授权决定及实际履行	引用贡献和资本条件，保留自身成立依据

三类记录之间应当通过明确的事项和决定建立联系。贡献确认之后，可以进入资本形成审查；资本条件得到确认后，可以触发约定的权益条件检查。但这些联系不是一律等额转换，更不是把一个账户中的数字搬到另一个账户就完成制度变动。

记录更新需要指明正在发生哪一种动作。补充贡献事实、登记资本对象、确认权益成立和记录支付完成，各自应当引用相应依据。某项业务可以在条件满足时联动多个记录，但任一条件尚未完成时，应当保留处理中或待核查状态，不能让其中一处更新被误认为全部过程已结束。

跨系统处理尤其需要对账。业务系统、资本记录和权益执行系统可能在不同时间收到变化，应当能够识别相同事项、处理版本和已完成步骤。重复收到同一有效决定，不应重复新增同一资本对象或同一权益；部分处理失败后，也需要根据实际状态继续或纠正，而不是直接重做全部操作。

三类记录不是三份可以相加的价值。一次交付可以同时形成贡献记录、关联一个资本对象并支持一项权益决定，但不能据此把其作用计算为三份新增积累。对账检查的是依据、范围和处理状态能否对应，不是要求三类账户具有相同余额。

只有单位、范围和计量口径一致的数量，才适合形成相应增减汇总。能力增强、资源消耗和合作关系变化，可能具有不同尺度，不能全部写入一个总额再求净增长。涉及财务报表时，还需要按照适用会计要求建立专门联系，而不是把治理记录直接复制为会计分录。

链上钱包还需要与权益账户区分。第三章已经说明，钱包控制属于技术能力，权利是否成立及如何变动需要另外的制度和法律依据。本章把这一区分转化为账户要求：钱包可以作为操作入口，权益账户必须继续保存权利来源、条件、限制与责任主体。

账户维护权限同样需要分工。能够补录材料，不意味着可以确认贡献；能够维护资本状态，不意味着可以取消权益；能够提交链上操作，也不意味着可以自行修改分配条件。权限配置应当与实际职责相对应，重要变更需要留下决定依据和操作记录。

参与者则需要能够查阅与自身有关的贡献、资本关联及权益状态，并取得足以理解差异的说明。系统可以按权限展示不同范围，但不能只展示一个最终数字而隐藏形成依据。三类记录的分别表达，最终要使共同创造中的主体能够理解自己如何被承认，以及哪些条件仍在影响后续安排。

四、资本状态的维持、调整与终止

资本形成不是一次确认之后永久不变的事实。资源会消耗，方法会更新，合作条件会变化，已经形成的能力也可能失去用途。治理需要持续检查资本对象目前能否发挥作用，并根据有依据的变化调整状态。历史上曾经形成，与当前仍然可用，需要分别回答。

状态维护应当从复查条件开始。不同对象可以采用不同的检查周期和触发事件：使用权限到期、维护中断、关键依赖变化或出现实质性质量问题，都可能要求重新检查。复查频率应当与实际变化和影响相称，避免只为保持登记活跃而进行没有内容的确认。

状态表达也不宜由一个“有效”或“无效”覆盖全部情况。对象可能存在但暂不可用，部分用途受到限制，长期作用仍待观察，或者正在办理接续安排。事实状态、使用状态和制度处理状态可以分别维护，再向有关主体提供清楚的综合说明。

维持资本状态需要持续行动及资源，而不只是延长记录期限。维护人是否履行工作，必要资料是否更新，接续人员是否具备能力，以及依赖关系是否仍然成立，都可能影响判断。负责维护的人更替时，应当保留职责交接和必要材料，使对象的连续性不完全依赖原操作人员。

资本增强也需要得到适当识别。新增资源、知识改进和关系扩展可能提高原有对象的作用范围，但应当区分维护原有能力与形成新增能力。若新增贡献改变了有关条件，可以建立新的版本或关联记录，说明哪些来源继续发挥作用，哪些后续工作提供了新增基础。

资本下降则可能来自不同原因。资源耗用、技术过时、需求变化、关系中断和维护不足，都可能使作用减弱。调整记录应当说明观察到了什么，以及哪些结论来自估计。价值估计下降不一定意味着对象已经不能使用，对象暂时闲置也不一定意味着其全部未来作用消失。

估计变化、事实纠正与责任认定需要分别处理。根据新资料调整当前判断，不意味着原确认者当时必然失职；发现原始材料虚假，则需要追溯受影响事项；损失由谁承担，还要结合职责和适用安排。系统不应把所有下降都转成对原贡献者的扣减。

资本对象的拆分、合并和替代同样需要保留联系。多个对象组合成新的能力时，应当检查原对象是否继续独立发挥作用；旧对象被新版本替代时，则需要明确当前采用哪个版本。新旧记录同时保留可以支持追溯，但在汇总时应当避免对同一作用重复计算。

部分条件失效时，可以按授权程序限制有关使用或启动复核，但应当说明范围、原因及恢复条件。原资本记录与其关联权益也不必同步冻结。为了核实某项使用能力而暂停全部无关权益，可能超出必要范围；具体处理仍需回到相应制度依据。

终止资本状态，需要明确终止的对象及含义。可能是资源已经耗尽，许可或合作条件结束，对象被替代，或者组织依程序决定不再将其纳入后续创造。终止说明当前安排发生变化，不意味着相关贡献从未发生，也不意味着过去的使用结果应当全部取消。

参与者退出与资本对象终止也可能不同步。某个人停止参与后，已经形成且具备接续条件的方法可能继续使用；某项能力若依赖持续合作，则需要重新检查可用范围。权益是否继续、如何结算或是否需要后续协作，应当依据原有安排处理，不能只由账户停用决定。

终止程序应当检查尚未履行的义务。是否存在已经成立的请求、尚待结算的费用、必要的交接或资料保管责任，都需要说明。资本对象不再产生作用，并不会自动提供清偿这些义务的资源，也不会因删除记录就使义务自然消失。

对于涉及多个组织或主体的安排，终止还需要协调通知和状态同步。谁应当获知变化，谁停止采用原状态，哪些系统需要保留历史，哪些主体负责后续处理，应当有明确责任。一个系统显示“已关闭”，不等于全部相关安排已经结束。

技术上的撤销、停用或销毁，应当准确对应其操作对象。可以撤销某个操作权限，标记某份凭证不再用于当前用途，或按授权终止某个合约功能，但这些动作的制度效果需要有相应依据。不能把凭证销毁直接表述为所有权、收益请求和历史责任都已一并消灭。

状态决定仍应当允许有依据的异议和修订。参与者可以提出用途仍然存在、维护责任已被履行或终止依据有误等材料。程序应当保留适当复核路径，同时使已经明确结束的事项不被无理地无限悬置。稳定性来自清楚的处理条件，而不是拒绝一切后续证据。

面向未来，本书提出一个需要检验的方向：使资本记录持续连接来源贡献、当前可用条件与未来维护安排，并将状态变化及时传递给相关责任人和权益程序。这种结构有望使资本治理从积累历史数量，推进到维护可持续创造的条件。但若系统只奖励登记规模、增加维护负担，或让状态管理者掌握不受约束的权益取消权，就需要调整其设计。

资本形成条件与账户体系由此构成共同创造进入长期安排的基础。贡献账户保存来源与承认，资本记录说明积累及其存续条件，权益账户组织具体主张和义务。三者保持联系，也各自保留判断边界，才能使状态变化得到准确解释。

下一章将进一步讨论这些权益怎样被分别表达，哪些适合账户记录、数字凭证或通证，以及凭证转移如何与实际权利变动衔接。资本可以为权益安排提供对象和条件，权益能否成立、由谁履行以及如何变化，仍需要明确的制度依据。

定稿补强：资本形成决定与会计确认分开

资本形成决定是治理程序：它判断一项贡献是否被组织吸收、能否持续发挥作用、需要何种维护以及由谁承担风险。会计确认是另一套程序，需要依适用财务报告框架判断资产、负债、权益、收入或费用的定义、确认、计量与列报。前一程序成立，不表示后一程序已经完成。

因此，资本形成决定书应设置“会计处理另行评估”栏，记录适用准则、会计主体、判断责任人、是否确认、金额或费用化处理、后续计量与披露。内部生成的知识、关系与能力可以在治理上被持续维护，但若不能辨认、控制或可靠计量，可以只进入治理记录而不进入资产负债表。

三账体系也应保持接口而非合并：贡献账户保存事实与证据，资本记录保存组织判断与维持条件，权益账户保存具体权利义务。会计总账依自己的控制和关账程序接收必要结果。任何跨账转换都要有唯一事件标识、批准依据和可逆转的差异处理。

本章工具与图表

本章的制度关系可结合[附录五](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

图17-1 贡献账户、资本记录与权益账户

事实、资本状态与权利请求分别记录，避免一套积分包办全部关系



《区块链——利益相关者资本论的底层技术》V1.0 · 可编辑SVG

图17-1 贡献账户、资本记录与权益账户

图17-1 贡献账户、资本记录与权益账户。事实、资本状态与权利请求分别记录，避免一套积分包办全部关系

本章注释

- [SRC-052] 国际财务报告准则基金会（IFRS Foundation）：IFRS 基金会：IAS 38《无形资产》。[原文或官方页面](#)
 - 本章引证：IFRS 基金会：IAS 38《无形资产》。
 - 支持范围：用于确认财务、审计、内部控制或公司治理中的规范口径，本书引用主题包括：IFRS基金会：IAS 38《无形资产》、IFRS 基金会：IAS 38《无形资产》。
 - 使用边界：规范口径需要结合适用主体、报告目的和具体交易事实，不宜机械移用于链上权益。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-075] 万维网联盟（W3C）：PROV Data Model。[原文或官方页面](#)
 - 本章引证：W3C：PROV 数据模型中的衍生关系。
 - 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：W3C：PROV 数据模型、W3C：PROV 数据模型中的衍生关系。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第十八章 权益结构、数字凭证与权利转移

资本形成使共同创造留下能够延续的资源、能力与关系，权益安排则进一步说明参与者如何在其中获得承认、提出请求和参与决定。二者具有联系，却不能相互代替。共同事业拥有某种能力，不等于所有贡献者已经取得相同权利；某个主体持有数字凭证，也不意味着其能够要求组织履行凭证名称所暗示的一切。

上一章建立了贡献账户、资本记录与权益账户的分工。本章进一步讨论权益账户究竟表达什么，以及这种表达如何进入数字凭证和转移程序。核心问题是把权利内容、主体、义务和条件说清楚，再选择能够准确承载这些内容的技术形式。

本书将权益结构理解为不同权利、资格和限制之间的制度安排。数字技术可以使其中一部分更容易识别、核验和执行，但必须说明技术状态与制度效果怎样对应。账户变化、凭证交付、通证控制转移和法律上的权利变动，可能相互关联，也可能分别发生。

一、所有权、收益权、治理权与使用权的区分

“拥有权益”只有在对象和内容明确时才具有可检查的含义。拥有某项财产、可以请求某类回报、可以参与某项决定，以及可以在一定条件下使用资源，回答的是不同问题。本书以所有权、收益权、治理权和使用权展开分析，同时承认具体制度中的权利可能交叉组合，并不将四者当作穷尽全部法律关系的分类。

所有权首先需要明确指向的对象。对某项资源的所有权、持有某种企业股权和参与一项共同资本安排，不是同一对象上的同一种关系。制度文本本若只写“共享所有权”，却没有说明共享什么、由谁确认及受到哪些限制，就难以支持后续操作。

所有权的具体内容和变动条件需要依据有关对象及适用法律判断。数字记录可以描述权利归属，也可以记录有关处分行为，但一个系统中的“所有者”字段首先具有该系统定义的含义。它是否对应某种法律权利，还要检查记录的效力依据与现实对象的联系。

收益权在本书中用于概括按照特定安排取得经济回报的权利，需要进一步说明其性质。请求约定报酬、参与符合条件的收益分配以及取得某种剩余回报，可能具有不同来源和实现条件。不能把它们都写成一个没有期限、口径和责任主体的“分红权”。

收益安排尤其需要区分已成立的请求与依赖未来条件的资格。完成约定事项后产生的支付请求，和只有在形成可分配资源后才参与计算的资格，承担的不确定性不同。制度应当直接说明差别，而不能先展示成同一种余额，再在履行时才解释其实际限制。

治理权涉及参与组织决定的权限和程序，可以包括知情、提案、审议、表决、监督及请求复核等不同内容。取得其中一种，不意味着同时取得所有内容；有权投票，也不意味着可以越过既定范围直接操作全部资源。治理权的对象和程序，比一个笼统的票数更重要。

治理权还应当与技术管理权限区分。维护系统、升级程序或持有管理密钥，是实现某些操作的能力；这些能力是否得到制度授权，以及应当依据谁的决定使用，是另一项判断。节点参与账本确认的资格，也不能直接作为参与企业全部治理的依据。

使用权则说明主体可以在什么范围、期限和条件下利用资源或服务。它可能涉及排他使用、共同使用、特定用途或一定额度，具体性质需要结合安排判断。获得读取权限不等于可以任意复制和传播，获准使用成果也不等于取得其全部所有权。

使用的实际条件同样需要表达。系统允许登录，只说明入口开放；资源容量、维护状态和必要配套是否满足要求，决定了使用是否能够实现。对服务或组织能力的使用，尤其不能仅以一个访问凭证已经签发作为履行完成的证明。

权益类型	需要明确的核心内容	不宜自动推导的其他权利
所有权	对象、归属、处分条件及适用限制	对组织全部事务的直接决定权
收益权	回报来源、计算口径、请求条件及履行方式	所有权或全部治理权
治理权	决策事项、参与程序、权限范围及约束	对资产的任意处分或个人收益保证
使用权	使用对象、用途、期限、额度及配套条件	所有权、再许可权或无限期占用

权益可以按照共同创造的需要组合。一个主体可以取得限定使用和特定收益安排，另一个主体可以承担维护职责并具有相应治理参与权限。但组合应当有清楚依据，不能因为某项凭证承载多种功能，就默认这些功能在成立、变更和退出时永远同步。

不同权益的转让性也可能不同。某项经济请求在满足条件时可以转移，与任职或持续履行相关的治理资格则可能要求另行审查。制度需要逐项说明哪些可以转让、哪些只能委托行使、哪些必须随关系变化重新确认，不能给整组权益设置一个没有区分的转移开关。

共同创造的历史归属还应当独立保留。某项收益安排可以按规则转让，不意味着原有贡献事实改由受让人完成；受让人取得某种凭证，也不因此继承原贡献者的专业能力或合作关系。贡献、资本来源与权益持有，需要通过不同记录保持联系。

权益之间也可能出现冲突。使用范围扩大可能影响其他使用者，某类收益安排可能影响共同维护资源，治理决定也可能改变后续参与条件。清晰分类有助于识别受到影响的主体，并确定应当采用的审议和授权程序，而不是让一种权益名称覆盖所有后果。

因此，区分四类权益并非把共同关系切碎，而是为组合提供准确基础。每项权利能够单独说明其对象、依据和限制，组织才有条件安排它与其他权利的联系，并在某项条件变化时避免不必要地改变全部关系。

二、权利主体、义务主体与兑现条件

权利结构需要落实到具体主体。谁可以主张，向谁主张，要求完成什么，以及在什么条件下履行，决定了权益能否进入实际协作。“由生态保障”“系统自动兑现”之类表述，如果没有进一步的职责安排，就不足以说明由谁承担后续行动。

权利主体应当与账户控制者、凭证持有者和实际受益者分别识别。自然人可以通过代理人操作，组织可以由工作人员提交请求，托管服务也可能代为控制数字工具。系统需要记录谁以什么身份行使哪项权利，避免把经办行为误写成权利归属。

义务结构则应当结合权利类型分析。支付或提供服务的请求需要明确相应履行者；治理参与需要明确谁组织程序、提供信息并落实有效决定。所有权等财产性权利还涉及与其他主体的关系，不能一律简化为“某个发行者欠持有人一笔钱”。本书强调的履行责任，是使实际行动安排清楚，并不把全部权利改写为单一债务关系。

数字凭证的出具者也未必就是全部义务的承担者。出具者可以证明某项资格或记录某个决定，资源提供者、支付者和程序组织者则可能另有其人。制度应当说明各自职责，不能仅凭凭证上存在一个签名，就推定签署者承诺履行所有关联事项。

权益成立需要有明确依据。组织规则、双方约定、有权决定或其他适用制度，可以分别产生不同效果。记录应当能够指向具体版本、适用范围和必要的接受或生效程序。一个网页上公开的计划，与已经对特定主体成立的安排，需要保留区别。

条件也需要拆分为资格条件、履行条件与操作要求。参与者是否符合约定身份，贡献或其他事项是否已经满足要求，当前请求是否由有权主体提出，分别影响不同环节。操作材料暂时不齐，不应直接显示为权利不存在；身份尚未核实，也不能被系统自动补成已经有效。

对于有条件权益，应当说明条件由什么事实触发、谁负责确认以及如何处理争议。条件若完全依赖承担义务的一方任意决定，而没有范围、期限和复核安排，权利主体就难以形成稳定预期。技术可以执行条件检查，条件本身仍需受到制度约束。

本章所说的兑现，不仅指支付金钱。收益请求需要实际履行，使用权需要获得相应资源或服务，治理权需要有真实可参与的程序，其他权利也需要具备适当行使条件。凭证已经到达钱包，通常只能证明凭证取得这一环节，不能统一表示上述事项已经实现。

涉及回报时，需要说明资源来源、计算期间、采用口径和支付责任。可分配资源尚未形成的安排，应当如实呈现其条件；已经成立的支付义务，则不能仅因系统没有预先存放资产而被重新解释为不存在。权利成立、资金准备和实际支付，是不同状态。

资源准备能够改善履行条件，但其效果也需要具体说明。合约中存放了可用资产，可以支持某些自动支付；仍需检查哪些主体有权操作、资产是否实际用于相应义务，以及是否存在其他限制。屏幕显示的额度，不足以单独证明资源已被适当配置给特定权利。

履行期限与请求程序应当相互配合。何时可以提出请求，收到请求后何时处理，哪些补充材料确有必要，以及未按期履行时怎样回应，都应当清楚。不能通过不断增加事后要求，使已经满足条件的主体长期停留在等待状态。

分阶段履行还需要区分已完成与剩余部分。部分支付、部分开放使用或一次治理程序完成，可以分别形成记录，但不当然终结全部义务。相关回执应当限定其范围，并与原请求对应，避免同一操作被重复计为履行，也避免部分履行被展示为全部兑现。

履行依赖其他主体时，需要识别关键连接。组织可能依赖支付服务、资源托管或外部业务确认来完成安排，各环节应当说明职责和失败后的处理。技术提供者发生故障，并不会自动回答原义务由谁承担；需要依据既有安排判断后续替代和处理责任。

当资源不足、系统中断或现实条件变化时，程序应当表达发生了什么、影响哪些请求以及准备怎样处理。它可以依据有效安排启动延期、替代履行或其他程序，但不宜通过删除记录掩盖未履行状态。争议、不能即时履行与权利已经终止，需要分别呈现。

多方共同承担的事项尤其需要避免责任空白。应当说明各方分别完成什么，何时需要协调，哪一环节负责向权利主体反馈。共同协作并不天然意味着每一方都承担全部义务，也不应成为每一方都可以推给他人的理由。

本书据此主张，把权益描述写成可以检查的关系：主体清楚，内容明确，条件有据，履行有责，结果可查。这样的结构既可以支持技术执行，也能在技术无法覆盖的环节保持责任连续，为数字凭证提供真实的制度内容。

三、账户记录、数字凭证与通证的选择

权益内容清楚之后，才有条件选择表达形式。账户记录便于持续维护主体与权益状态，数字凭证便于携带和出示特定声明，通证则可以按照协议组织持有、授权和流转。三者并非完全互斥，一套制度可以同时使用，但需要说明每种形式承担哪项功能。

账户记录适合持续管理多项具有不同条件的安排。它可以分别显示资格、成立状态、履行进展和争议事项，并根据有权决定更新。记录由谁维护、依据什么更新以及参与者怎样核查，决定了账户能否发挥作用。集中维护和共同维护可以采用不同保障方式，并不因名称不同就自动决定质量。

账户也可以作为多种凭证背后的状态依据。对外出具凭证时，组织可以只披露特定事项，而保留较完整的内部记录。需要明确凭证反映哪个时间点、哪个范围，以及后续变化怎样被采用者发现。旧凭证内容曾经正确，不等于其目前仍适用于同一请求。

数字凭证首先是一种可出示的表达。它可以声明某个主体满足资格、某项权益已经确认或某次履行已经发生。采用者需要核实出具者、内容、状态及本次使用条件，而不是只看文件是否具有电子签名或区块链标记。

第十三章已经区分凭证的出具者、持有者、所描述主体和验证者，并说明密码学验证不自动证明声明事实。用于权益表达时，还要增加本章的专门检查：该凭证是否对应一项已经成立的权利，采用者是否有义务据此履行，以及当前状态是否仍然有效。

通常的文件型凭证可以被复制。若凭证用于证明身份或历史事实，复制可以方便核验，而不增加新的资格。若制度需要限制同一项权益只能使用一次，则还需要核对当前状态、已使用记录或其他有效机制，不能靠文件只能由一人保留这一不成立的假设来保障。

通证的不同之处，在于系统可以按协议维护可核验的持有或余额状态，并约束相应操作。它可以支持某些权益的流转，也可以承载受到转移限制的资格。但通证采用什么技术标准，并不直接确定它属于所有权、收益请求还是其他安排。

ERC-721 提供了查询通证所属地址、授权操作和转移等接口。它规范的是这类通证在合约中的基本交互方式。本书据此区分接口能力与制度内容：标准能够支持记录和执行某些转移，但不会自行规定所关联现实对象的全部权利。Ethereum：ERC-721 非同质化通证标准〔1〕

通证是否具有相同单位，也需要与权益内容一致。若不同持有者的有效期间、资格或限制不同，就不能只因数量相同便假定每个单位具有相同含义。相反，对确实相同的安排，采用数量记录可能更便于管理。选择单位形式应当根据权利内容，而不是为了方便交易而提前简化。

表达形式	主要适用需求	需要补充的制度与技术条件
账户记录	持续维护主体、权益及履行状态	维护权限、变更依据、查询与纠错程序
数字凭证	向特定采用者出示可核验声明	出具资格、主体绑定、证明范围与状态检查
通证	按协议维护单位、控制及流转状态	权益解释、转移限制、现实衔接与异常处理

选择还应当考虑是否真的需要持有人之间流转。若资格依赖持续任职或专业职责，方便出示和验证可能比公开转让更重要。若制度需要转移特定请求，则可以围绕转移对象和条件配置机制。可转让性是一项需要论证的制度能力，不是数字化之后必须增加的属性。

本书建议同时区分凭证的三种可能作用：证明已有关系，帮助行使某项权利，以及依照适用制度参与权利的设立或变动。第三种作用尤其需要明确效力依据。系统不能自行宣布任何记录都具有设权效果，也不应在制度确已赋予相应功能时把它仅当作普通截图。

账户与凭证并用时，需要说明哪个记录承担哪类当前状态判断，以及发生冲突后怎样处理。签名凭证、链上状态和外部登记可能各自表达不同层次，不能仅以技术更新时间较晚为由覆盖其他有效依据。预先确定核查与纠错程序，有助于避免并存记录形成相互矛盾的主张。

隐私和可取得性也影响形式选择。完整的参与关系和权益条件不必全部公开，凭证可以按用途披露必要内容；有权主体又必须能够取得足够依据核查自己的安排。选择性披露、受控访问和链下保存可以组合使用，公开可见不应成为可核验的唯一方式。

长期维护需要考虑补发、密钥恢复、出具者变化和系统迁移。重新签发一份凭证，可能只是恢复出示能力，也可能伴随新的有效条件，需要分别表达。恢复程序应当识别原主体并处理旧凭证状态，避免把技术恢复误写成新权益发行。

表达形式还会带来成本和权力结构。谁提供钱包，谁控制状态查询，谁能够撤销凭证或升级合约，都会影响参与者是否可以实际行使权利。技术可替换性、资料迁移和必要的替代核验路径，应当与权益本身的持续性一起设计。

因此，选择账户、凭证或通证，应当以权益结构的准确表达和实际履行为标准。形式越能让主体理解条件、核实当前状态并在需要时完成适当行动，就越有制度意义。发行数量、公开流通或技术复杂程度，都不能替代这种判断。

四、凭证转移与权利变动的对应条件

凭证转移需要先说明转移了什么。发送凭证文件可以只是提供副本；更换保管者可以只改变技术控制；按照协议改变通证持有状态，可以完成一定范围的链上转移。只有在相应制度将这些动作与特定权利变化建立联系时，才能进一步判断原主体与新主体的权利如何变化。

第三章已经建立技术控制、制度认可和法律权利的分层。本章沿用该模型判断凭证转移：链上持有状态改变只完成技术层事实，只有满足相应制度与适用法律的条件时，才可能对应特定权利的变动。

第三章也已经说明，特定电子可转让记录可以在适当立法与实体法条件下承担纸质单证的相应功能。这里不能把该结论扩展为所有通证都具有同样效力；需要回到具体对象、适用范围、可靠性条件和相应法域逐项判断。

要建立可靠对应，首先应当明确被转移的权利对象。是某项财产的权利、一段期间的收益请求、一定范围的使用资格，还是其他安排，决定了需要核查的条件。若凭证承载多种权益，转移程序需要说明哪些随之变化，哪些仍由原主体保留或需要另行确认。

转出方是否具有相应权利及处分资格，也需要检查。技术上能够签署转移，不足以单独证明其有权处分关联的全部权益。代理、托管、共同控制或受到限制的持有，应当保留适当授权条件；技术凭证被盗用时，后续权利效果则需要依据事实和适用制度判断。

转入方的条件同样可能重要。某些权益可以面向符合一般条件的主体转移，某些则依赖成员资格、使用能力或其他关系。程序应当在适当阶段检查这些条件，并说明不满足时如何处理。收到通证不应成为绕过原本有效资格要求的隐蔽途径。

各方的意思和转移范围需要明确。交付给代理人保管，与出售相应权利，不是同一种安排；委托他人投票，与转让治理资格，也需要区分。若承接涉及义务、持续职责或其他主体的利益，还须按具体制度处理必要的同意和程序，不能仅靠改变接收地址统一完成。

现实衔接条件可能包括登记、通知、交接或其他手续，其必要性取决于权利和适用制度。系统应当记录哪些条件已经完成，哪些仍未完成，并据此表达当前状态。不能把链上交易确认作为所有外部步骤均已满足的默认回执。

时间边界也需要说明。转移前已经形成的请求归谁，转移后的使用或分配由谁参与，某次治理决定按哪个时点判断资格，都可能影响双方利益。记录应当保留约定期间和适用时点，避免原持有人与新持有人重复请求，也避免一段有效主张因切换账户而被遗漏。

在对应关系明确后，技术可以把条件落实为可检查的流程。可以登记转移请求，核验主体和资格，取得必要授权及外部确认，再依规定更新权益与控制状态，并向履行者发出所需信息。这些步骤是否可以合并执行，需要结合系统能力和现实条件判断。

涉及同一执行环境内、能够同时完成的状态变化时，程序可以按相应机制实现协调更新。涉及链下登记、实际交付或外部支付时，各环节可能在不同时间完成。此时需要保留待完成、已完成和失败等状态，并明确超时、撤回或补救条件，不能假设一笔链上交易能够自动保证外部行动同步发生。

转移的排他性也需要限定范围。共同账本可以在协议条件下拒绝某些重复支出，但同一现实权益若多个互不协调的系统中被重复表达，单个账本未必能够发现全部冲突。需要明确权威依据、跨系统核对及重复主张处理，而不是仅依赖每个凭证都有不同编号。

原凭证的后续状态应当与转移效果对应。转移完成后，旧副本可能仍然存在，验证者需要按规则检查它是否仍可用于请求。对不可重复行使的权益，应当防止旧凭证继续触发履行；对历史证明，则可以保留其原有证明意义。停止当前行使能力，不要求将历史事实一并抹去。

链上最终性与制度上的争议终结也不是同一回事。协议可能已不再按通常机制回退交易，但有关授权、欺诈、错误登记或外部条件的争议仍可能存在。处理可以涉及新的状态记录、权限限制或其他制度程序，具体效果需要依据适用安排；不能承诺任意回滚，也不能以技术难以回滚否认必要救济。

对转移结果的核验应当同时检查技术与制度两个层面。技术层面关注操作、确认及当前控制状态；制度层面关注主体、对象、条件和外部程序是否对应。只有各层已经满足其要求，才能在相应范围内报告权利变动完成，并说明是否仍有未履行事项。

面向未来，本书提出一个需要检验的方向：使一项数字权益的表达能够同时呈现权利内容、当前主体、义务安排、适用条件和变动依据，并在每次转移时保留这些联系。其目标是让可流转的凭证携带可以理解和核查的制度语义，而不是仅在地址之间移动一个标记。

这一方向需要稳定的解释规则、现实履行条件和可处理分歧的程序。如果技术互通却导致不同组织对同一凭证赋予冲突含义，或者转移便利性使责任关系逐渐无法追溯，就应当限制自动化范围并修订衔接条件。能够转移多少次，不应取代对每次转移是否适当的判断。

权益结构由此为数字凭证提供内容，为权利转移提供条件。所有权、收益权、治理权和使用权可以被分别表达，也可以依制度组成相互联系的安排。区块链的重要作用，是帮助参与者共同检查其中的控制与状态变化；这些变化如何进入实际权利关系，仍由明确的制度与法律依据衔接。

下一章将进一步讨论通证机制与流转规则，研究哪些需求适合通证表达，以及发行、归属、锁定、撤销等操作怎样对应具体安排。只有先把权益说明白，通证才可能成为共同创造的有效工具。

定稿补强：权利束的法律与财务分类

权利束能够帮助制度设计者分别配置收益、治理、使用和退出，但“权益”这一名称不决定法律或会计分类。具有现金偿付、赎回、到期、保证收益、持续服务或其他结算条件的安排，可能在不同规则下形成合同义务、负债、员工报酬、会员资格或其他关系。发行人和持有人需要分别分析。

在采用账户、数字凭证或通证表达之前，应完成两份备忘录。法律分类备忘录按持有人权利、发行目的、可转让性、收益预期、发行人与二级市场流转审查可能适用的证券、支付、储值、集体投资、消费者或其他制度；财务分类备忘录记录现金义务、结算选择、到期、条件、服务期和终止。分类取决于经济实质、法域和事实，不能由技术名称预先决定。

本章工具与图表

本章的制度关系可结合[附录五](#)、[附录十二](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。



图18-1 所有权、收益权、治理权与使用权的权利束

图18-1 所有权、收益权、治理权与使用权的权利束。权利可组合、分离、附条件或不可转让；凭证只是表达与控制工具

本章注释

1. [\[SRC-027\] Wiserunion Improvement Proposals: ERC-721 非同质化通证标准. 原文或官方页面](#)

- 本章引证：Ethereum：ERC-721 非同质化通证标准。
- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：ERC-721通证标准、Ethereum：ERC-721 非同质化通证标准。
- 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第十九章 通证机制与流转规则

通证可以把部分制度安排表达为共同可核验的单位和状态，并让取得、持有、使用与转移按照明确规则发生。它因此可能成为利益相关者资本治理的一种工具。但通证的作用取决于它究竟承载什么、由谁履行相应义务，以及流转怎样影响原有关系，不能仅凭发行了一种数字单位就判断共同创造已经获得了新的资本基础。

上一章区分了权益结构、表达形式与权利转移。本章进一步讨论，当组织决定采用通证时，怎样把制度内容落实为单位属性和生命周期规则。通证机制需要回答的不只是如何分发，还包括哪些条件允许取得、哪些操作受到限制、状态怎样改变，以及这些安排怎样影响参与者的行动。

本书将贡献激励、交易价格和企业价值分别讨论。通证可以影响激励，也可能产生市场价格，但它们与真实贡献、组织能力和可分配资源之间都需要具体机制连接。通证设计的质量，应当由它是否改善这些联系来检验。

一、何种制度需求适合通证表达

通证表达首先适用于某些能够清楚界定为单位、需要共同维护状态并按照规则行使的安排。单位可以描述一定范围的使用额度、某项制度下的参与资格或特定权益的份额。采用之前，需要说明每个单位意味着什么，适用哪个范围，以及哪些主体承认并履行相应安排。

单位化并不是单纯选择一个名称和小数位数。若不同单位在期限、义务、使用限制或权益内容上有实质差异，就需要保留这些差异。只有当制度允许在有关用途下按相同单位处理时，数量汇总才具有清楚含义。数学上可以相加，不足以证明制度内容可以合并。

需要防止同一额度被重复使用，是通证可能发挥作用的一个方向。在参与者遵守同一协议和安全条件的范围内，共同状态可以记录额度由谁控制、是否已经使用，以及哪些请求应当被拒绝。若所对应的资源和权限仍由外部系统管理，还需要把链上状态与实际服务衔接。

多方需要识别同一种单位，也是采用通证的可能理由。标准接口可以减少不同工具理解余额、授权和转移方式时的技术差异。ERC-20 规定了余额、总量、转移和授权额度等基本接口，支持相关通证与应用交互；它并不规定这些单位必然代表哪一种经济或法律权益。Ethereum：ERC-20 通证标准〔1〕

需要在符合条件的主体之间流转时，通证还可以帮助记录原控制状态的变化和新控制状态的成立。这种能力能够服务于某些资源调配和权益安排，但转移对象、转入资格及外部履行条件仍需明确。接口通用，只说明操作可以被技术理解，不说明所有组织对其权利内容具有相同认识。

通证也可以用于受到严格限制的参与安排。制度可能只需要验证资格或记录使用，而不需要公开交易。是否开放转让、允许何种用途以及由谁维护资格，应当按实际需求决定。采用通证并不要求同时建立一个面向所有人的市场。

对于主要依赖身份、专业职责或细致例外判断的安排，普通账户和数字凭证可能已经足够。若制度并不需要单位之间流转，也没有多方共同维护状态的必要，增加通证可能只是增加密钥、交易费用和恢复成本。技术选择应当比较它实际解决的问题和新增负担。

本书建议在采用之前回答三个相互联系的问题：没有通证时，哪项协作困难难以处理；通证的具体机制怎样改善这一困难；这种改善需要哪些现实资源、制度责任和持续维护。回答应当能够被实际效果检验，而不是停留在“增强共识”或“激活生态”等笼统目标上。

制度需求	通证可能提供的能力	必须另外落实的条件
共同维护额度或份额	核验余额、使用及重复支出状态	单位含义、适用范围与真实资源联系
多方识别同类安排	以约定接口查询、授权和处理	语义一致、参与资格与履行责任
允许适当流转	维护控制变化并执行部分限制	可转移的权利、转入条件与外部程序
限定资格或用途	按身份或状态检查允许的操作	资格来源、恢复、撤销与隐私安排

通证还需要明确表达的层次。贡献记录说明发生过什么，资本记录说明形成了哪些可持续条件，权益通证则只能在适当依据下表达相应权益。若将三者混成一种单位，就可能让购买者看起来取得他人历史贡献，或者让未经确认的贡献自动变成可转让权益。

不同层次可以通过规则联系，但转换本身需要有条件。贡献确认可以使参与者进入某种激励安排，满足进一步条件后取得相应通证；通证被使用或兑现，又可以产生新的业务记录。每一步都需要说明依据，不能只以通证余额变化代替全部制度过程。

组织还应当确认通证承诺可以被持续支持。若单位对应服务，需要有服务能力；若单位关联经济请求，需要有明确履行安排；若用于治理，需要有实际决策程序。技术上能够无限创建数字单位，不意味着组织能够无限扩大相应能力或义务。

规则制定者和技术管理者的权限也应当进入设计。谁可以增加发行、改变使用条件、限制地址或替换执行逻辑，都会影响持有者的预期。公开说明这些权限，并使重要变更受到相应程序约束，是通证表达制度内容的一部分。

因此，通证适合承载的是能够被明确说明、共同核验并实际履行的部分制度关系。它的优势应当落在具体协作环节上。若真实困难来自目标不清、贡献无法确认或义务无人承担，增加一种可流转单位并不会自行解决这些问题。

二、可替代性、可转让性与身份绑定

可替代性、可转让性与身份绑定是三个不同维度。可替代性回答同类单位在有关用途下能否相互替换；可转让性回答单位或关联权益是否可以由一个主体移向另一个主体；身份绑定则说明有效持有或行使是否依赖特定主体及其资格。三者可以形成不同组合。

可替代性需要以实际权利内容为依据。数量相同、有效期相同且使用条件一致的单位，可以在相应范围内按同类处理；若发行批次、请求顺序、资格或限制不同，就需要检查这些差异是否影响替代。相同符号或同一合约地址不能自动抹去制度上的不同条件。

非同质化的标识则帮助区分特定对象，但唯一编号本身不保证现实对象唯一，也不保证其他系统没有发行与其重复关联的凭证。编号解决识别，实际对应关系仍需核验。不能把技术上的可区分性直接当作全部权利的排他性证明。

可替代性也不等于开放流通。同类额度可以仅供合格成员持有，彼此具有相同用途，却受到转让限制；某个独特对象的凭证则可能按规定允许转让。将“同质化”直接等同于自由买卖，会跳过参与资格和权利性质的判断。

可转让性需要明确对象、范围和条件。是转让全部单位，还是允许部分额度转移；是所有合格主体之间可以流转，还是必须经过一定审核；是否受期限、事项或总量限制，都需要在规则中说明。技术执行应当与这些条件对应，不能只保留一个不加区分的转移按钮。

身份绑定可以服务于成员资格、专业权限或不可转移的历史承认。有效行使可能依赖自然人、组织或特定关系，系统需要核实这种联系，而不是仅把某个地址永久列入名单。地址控制者可以变化，主体也可能需要更换操作工具，二者不能预设为永远一致。

ERC-5192 为与账户绑定的非同质化通证提供了最小接口：在锁定状态下，相应合约中的通证转移功能应当拒绝执行。这说明协议可以表达一种转移限制，但账户锁定本身不构成自然人身份核验或唯一性证明。Ethereum：ERC-5192 最小账户绑定通证接口〔2〕

技术上的不可转让也不宜被解释为任何经济控制都绝不可能变化。托管关系、账户控制或代理安排仍可能影响谁实际作出操作。制度如果关注的是特定主体持续参与，需要核验主体和关系状态，并检查允许的代理范围，不能只依赖单一转移函数是否开放。

身份绑定还必须容纳恢复。丢失密钥、更换设备或调整组织经办人，可能需要迁移操作能力，而不是把原权益永远锁在无法使用的地址上。恢复程序应当确认原主体、限制旧操作手段并保留关联记录，使技术接续不会造成新增资格或不当转让。

关系终止与历史记录的意义也要区分。任职资格结束后，可以停止与该角色相关的新增操作；曾经完成的贡献仍然可以作为历史事实保存。将资格凭证撤销，不应自动表示贡献从未发生，也不宜把历史承认设计成持有者永久公开全部关系的负担。

隐私保护需要说明哪些身份联系必须向谁证明。系统可以在限定事项中核验资格，并只提供必要信息；防止重复取得某项资格，也不必默认公开全部账户关系。身份绑定的目标是使适当主体行使适当权限，而不是扩大无关观察。

同一主体拥有多种通证时，各种绑定和流转条件需要分别维护。可以转让的经济权益，不应因同时持有不可转让资格就被混成一项整体；资格终止，也不应无依据地带动所有其他权益消失。不同状态之间的联动必须来自明确规则。

治理资格尤其需要考虑转让带来的权力变化。若表决权直接随可交易单位移动，制度就选择了一种以该单位持有状态配置权力的方式。它能否代表不同利益相关者，需要另行论证；有足够资源取得通证，不等于已经具有相同的贡献、责任或代表关系。

本书据此主张，先逐项确定单位是否可替代、是否允许转移以及是否依赖身份，再选择相应的技术形式。对这些维度的分别设计，能够同时容纳资源流动、身份连续和稳定承诺，也有助于在条件变化时只调整必要的部分。

三、发行、归属、锁定、撤销与销毁

通证生命周期需要同时表达技术操作与制度决定。发行涉及单位如何产生并进入安排，归属涉及参与者何时满足取得或保留有关权益的条件，锁定限制特定操作，撤销改变某项资格或有效状态，销毁则按实现方式减少或终止相应通证单位。它们可能相互联系，但不能被当作同一过程的不同名称。

发行首先需要有明确权限和用途。谁能够决定发行、依据什么规则、面向哪些事项以及受到什么总量或期间限制，应当可以核查。技术人员能够调用创建单位的功能，并不构成其自行决定新增权益的依据。发行规则应当与上一章的权利内容及履行责任相衔接。

制度上的发行批准、技术上的铸造和向参与者分配，也需要分别记录。可以预先创建一批单位并由组织保管，再按条件分配；也可以在有关条件满足后创建相应单位。预留在合约或组织账户中的通证，不应全部被展示为参与者已经取得的权益。

新增单位的影响需要按其功能判断。如果某项安排按单位占比配置有限资源，增加参与单位可能改变原有持有者的相对比例；若单位对应新增服务能力，则需要检查能力是否同步形成。发行增加并不自动意味着资本增加，也不能保证有关义务获得了更多履行资源。

归属在本章中主要指，依据既定条件确认参与者对有关通证或关联权益的取得安排。它可以取决于时间、已确认贡献、持续参与或明确的里程碑。制度应当说明归属的对象，以及它对取消、转移和履行有什么影响，不能把一个技术字段直接当作全部法律归属的结论。

条件归属需要证据和确定程序。时间经过可以由系统处理，交付质量或持续履行则可能需要外部核验。满足部分条件时，可以按照约定确认相应部分；尚未满足的部分应当保留其条件状态。不能因为单位已经创建，就跳过贡献确认和必要的业务判断。

归属、释放与可转让也可能不同步。参与者可以已经满足取得条件，但仍受一定期间的转移限制；某项单位可以具备领取条件，却尚未被实际领取。系统应当分别表达已归属、可领取、已领取和可转让的范围，使持有者理解哪些动作目前可以完成。

智能合约可以执行部分时间安排。OpenZeppelin 的归属钱包提供按约定时间表释放资产的机制，其文档同时指出，该钱包的控制权可以转移，因此锁住资产并不保证关联的未归属经济安排完全无法被转移。本书据此强调，应当检查完整的控制关系，而不仅是表面的释放日期。OpenZeppelin：归属钱包及时间安排〔3〕

锁定需要说明限制的具体操作。禁止转出、暂停领取、限制使用或停止某类授权，具有不同含义。已经锁定的通证是否仍可参与某次治理或其他安排，也需要单独规定。锁定期限、解除条件及紧急处理权限，应当随状态一起清楚呈现。

锁定可以帮助执行时间承诺或保留争议处理条件，但不能单凭锁定推定忠诚、真实贡献或履行能力。参与者暂时无法转出，不说明其必然持续提供有效工作；流通数量暂时减少，也不保证价格上升。制度应当根据需要限制操作，而不是把限制本身作为价值创造的证明。

撤销需要明确针对哪一项制度状态。可以撤销某个资格、未满足条件的分配安排或已被认定错误的确认，但各自依据不同。已经归属的部分是否可以调整，需要适用规则和相应程序；管理员能够技术上冻结或移除记录，不意味着其可以任意取消既有权益。

撤销操作授权又与撤销权益不同。停止某个代理人代为转出的权限，通常只是改变操作条件；有关权益是否仍由原主体享有，需要保留原有依据。系统应当区分这类操作，避免用同一个“撤销”标记掩盖不同后果。

销毁则需要核实实际实现。通过具有相应逻辑的销毁操作减少记录中的总量，与把通证转入一个通常无法使用的地址，不一定具有相同的供应记录效果。应当说明哪些单位已经在协议中终止，哪些仍被计入总量但无法正常流通，而不能只凭展示标签判断数量变化。

销毁也不自动等于履行。在某些安排中，消耗或销毁单位可以是领取服务的一步，但还需要确认服务是否提供；在其他安排中，销毁可能只意味着持有人放弃某项技术单位。它对关联权利和义务有什么效果，应当由制度说明，不能概括为销毁后全部责任都消失。

环节	需要明确的制度问题	不宜混同的状态
发行与分配	谁批准，面向什么用途，哪些单位交给谁	已批准、已铸造、组织保管与已分配
归属	参与者满足哪些取得或保留条件	预期资格、部分归属与已满足条件
锁定与释放	限制什么操作，何时及怎样解除	已归属、可领取、已领取与可转让
撤销	改变哪项资格或授权，依据什么程序	操作权限、权益状态与历史事实
销毁	终止哪些技术单位，如何影响关联安排	供应减少、失去流通能力与实际履行

数量核对需要采用清楚口径。发行上限、已创建总量、组织保管数量、已分配数量和实际可流通数量，可以分别有意义，却不是可以互相替换的概念。针对固定计量单位且没有其他自动增减机制的系统，可以将期初数量、新增和销毁进行核对；存在其他机制时，需要单独解释其影响。

迁移和跨系统映射还应当检查重复表达。原系统中的单位被锁定，新系统中出现关联单位，可能是同一安排的不同技术表现，不能直接视为两份新增权益。需要说明兑换、解除和失效条件，并通过核对避免重复使用。具体跨组织衔接将在后续章节进一步讨论。

整个生命周期都需要保留规则版本、决定主体、时间、对象和结果。异常操作、条件争议或系统中断时，应当能够恢复到可解释的处理状态，并使受影响主体获得必要说明。通证机制的完整性，体现为各个环节能够对应制度，而不是只有发行和转移两种动作。

四、贡献激励、交易价格与企业价值的区分

贡献激励关注制度怎样影响参与者的行动。通证可以使获得资格、使用资源或参与某项回报的条件更清楚，也可能降低部分核验和分配成本。但参与者是否因此作出更有用的贡献，仍取决于认可是否可信、条件是否合理，以及相应安排能否实际履行。

激励需要先明确希望促进什么。提高交付质量、支持知识共享、维持长期协作与鼓励必要维护，可能需要不同规则。若只按活动次数发放，参与者可能优先增加可计数动作；若只奖励可见结果，支持性工作又可能被忽略。发放机制应当返回前几章形成的贡献确认与计量条件。

通证激励也不必全部依赖出售。某些单位可以用于适当的资源使用、参与机会或其他明确安排。参与者愿意取得单位，可能来自这些功能，也可能来自对未来交易价格的预期。制度需要说明预期建立在什么基础上，不能把依赖买方接手的安排表述为组织已经保证的回报。

奖励来源应当能够追溯。组织从已经持有的通证中分配，与新增发行，是不同的数量变化；支付真实经营资源，与发放一项未来有条件资格，也具有不同后果。发放了更多单位，只说明完成了相应技术或制度动作，不自动说明参与者获得了等额可支配资源。

若单位使持有人参与某个有限资源池，新增发行还可能改变相对份额。评价激励效果时，需要同时考察新增参与是否扩大了真实创造基础，以及有关分配条件是否保持清楚。不能仅用每期奖励数量证明参与者不断增加财富，也不能把所有新增发行一律视为没有组织作用。

交易价格回答的是在特定市场条件下，买卖双方以什么条件完成交换。它受到供求、流通限制、预期和交易条件影响，可能吸收关于真实作用的信息，也可能与经营情况显著偏离。价格上涨不能单独证明贡献增加，价格下降也不能直接否定已经核验的履约事实。

市场报价还需要结合成交规模理解。Uniswap 的说明指出，交易对流动性池价格的影响与流动性有关，较低流动性可能对应较大的价格冲击。这说明一个显示价格不能直接代表任意数量都能按同样条件成交。Uniswap：价格冲击与流动性〔4〕

以某个参考价格乘以流通数量，可以得到相应口径的流通市值估计；采用其他供应口径，则必须另行说明。这样的计算并不等于全部持有人可以同时获得同额现金，也不等于组织已经拥有这些资源。少量成交形成的价格，不能被无条件应用于全部单位的兑现。

二级市场交易中的资金通常由买方向卖方支付，具体费用另按交易安排处理。它不因交易对象与企业有关，就自动成为企业收入。企业取得的发行资金、服务收入、交易费用及其承担的相关义务，也应当分别核算，不能把所有资金流入都解释为已经创造的利润。

企业价值则需要结合持续经营、资源和能力、未来经济作用及其实现条件分析。通证可能只对应其中一项用途或一部分安排，也可能没有对企业整体价值的直接请求关系。因此，通证市场估值与企业价值之间，需要先说明具体权利和经济联系，不能直接画等号。

即使通证关联某种收益安排，其价格也不因此成为精确的经营评价。分配范围、优先条件、期限、风险和市场流动性都会影响解释。持有人取得的是哪种请求或资格，需要回到权益结构，而不能仅凭单位能够交易就推断其等同股权。

贡献、价格与经营能力之间可以形成实际联系，但需要逐步验证。制度激励可能支持有效投入，投入可能形成可持续能力，能力可能改善经营结果，而有关结果又可能影响权益履行和市场预期。每一步都有条件，也可能中断，不能只凭价格变化倒推出整条联系已经成立。

价格信号还可能反过来改变协作。短期交易受到过度关注时，维护、培训和长期探索可能被挤压；若市场转移与治理权紧密绑定，购买行为还可能改变决策结构。组织需要辨认这些变化是否符合共同创造目标，而不是只以交易活跃衡量制度成功。

锁定、销毁和回购等安排同样需要回到具体效果。减少某种口径的可流通数量，不保证需求、经营能力或履行资源增加；使用组织资源支持市场交易，也需要说明授权、资源用途及其对其他义务的影响。供应操作与价值创造应当分别评价。

评价通证机制时，应当同时观察贡献质量、履行可靠性、参与者实际取得的利益、必要协作是否持续以及运行成本。交易价格和活跃度可以作为特定观察信息，但不足以替代这些指标。还可以在条件适当时与不采用通证的安排比较，检查改善究竟来自通证机制还是其他组织变化。

本书尤其重视参与者能否理解自己的选择。奖励数量、归属状态、转移限制、实际用途和实现条件应当分别可查，不能只显示一个随参考价格变化的“总价值”。透明表达不是要求展示所有技术细节，而是使参与者能够判断自己取得了什么、还依赖什么。

面向未来，本书提出一个需要检验的方向：让通证机制围绕真实贡献、可用能力和可履行权益形成反馈，并允许治理根据证据调整规则。调整需要保留授权、版本和稳定承诺，不能让价格算法或短期指标自行改写参与者的权利。若机制只增加发行和交易，却没有改善共同创造，就应当重新判断其必要性。

通证由此被置于利益相关者资本治理的具体位置：它可以表达单位、约束操作并支持部分协作，但不代替贡献事实、资本形成和价值判断。单位能否正确流转与组织能否持续创造，需要分别检验，再通过清楚的权益和履行安排建立联系。

下一章将转向收益核算与分配执行，进一步讨论哪些资源可以进入分配，谁在什么期间符合条件，以及链上记录如何与实际支付对账。只有来源清楚、计算有据并完成相应履行，制度中的回报安排才真正进入共同创造者的现实生活。

定稿补强：通证按经济实质而非名称处理

同一种通证标准可以承载完全不同的制度关系，不同技术标准也可以表达相似义务。因此，发行人与持有人都应根据取得方式、权利义务、业务模式、流动性、赎回、减值、终止和披露要求分析处理，而不能建立一种适用于所有通证的会计或法律结论。

发行、归属、锁定、撤销与销毁应分别影响技术状态和基础义务。销毁一个技术单位不当然消灭发行人的链下责任；撤销资格也不能无依据地消灭已经成立的请求。需要合规识别的价值流转，应采用第十三章的分级身份方法，避免一方面让高风险流转无法追责，另一方面为低风险参与过度收集数据。

本章注释

1. [SRC-024] Ethereum Improvement Proposals: ERC-20 通证标准。[原文或官方页面](#)

- 本章引证：Ethereum：ERC-20 通证标准。
- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：Ethereum：ERC-20 通证标准。
- 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-025] Ethereum Improvement Proposals: ERC-5192 最小账户绑定通证接口。[原文或官方页面](#)

- 本章引证：Ethereum：ERC-5192 最小账户绑定通证接口。
- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：Ethereum：ERC-5192 最小账户绑定通证接口。
- 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

3. [SRC-017] OpenZeppelin: OpenZeppelin 的 VestingWallet 文档。[原文或官方页面](#)

- 本章引证：OpenZeppelin：归属钱包及时间安排。
- 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：OpenZeppelin：归属钱包及时间安排、OpenZeppelin 的 VestingWallet 文档。
- 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
- 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。

4. [SRC-070] Uniswap Labs: Uniswap: 价格冲击与流动性。[原文或官方页面](#)

- 本章引证：Uniswap：价格冲击与流动性。
- 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：Uniswap：价格冲击与流动性。
- 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
- 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第二十章 收益核算与分配执行

共同创造能否成为共同成长的资本，既取决于组织能否形成持续创造的能力，也取决于参与者能否依据清楚的制度分享成果。贡献得到确认、权益已经表达、通证可以流转，只完成了其中一部分。回报还需要经过资源确认、资格核验、金额计算和实际履行，才能进入参与者的生活与后续行动。

上一章将贡献激励、通证价格与企业价值分别讨论。本章进一步追问：组织究竟以什么资源履行回报安排，这些资源可以分配给谁，采用哪一版规则计算，又怎样证明已经完成支付。市场报价不能回答这些问题，智能合约中的余额和分配按钮也不能独立回答。

本章所说的收益核算与分配执行，涵盖利益相关者回报安排中的资源核算和履行程序，但不把所有回报都归为利润分红。报酬、费用偿付、有条件的收益分享与其他经济请求，可能具有不同依据。制度技术的任务，是让这些差别在从业务到支付的全过程中保持清楚，并使每项处理能够追溯到事实、规则与责任。

一、收益来源与可分配资源的确认

收益首先需要回答来源问题。组织通过提供产品或服务取得的收入、持有资产产生的回报、处置资源取得的款项，以及外部主体提供的资金，具有不同经济性质。来源不同，伴随的成本、义务、限制与持续性也不同。如果只把所有流入汇总为一个“收益池”，参与者就难以判断自己分享的是经营成果、资产处置所得，还是需要组织继续履行义务的资金。

核算应当从明确边界开始。哪一个主体承担回报义务，核算哪一项业务或哪一个范围，覆盖什么期间，采用什么计量单位，都需要事先说明。共同事业可以跨越多个组织，但各组织拥有的资源和承担的义务不能因此自动合并。合作方账上存在资金，并不意味着支付主体已经能够支配这些资金；组织之间发生内部划转，也不必然形成共同体系新增的经营成果。

收入确认与收款时点需要分别处理。在 IFRS 15 所适用的客户合同收入核算中，收入确认与承诺商品或服务的转移及履约义务的满足相关。因此，收到了预付款和已经完成收入确认，不能仅凭资金到账被合并为一个事实。这里引用这一原则，是为了说明核算需要业务依据，具体组织仍须使用其适用的会计制度。IFRS Foundation：IFRS 15 客户合同收入〔1〕

利润与现金流同样回答不同问题。某个期间已经确认的经营成果，可能包含尚未收回的款项；账户现金增加，也可能来自借款、出资或资产变现。IAS 7 将现金流区分为经营、投资与筹资活动，并在间接法中通过非现金事项等调整连接损益与经营现金流。核算中的这种区分，提示分配制度不能把利润、收款和账户余额当作同一个数字。IFRS Foundation：IAS 7 现金流量表〔2〕

对利益相关者资本治理而言，回报安排的性质还会影响成本与分配的边界。按约定应当支付的劳动报酬、采购款或费用偿付，不能只因领取者也是共同创造者，就全部移到利润形成之后再决定是否支付。某项回报应计入何种核算项目，需要根据其实际性质和适用制度判断。若已经作为成本或义务处理，后续计算也应避免以同一名义再次扣除或重复分配。

由此，可分配资源需要经过三方面核验：分配依据允许什么，现实资源能够支持什么，有权程序决定本期安排什么。第一方面涉及权益和用途边界，第二方面涉及资源控制与履行能力，第三方面涉及具体方案的有效形成。三者相互制约，不能让账户可见余额替代全部判断，也不能让一个分配决定凭空补足缺失的资源。

资源控制应当查明对象和限制。代为保管的资产、限定用途的资金、已为其他义务作出安排的资源，以及尚未收回的款项，都需要分别表达。即使某项资产已经在组织控制的钱包中，也需要判断其经济归属、使用约束与实际可转移状态。控制能力可以支持履行，却不是任意分配的充分依据。

准备本期分配时，还要识别与履行有关的必要支出、既有义务和资源需求。这里不能使用一条脱离核算口径的通用减法：某项支出若已反映在所采用的净额中，再次扣除就会压低结果；某项资源若同时被多个分配池引用，又会夸大支付能力。每一项调整都应说明进入哪一个口径、是否已经计算，以及对哪些安排产生影响。

核验对象	需要说明的内容	可以支持的判断
业务成果	来源、期间、履约事实与核算依据	哪些成果可以纳入本期核算
资源状态	归属、控制、限制与可用时间	哪些资源能够用于相应履行
既有安排	已成立义务、用途承诺及已占用额度	哪些资源不能再次安排
分配决定	WISERUNION 权限、对象、额度、条件与生效记录	本期可以按何种方案执行133 / 240

组织保留资源用于维护、研发和长期能力建设，可以服务于共同成长，但保留安排也需要接受治理。其依据、用途、期限与效果应当可解释，不能长期依靠一个没有边界的“发展需要”压缩所有回报。反过来，分配比例不断提高也不自动意味着治理改善；若由此损害必要维护和持续履行能力，当期领取者的收益可能以未来参与者承担成本为代价。

对于现金以外的分配，还需要明确交付对象。支付某种数字资产、提供使用额度和支付约定货币，是不同履行内容。计量价格可以帮助比较，却不能自行将一种对象替换成另一种对象。兑换时点、费用承担、价格来源和差额处理，应当与原有权利安排衔接；有无被认可的替代履行依据，比系统是否支持兑换更重要。

组织自行发行的单位尤其需要单独说明。增加单位数量可以完成一种奖励或资格配置，但不能仅以参考价格乘以数量证明形成了等额可分配经营资源。若单位对应未来请求，还应继续记录其条件与相关义务；若其回报依赖外部买方接手，也应保持这一来源区别。

资源确认最后应形成可复核的核算说明。它应连接业务证据、核算调整、资源清单与分配授权，并保留尚待确认的事项。记录摘要或核验结果可以进入共享账本，明细则依据必要性与权限保存。账本使各方更容易识别共同采用了哪份结果，结果是否完整、真实和适当，仍需要业务核验与独立复核支持。

确认资源的意义，是为承诺建立可履行的基础。如果本期尚无满足条件的新增分配资源，就应如实表达；对于此前已经成立而尚未支付的义务，则继续记录其金额、期限和处理状态。没有新的分配能力，与没有既有支付责任，是两个需要同时看清的问题。

二、分配资格、规则版本与计算周期

资源确认之后，需要识别谁有资格参与哪一项分配。贡献事实、资本记录、收益资格与应付金额之间虽然可以建立联系，却不能省略中间的制度条件。完成贡献可能取得某种计量结果；该结果是否进入资本安排，以及何时形成经济请求，需要分别适用对应规则。钱包持有量只有在特定制度明确赋予相关效果时，才能成为分配依据。

资格应当对应具体安排，而不是一个永久通用的“成员”标签。同一主体可能在不同业务、期间和角色下拥有不同资格。曾经参与合作不必然意味着无限期分享一切新增成果，当前退出某项角色也不必然使已经形成的请求消失。核验需要把主体身份、权利来源、有效期间、附加条件与适用范围联系起来。

本书主张将资格名单、计算结果和履行清单分别保留。资格名单回答谁可以进入某项计算；计算结果回答依规定口径得到多少；履行清单则在请求已经成立、支付安排已经有效且操作条件具备时，说明接下来应完成什么。三者可以由同一系统连接，但不宜用一个“待领取余额”覆盖全部状态。

规则版本决定这些连接怎样发生。一个完整版本至少应能指向资格条件、资源口径、权重或比例、期间定义、调整办法、舍入规则和必要的例外程序，并说明制定权限及生效时间。程序版本与制度版本也应对应：计算程序经过修改，不当然意味着有权改变参与者的回报条件；制度修订生效，也需要确认执行系统已经准确承接。

分配中的时间不是一个日期。贡献发生期间、成果核算期间、资格确定时点、决定生效时间、可申请时间和实际支付时间，可能分别存在。某月支付上季度已经成立的请求，并不会因此将贡献或经营成果改归本月。区分这些时间，才能解释跨期变化以及为什么同一参与者在不同清单中呈现不同状态。

对于可流转权益，需要说明收益资格怎样随时间划分。如果采用某个时点的持有状态，就应明确该时点与所属期间的关系，转移前已经独立成立的请求是否随同转移，以及怎样防止转出方与转入方重复领取。如果采用期间内的有效持有量或其他连续条件，也应说明计算范围与中断处理。没有哪一种时间设计天然适合全部权益。

身份与地址之间的对应也须采用正确的历史状态。地址更换、代理关系终止、托管转出或组织名称变更，可能只改变支付路径或经办主体。核验应根据有关资格与请求的归属处理，避免一个主体通过多个账户重复取得同一份额，也避免因更换工具而丢失既有请求。

在仅按有效权重分配一个已获授权、非负且确定的资源池时，可以用一个简单关系说明计算：某主体本期份额，等于该资源池乘以该主体有效权重占全部合格主体有效权重的比例。这一关系成立的前提，是权重口径一致、总权重大于零，并且该池不存在需要另行处理的优先安排、上限或其他条件。它描述一种方案，并不证明这种方案公平，更不适用于所有固定支付请求。

若工资、合同款等请求已经依其依据独立成立，就不能未经有效依据，把它们与有条件的剩余分享资格一起按池内余额同比缩减。若制度选择对不同类别分别配置资源，则需要先说明类别之间的安排，再在各类别内部计算。公式能够保证输入相同得到相同结果，不能替代对分类、权重与顺序的授权。

计算还包括对精度与边界的处理。最小支付单位、舍入方向、尾差归属、零权重、负向调整和金额上限，都可能影响结果。小额请求若因支付成本暂时合并，也应保留其归属和累计记录；是否设定处理期限及到期效果，需要有明确依据。技术上的最低转账额度不应悄然成为取消小额权利的规则。

为了使结果可以复算，每一批计算需要固定所使用的资源数据、资格数据、规则版本与必要参数，并记录生成和复核结果。这种固定是保留计算依据，不是禁止后续纠错。组织应当能够重现“当时为什么得出这一金额”，再解释新的证据导致哪些差异。

发现迟到证据、遗漏贡献或计算错误时，可以依既定程序进行补充计算、冲正或跨期调整。已经支付的部分、尚未支付的部分与仍有争议的部分应分别处理。不能为了让新结果看起来连续，直接覆盖旧版本；也不能把修正事实错误当作随意追溯改变分配政策的理由。

每期分配因此应形成一条可以跟随的关系：资源确认指向有效方案，方案指向适用资格与计算依据，计算结果再指向成立的请求和支付安排。参与者无需看到全部程序细节，但应能查明自己的资格、金额、期间、限制及提出异议的途径。可解释的结果，是制度执行获得持续认可的重要条件。

三、链上分配与链下支付的对账

分配执行可能全部发生在链上，也可能通过银行账户、支付服务或其他链下方式完成，还可能由多个环节共同构成。无论采用哪一种路径，对账都需要回答同样的问题：原来应向谁履行什么，实际发生了哪些操作，这些操作完成了多少义务，还剩下什么。技术路径可以不同，制度中的对象和责任必须能够对应。

首先应当区分分配结果的登记与资源转移。系统把某个金额记入参与者账户，可以表示计算完成、请求成立或额度可申请，具体含义取决于制度定义。只有在相应履行确实发生时，才能继续确认已付状态。将内部余额命名为“到账”，并不能消除领取限制、资金缺口或外部支付尚未完成的事实。

链上执行也存在多个阶段。交易提交、被区块收录、执行成功以及达到适用的最终性条件，需要分别观察。以太坊的接口文档分别提供交易回执中的执行状态，以及用于查询已最终确定区块的标识。这些信息支持技术核验，但它们并不直接说明某一现实经济请求已经得到完整履行。Ethereum：交易回执与区块状态查询〔3〕

具体支付还要检查正确的网络、资产标识、接收地址、数量和业务对象。合约调用成功可能只完成授权或更新某个记录；即使发生转移，也需要核验其是否对应约定资产与请求。存在转移费用、特殊余额机制或中间合约时，实际到达结果还须根据具体机制确认。一个交易编号不能替代这些对应检查。

当制度约定以某种链上资产向有效指定的地址履行，且相应转移满足既定条件时，该转移可以作为完成有关支付的证据。若原来约定的是链下货币到账、兑换后交付或其他结果，则应继续核验后续环节。协议中的最终性与义务是否履行完毕，具有不同判断对象，二者需要通过明确的履行条款连接。

链下支付同样不能只凭发起记录关闭请求。付款文件已生成、支付机构已受理、付款账户已扣款和收款结果已经确认，可能分别发生。回执的证明范围应当根据支付渠道判断；只表明提交或处理中，就只能支持相应状态。退款、退票、拒收或后续更正也应进入持续对账。

共享账本可以保存链下回执的摘要、来源和确认记录，但回执上传者仍承担相应的信息输入责任。摘要能够帮助核对文件是否为同一版本，不能证明回执内容必然真实。重要支付需要能够回到可信来源查验，并说明谁负责处理来源矛盾或状态更新。

履行阶段	应保留的主要依据	对外表达的状态
请求已成立	权益依据、适用结果与有效决定	已确认应付，注明金额和期限
支付已安排	经核验的收款路径、金额与操作授权	待执行或已排期
操作已提交	链上交易或链下支付指令的识别信息	已提交，结果尚待确认
履行已核验	符合约定范围的转移或收款证据	已支付相应部分，注明剩余部分
发生异常	失败、退回、分歧及后续处理依据	异常处理中，保留原请求联系

这张表表达的是履行关系，不要求全部系统采用同一套界面状态。关键在于每种状态都具有明确证据门槛，不能由经办者仅凭主观判断推进，也不能因为某个外部系统暂时没有返回结果，就自动将请求视为已失败或已完成。

为连接多条记录，每项支付请求应具有稳定的业务识别号，每次执行尝试另有操作识别信息。一次请求可以分次支付，也可以因失败而多次尝试；一次批量操作又可能对应多个请求。因此，对账需要保存请求、操作与实际结果之间的映射，逐项分摊金额，不能简单假定一笔交易就等于一个完整请求。

防止重复付款尤其依赖这种分工。同一请求同时允许链上领取和链下支付时，应有共同的领取或支付控制，并将已经进入执行、结果仍待查明的一部分单独保留。发生超时后，先查询原操作结果，再决定是否重试；只有确认不会形成重复履行，或已通过适当机制协调后续处理，才能重新发起。单个区块链拒绝重复支出，并不自动阻止另一个系统再次向同一主体付款。

跨系统操作通常不能被假定为同时完成。链上已经更新，银行支付却尚未完成；银行已经扣款，链上确认又暂时中断，都可能使两边处于不同阶段。此时应建立差异处理记录，指定核验责任并限制冲突操作。恢复后的任务是把实际结果准确接回原请求，而不是把所有记录强行改成同一种状态。

对账还需要统一金额解释。原请求采用何种单位，实际支付使用何种资产，换算依据是什么，手续费及适用扣缴由谁承担，都应在结果中明确。组织支出的总额、向收款人支付的净额以及依法或依约另行处理的款项可能不同；相关扣减必须有依据和去向，不能仅以总扣款与应付金额接近作为已经足额履行的证明。

在同一计量口径下，期初未履行请求、本期新增请求、有效调整、实际履行与期末未履行结果应当能够衔接。资源账户的变动则另行与资金或资产流水核对。两套衔接需要相互支持：支付流水真实存在，不证明全部应付对象已经覆盖；应付清单被标记完成，也不证明资源确已交付。总额相符之后，仍需逐项检查漏付、错付和重复支付。

已核验支付之后发生退回或错误确认，应通过有依据的更正反映结果，并保留原操作历史。多付部分的追索、抵扣或其他处理，需要相应依据和程序；不能因为系统能够从下一期余额扣除，就跳过有关主体的权利和异议处理。纠正记录与完成补偿也应分别呈现。

主动批量支付与参与者自行领取，都需要匹配实际使用条件。批量支付应追踪每个对象的结果；自行领取应说明申请条件、资源准备、操作成本 and 无法操作时的替代路径。已经取得资格的人长期无法领取，仍然是履行问题，不能用合约界面保持开放证明安排已经实现。

对账的透明性可以分层提供。参与者可以核验自己的请求、计算和支付记录，授权复核者可以检查总体勾稽关系，其他主体则在适当范围内了解分配总量与差异处理。个人收款账户和全部收入明细没有必要因此向所有人公开。可核验性应当扩大监督能力，同时保留合理的信息边界。

四、亏损、延期、退出与争议的处理

分配制度的完整性，体现于条件变化时仍然能够解释责任。经营亏损、现金不足、系统故障、资格争议和主体退出，影响的对象与后果各不相同。如果系统只设计顺利分配的路径，异常发生时就容易把不同问题统一处理为余额归零、暂停领取或等待通知，使原来承诺的边界变得模糊。

亏损首先需要在核算上说明来源、期间和影响范围。某项业务的损失是否影响另一项业务的分配，是否与共同承担的风险相关，应依据已经确定的组织和权益安排判断。不能仅因为全部账户位于同一平台，就默认任何局部损失均由所有参与者共同承担。

对于取决于未来可分配成果资格，亏损可能导致本期不满足新增分配条件；对于已经独立成立的支付义务，亏损则意味着履行能力可能受到影响，需要进一步处理。二者不能混写为“本期无收益，所以全部请求取消”。本书强调的风险承担，是识别各类主体依据什么承担哪些后果，而不是把组织困难转化为所有参与者无差别承担的责任。

制度若设置亏损结转、资源补足或后续收益先行弥补的机制，应事先说明适用范围、计算口径和时间条件，并接受相应授权约束。这类安排可能影响不同期间参与者之间的负担分配，因此还需解释新加入者、已退出者和持续参与者各自承担什么。不能在结果已经出现之后，仅因某一群体缺少技术控制权就把损失移到其账户。

经营损失与贡献事实也应分别记录。已经完成并获得确认的贡献，不因企业后来亏损而自动成为未发生；贡献所支持的资本能力却可能发生减损，相关权益的经济实现也可能受到影响。保留这种区别，才能同时承认历史行动、评价现实能力，并诚实说明回报的不确定性。

正常经营风险、事实造假、越权分配和操作过失，则需要不同的责任判断。发生损失并不当然证明某个经办者违规；存在违规证据，也不应仅用“共同承担风险”代替调查。技术记录可以支持重建事实，责任认定仍需要证据审查、利益冲突处理与有权程序。

延期处理应当明确延后的是哪个环节。核算尚未完成、资格仍在复核、支付已经到期但资金不足，以及支付渠道暂时中断，不能统一显示为“未解锁”。通知应说明影响对象、当前状态、原因、负责主体、预计处理时间及下一次复核安排。暂时无法确定最终时间，也应提供持续更新的责任和节点。

当已经成立的请求需要改变履行时间或方式时，应依据适用的权利安排和必要程序处理。技术管理员能够修改锁定时间，并不意味着已经获得修改支付期限的权力。对于可以分阶段履行的安排，应当保留原请求、已履行部分和后续安排，防止一次小额支付被误写为全部解决。

资源紧张时，支付顺序也需要有依据。适用法律、合同和有效制度对有关请求的约束，应进入方案判断，不能由界面排队顺序或管理者临时偏好替代。若已经进入需要专门清偿或重整程序的情形，内部算法也不能自行定义全部请求的地位。对资源不足的承认，应当促成有权处理，而不是使自动化执行越过其适用范围。

退出则应当拆分关系终止与请求结算。停止承担未来任务、失去某项持续资格、转让特定权益和领取已经形成的应付款，可以分别发生。退出账户的关闭时间不应决定全部历史权益是否存在。系统需要保留必要的身份联系、送达方式和后续结算渠道，使已经离开日常协作的人仍能处理未了事项。

退出条件还应说明未完成任务、条件尚未满足的奖励、有效锁定和后续证据修订如何处理。若存在结算准备或暂缓支付安排，需要明确依据、范围、期限及复核途径。已经满足条件的部分与尚待满足条件的部分应分别列明，避免用一个没有明细的“退出折扣”覆盖不同性质的调整。

争议处理可以从明确争议对象开始。参与者可能争议贡献事实、资格认定、规则适用、计算金额或支付结果，每一类需要不同证据和复核能力。账本上的共同确认可以证明系统曾采用某份记录，却不能排除该记录所依据的事实或授权存在问题。程序应让提出异议的人能够指向具体事项，而不必重新证明整个制度是否有效。

有效的处理需要受理渠道、提交依据、回应期限、回避安排和可说明理由的结果。涉及共同资源的事项可以接受相应监督，但个人明细仍应在必要范围内使用。无争议部分若能够依制度独立履行，应继续处理；确需保留争议资源时，也应记录范围和解除条件，避免局部争议成为无限期冻结全部回报的理由。

决定更正后，系统应把结果落实为补付、恢复资格、调整未付金额或其他有依据的行动，并与原记录相连。已经最终确认的链上交易未必能够被技术撤回，但组织仍可根据实际条件，通过新的操作、补偿或其他适当途径纠正其制度后果。历史不可轻易改写，并不意味着错误不再需要处理。

面向未来，本书提出一个需要检验的方向：让分配系统持续维护从资源来源到未履行请求的证据联系，使参与者能够在权限范围内核验承诺获得了多少资源支持、哪些履行已经发生、哪些差异仍待解决。这样的系统能否改善协作，需要观察遗漏和重复支付是否减少、争议处理是否及时、维护成本是否合理，以及参与者是否更容易理解并行使自己的权利。共享记录的规模，本身不是制度成效。

至此，从贡献确认、资本形成到权益配置与收益执行，形成了一条相互衔接又不能省略判断的制度过程。共同创造能够支持资本延续，资本运用可能形成经济成果，有效权益安排决定参与者可以提出何种请求，核算与支付则使有关请求得到实际处理。每一步都需要明确条件，也都需要有人承担决定、核验和纠错的责任。

下一篇将转向协同治理。谁有权确认分配方案、谁代表受到影响的主体、谁监督执行并修订规则，已经无法仅靠账本状态一致来回答。第二十一章将从技术共识与多方治理的分别配置出发，进一步讨论共同账本之上的组织权力与参与秩序。

定稿补强：可分配资源瀑布、税费与亏损

分配必须沿一条可解释的资源瀑布进行：先确认收入或其他资源来源，再扣除成本费用、税费与到期义务，检查法定或合同限制与必要储备，确认现金或其他支付资源可用，取得治理批准，最后计算个体应付。收入、利润、现金、通证价格和可分配资源不是同一个数值；任何一步尚未成立，都不能由后续公式补足。

层次	核心问题	责任证据
收入及资源来源	来源是否已经按适用口径确认	合同、业务和会计记录
成本、税费与义务	哪些金额必须先行承担	账簿、税务和支付凭证
限制与储备	是否存在资本维持、偿付、合同或治理限制	法律/财务审查与批准
可用现金或资产	能否实际支付，币种和时间为何	银行、托管或链上余额
分配批准	规则版本、周期、门槛是否有效	决议与快照
个体应付	毛额、代扣、费用和净额为何	分配明细与回执

分配批次还应记录税费类型、代扣主体、汇率来源与时点、手续费承担、支付失败和重新支付。发生错误或后续损失时，准备金、负余额、追回、抵扣、时效和争议规则必须在分配前有效存在，不得事后任意转嫁。组织应向参与者披露流动性和长期投入约束，使公式正确与组织持续经营同时接受审查。

本章的制度关系可结合[附录七](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。



图14-1 从承诺、贡献到权益与回报

图14-1 从承诺、贡献到权益与回报。每个箭头都是独立判断关口，不允许用一条记录跨越全部制度门槛

本章注释

- [SRC-054] 国际财务报告准则基金会（IFRS Foundation）：[IFRS 15 客户合同收入](#)。[原文或官方页面](#)
 - 本章引证：IFRS Foundation：IFRS 15 客户合同收入。
 - 支持范围：用于确认财务、审计、内部控制或公司治理中的规范口径，本书引用主题包括：IFRS Foundation：IFRS 15 客户合同收入。
 - 使用边界：规范口径需要结合适用主体、报告目的和具体交易事实，不宜机械移用于链上权益。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-053] 国际财务报告准则基金会（IFRS Foundation）：[IAS 7 现金流量表](#)。[原文或官方页面](#)
 - 本章引证：IFRS Foundation：IAS 7 现金流量表。
 - 支持范围：用于确认财务、审计、内部控制或公司治理中的规范口径，本书引用主题包括：IFRS Foundation：IAS 7 现金流量表。
 - 使用边界：规范口径需要结合适用主体、报告目的和具体交易事实，不宜机械移用于链上权益。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-029] Ethereum.org：[交易回执与区块状态查询](#)。[原文或官方页面](#)
 - 本章引证：Ethereum：交易回执与区块状态查询。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：Ethereum：交易回执与区块状态查询。

第五篇 协同治理：制度 如何运行、监督与修订

共同账本使参与者能够依据同一套协议核验记录，却不会自动回答共同事业应当朝什么方向发展。当组织需要决定资本如何使用、回报如何安排、谁承担风险以及规则如何改变时，问题已经超出交易是否有效、状态是否一致的范围，进入不同主体如何共同决定并承担责任的治理领域。

上一章讨论了收益核算与分配执行。分配依据的确认、支付方案的授权和争议结果的落实，都要求明确谁有权作出决定。即使程序能够准确计算并自动执行，决定本身仍然需要适当的权限来源、参与条件与责任安排。没有这些基础，自动化可能只是更快地执行一种缺乏共同认可的权力关系。

本章所讨论的多方治理，是让与共同创造有关的不同主体，按照事项、关系和责任进入相应的决策过程。它既需要让重要利益能够被表达，也需要形成可以执行和追责的决定。区块链可以支持资格核验、程序记录和权限约束，而治理的正当性与有效性，需要在这些技术条件之外继续建立。

一、账本验证权与企业治理权的分别配置

账本验证权首先指向技术系统中的任务：检查交易是否满足协议规则，确认状态转换是否有效，并在具体共识机制下参与记录顺序或最终状态的形成。不同网络对验证、提议、排序和确认作出不同安排，运行验证软件与取得区块提议资格也并不总是同一件事。本章将这些能力放在账本确认秩序中理解，不把它们概括为对企业全部事务的决定权。

企业治理权则指向组织事项。谁可以提出资源配置方案，谁可以批准预算，谁可以决定某类权益条件，谁可以监督管理者，以及谁有权修订共同规则，都属于治理需要回答的问题。这些权限的依据来自组织制度及其适用的法律、合同与授权关系，而不是来自某个主体拥有更强的计算能力或更多的验证节点。

二者处理的正确性也不同。账本验证可以检查一笔支出是否得到系统要求的签名，却未必能够判断该项支出是否符合获批预算、是否遗漏利益冲突披露，或者是否损害某类参与者的既有权益。系统只会核验已经被准确表达并纳入执行的条件；尚未进入程序的制度要求，仍需要其他核验与责任机制承接。

因此，需要把协议条件与组织授权逐项连接。若一项资产转移要求有效预算、特定角色批准和独立复核，系统就应尽可能核验这些条件或它们的有效证明，并保留链下判断的依据。签名有效能够支持“某项密钥完成了授权动作”的判断，授权者是否在职责范围内行动，则还要回到组织权限。

协议自身的治理也应与企业治理区分。协议升级决定网络规则如何变化，应用治理决定某个系统怎样运行，企业治理决定现实组织怎样配置权利与责任。以太坊的治理说明明确区分核心协议变更与协议上的应用活动，并说明协议变更涉及链下的多方协调。这提示我们，即使讨论同一个技术生态，也不能把不同层次的治理压缩为一次统一投票。Ethereum：协议治理与参与主体〔1〕

本书据此主张，制度设计应先列出治理事项，再配置参与权限。对日常业务，可以在明确预算和职责内交由管理者决定；对跨部门资源调整，可以设置相应的共同审议；对影响基本权益的事项，则需要更严格的授权和受影响主体参与。不同层级能够分工，组织才不必把每项操作都交给全体表决。

权限层次	核心判断对象	需要明确的责任
账本验证与确认	记录是否符合协议、状态如何形成	按协议完成核验并承担相应网络职责
制度决策	某项组织安排是否应当采用	说明授权、利益影响、理由与决定依据
业务与技术执行	如何落实已经有效的决定	在权限和范围内执行并报告实际结果
监督与复核	程序、执行及结果是否符合要求	发现偏差、提出纠正并追踪处理

分别配置不意味着这些层次必须由完全不同的人承担，而是即使同一主体兼任多项职责，也需要说明每次以何种身份行动。技术维护者可以具有正式治理资格，但其表决依据应来自该资格；治理代表可以参与技术核验，但其代表身份不会使无效交易自动变得有效。

技术管理权限尤其需要纳入治理。能够升级合约、更换身份核验机构、修改数据输入源或调整紧急暂停条件的人，可能实质影响其他主体的权利行使。这些能力即使被命名为“运维”，也不能因此免于授权、监督与记录。判断权力大小，应看它能够改变什么，而不只看岗位名称。

将关键操作交由多人签署，可以减少单一密钥控制的部分风险，但签署人数并不直接证明代表性。多把密钥可能由同一控制者掌握，也可能由同一利益群体任命的人员持有。组织应同时核验技术上的操作分离与制度上的角色独立，才能理解多人签署真正提供了何种约束。

反过来，有效决定也需要真实的执行路径。表决通过后，若管理者仍可无理由拒绝执行，或者技术管理员可以另行改变执行内容，治理参与就难以产生稳定效果。制度应明确执行责任、完成条件和偏差报告，并让原决定与实际操作保持可核对的联系。

技术故障不宜被解释为原有治理授权自然转移。网络中断、密钥遗失或服务商退出时，组织仍需要依既定安排恢复操作、调整工具或采取适当替代方式。恢复程序可以赋予有限的临时权限，但应说明范围、期限与复核要求，避免维护连续性成为永久扩大控制权的理由。

区块链在这一层面的制度价值，是帮助各方检查权限是否得到遵守、决定是否被准确执行，以及例外是否留下依据。共同账本能够降低部分信息不对称，企业治理则为账本上的行动提供目的、边界与责任。两者衔接得越清楚，技术执行越能服务于真实的组织协作。

二、多类利益相关者的代表、提案与监督机制

共同创造涉及不同主体，但“受到影响”并不自动导出对所有事项拥有同等决定权。员工、客户、供应商、出资者、合作伙伴以及其他与组织存在重要关系的主体，其投入方式、依赖程度、风险承担和既有权利可能不同。多方治理需要把这些关系说明白，再决定各主体以何种方式参与哪些事项。

本书主张从事项影响出发识别参与范围。劳动安排直接影响承担工作的主体，产品使用规则涉及使用者，持续供给条件影响供应协作，资本使用与回报安排则可能同时影响多类主体。对于跨越多个关系的重大事项，应当说明各类影响如何进入讨论，而不是只邀请最容易召集或最容易量化的一方。

关系识别也应关注尚未充分进入账本的人。没有通证、缺少数字工具或尚未取得内部账户，不等于不受组织行为影响。对无法直接参与的相关利益，可以在有依据的范围内设置意见征集、专门评估或代表表达机制。代表者的任务和授权应当公开，不能仅以“代表未来”或“代表公共利益”的名称取得无限权力。

参与权可以分层安排。获得相关信息、提出意见、提交提案、参与审议、表决、监督执行和申请复核，分别具有不同作用。某一主体没有对全部经营事项的表决权，仍可以拥有与其权利相关的知情或异议渠道；某个代表有权提出建议，也不能被系统展示为已经获得最终批准权。

代表机制的关键，是建立代表与被代表者之间可检查的关系。代表如何产生，任期多长，负责哪些事项，应向谁报告，能否被撤换，以及职位空缺怎样补足，都需要明确。治理机构邀请某人列席，可以增加信息来源，但若缺少受代表群体的授权，就不宜将其意见直接等同于该群体的认可。

同一类别内部也存在差异。不同岗位的员工、不同规模的供应商、不同使用条件的客户，未必具有一致诉求。代表席位的安排应能够识别这些差异，避免最活跃、最富有资源或最接近管理层的一小部分人长期代替整个类别发言。具体方式可以包括适当的分组、轮换、公开征集与直接反馈，是否采用以及如何组合，需要结合事项规模与参与成本判断。

代表还需要获得履职条件。及时、易理解的信息，必要的准备时间，适当的专业支持和与被代表者沟通的渠道，决定了一个席位能否产生实际作用。如果会议材料只在表决前短暂出现，或者关键解释只能由提案方提供，形式上的参与就可能缺少独立判断基础。

参与成本应在组织制度中得到正视。治理工作消耗时间与专业劳动，完全依靠无偿投入可能使有闲暇、有资源的主体占据优势。合理的支持与补偿需要透明，并与代表职责相联系，避免演变为购买立场。是否参与治理，也不应在没有适当依据时成为领取已成立报酬或维持基本合作关系的额外条件。

提案机制则决定哪些问题能够进入共同讨论。提案资格、提交形式、必要资料和受理责任应当清楚，技术平台不能只开放一个输入框而不说明后续处理。提案至少需要解释拟解决的问题、建议方案、受影响主体、所需资源和主要不确定性，使不同参与者能够讨论同一个对象。

提出议题的门槛与作出决定的门槛应当分别设置。为了避免滥用，可以对正式提案设置合理的支持或资料要求，但也应保留让少量主体提出重要问题的途径。受理者拒绝纳入议程时，应说明适用理由并提供适当复核；否则，控制议程的人可能在投票发生之前就决定了治理结果。

提案进入程序后，实质修改也需要可见。调整影响对象、资源规模或权益条件，可能改变原先支持者的判断，不能仅保留提案名称就沿用所有先前授权。系统应记录版本、说明差异，并依据修改程度决定是否需要重新审议。这里的版本记录服务于真实理解，而不仅是保存一份文件摘要。

监督机制应当覆盖决定之后的行动。谁核验执行是否超出范围，谁检查预算使用，谁接收未履行报告，以及谁能够要求作出解释，都需要明确。监督者应在必要范围内获得证据，并具有独立报告渠道；若其接触信息和报告结果完全取决于被监督者同意，监督就容易失去实际作用。

数字工具能够降低这些程序的部分成本。它可以按角色发送通知，核验参与资格，记录提案处理和回应状态，并使授权者追踪代表的行动。与此同时，工具也应提供适当的辅助或替代参与方式，使缺少特定钱包、设备或技术能力的人不至于被程序性排除。治理的可达性应通过实际参与来检验。

代表、提案与监督因此构成连续的责任关系：相关主体能够表达问题，代表能够把问题带入有权程序，决定形成后又能够被追踪和质询。多方参与只有进入这条关系，才有机会改变组织如何理解问题、配置资源并承担后果。

三、表决权重、授权委托与决策门槛

表决把经过讨论的意见转化为能够识别的集体结果，但它的意义取决于谁有资格、每份意见具有多大权重，以及什么条件下结果可以成为有效决定。相同的赞成票数，放在不同的资格集合和门槛规则中，可能产生不同效果。制度必须先说明计算所表达的权力关系，再让程序执行计算。

按人配置权重，强调在特定共同体中的成员地位；按出资或某类权益配置权重，强调相应风险与权利关系；按代表类别配置席位或权重，则试图让不同关系进入共同决定。这些方式分别服务于不同判断，不能只用技术复杂程度比较优劣。组织应当解释某一事项为什么适用某种安排，并与既有权利结构衔接。

贡献记录也可以在有明确依据时参与某些资格或权重的确定，但贡献分数不宜直接成为全部事项的通用票数。不同贡献的计量边界、长期影响与不确定性，本来就需要分别处理。把它们合并成一种永久治理权重，可能让某个时期的评价结果长期控制与其无关的未来事项。

同时，需要防止资格计量中的循环授权。如果拥有较高权重的人可以独自决定贡献标准，又可以通过该标准增加自己的权重，权力就可能在程序表面合规的情况下持续集中。涉及资格和权重本身的改变，应设置相应的独立复核、受影响主体参与和生效边界，使现有优势不能毫无限制地改写未来参与条件。

多类主体共同参与时，可以考虑分类表决与总体表决相结合，或对特定事项增加受影响类别的同意条件。这样的安排有助于显露不同群体之间的分歧，但也会增加协调成本。分类范围应当与真实关系相联系，不能为了使某项提案通过，临时拆分或合并类别。

同一个人具有多重身份时，规则需要说明其参与方式。一个主体既可能是员工，也可能持有某项资本权益；两种关系确实可能分别支持相应权限，但不能因重复登记而在同一资格中重复计票。系统应当区分经制度认可的多重参与，与通过多个账户扩张同一份权力的行为。

授权委托可以降低参与成本，使缺少时间或专业能力的主体仍能通过受托者表达意见。委托的对象是特定权限的行使，不当然转移相关资产、收益请求或身份。能否转委托，是否限定议题，是否需要遵循明确指示，期限多长以及如何撤回，都应进入授权记录。

委托的生效时点尤其重要。对于已经固定资格与权重的表决，撤回或更换委托如何影响本次投票，需要事先说明；不能允许委托人与受托人对同一权重分别投票，也不能用“可以随时撤回”的界面承诺掩盖本次计票已经固定的事实。当前授权、历史投票与未来权限应分别表达。

受托者还应报告其实际立场与理由，并披露与议题有关的利益关系。大量分散主体把权重委托给少数代表，可能提高专业性，也可能形成新的控制中心。因此，需要观察有效权重集中于谁、授权者是否理解其选择，以及撤回和替换是否真正可行，而不只统计名义参与人数。

决策门槛至少涉及四个不同问题：事项是否在本机构权限范围内，参与程度是否达到要求，赞成意见是否满足通过条件，以及是否还需要特定类别或有权主体的同意。前一个问题没有解决，后面的票数不能自动补足权限；满足总体通过条件，也不等于已经满足全部附加条件。

决策条件	必须定义的口径	需要避免的混淆
事项权限	可决定的对象、范围及保留事项	多数赞成被当作无限授权
参与门槛	合格主体或权重总量、计入参与的行为	少量活跃账户被当作全体认可
通过门槛	赞成比例及其分母、弃权 and 无效票处理	不同口径下的百分比直接比较
附加同意	适用类别、触发条件与相应程序	总体结果覆盖特定权益保护

分母是门槛规则中不可省略的内容。以全部合格权重、实际参与权重或有效赞成与反对权重为分母，得到的通过条件不同。弃权是否计入参与门槛，利益冲突回避后怎样调整资格集合，空缺席位如何处理，都需要明确。没有参与也不能在没有依据时被记作赞成。

治理合约本身就体现了这种可配置性。OpenZeppelin 的 Governor 文档将投票权来源、参与门槛、计票方式及投票期间等作为需要选择的组成部分，并提供委托与延迟执行等机制。这些工具可以落实已选规则，但文档中的模块和参数并不为任何企业自动确定合适的治理制度。

OpenZeppelin 链上治理的权限与计票与执行配置 [2]

门槛的严格程度应与事项影响和可逆性相称。日常授权范围内的操作需要及时性，重大且难以恢复的权益变化则需要更充分的审议。提高门槛可以约束仓促决定，也可能使必要行动长期受阻；降低门槛可以提高决策速度，也可能使少量活跃主体控制结果。制度应同时说明未通过、平票和长期无法形成决定时怎样继续处理。

技术设计还应使资格与计票状态具有可核验的时间依据。通过适当的历史记录固定某次表决所使用的权重，可以减少同一单位在流转中重复取得计票效果的风险，但不能单独解决提前集中持有、利益交换或资格造假。限制某种技术操作之后，仍需判断实际控制关系是否符合制度目的。

表决结束与决定执行之间也可以保留适当间隔，用于检查执行内容、处理程序异议或完成必要准备。间隔只有与可用的质询、暂停或复核权限配合，才可能提供实际保护；若参与者只能看到即将发生的后果而无法采取任何有效行动，等待本身不能构成治理保障。

表决结果最终应说明采用哪份提案、哪一版规则、哪些资格数据和怎样的计票口径，并列出是否仍待其他程序完成。可复算能够提高程序透明度，决定是否妥当则还要结合证据、理由和利益影响评估。治理质量既需要计算准确，也需要集体判断能够得到解释和纠正。

四、少数利益保护与利益冲突处理

多数规则能够帮助组织形成行动，却不能独立保证每一种利益都受到适当对待。少数可能指票数较少的主体，也可能指长期缺少议程影响力、承担集中损失或难以退出的一类参与者。即使每次计票都准确，若某些群体持续只能接受他人决定，多方治理仍可能在实际运行中失去平衡。

少数利益保护首先需要界定共同决定的边界。组织可以在权限范围内选择发展方向和资源安排，但参与者已经依法或依有效约定取得的权利，是否以及如何调整，仍需依据相应规则判断。表决能够形成组织意见，不意味着多数可以仅凭票数取消任意主体的请求或豁免既有责任。

本书将保护安排理解为参与前、决定中和结果后的连续程序。参与前需要适当通知、相关信息和表达机会；决定中需要识别特别影响、处理回避并适用正确门槛；结果后需要提供理由、复核与必要救济。把保护只设置为最后的投诉入口，容易使少数主体在关键事实和程序已经固定后才被允许发声。

特别影响应当通过具体关系判断。如果某项决定使收益主要流向一类主体，而成本集中由另一类主体承担，就应解释这种安排的依据、替代方案以及受到影响者的参与情况。总体收益为正，并不自动回答负担分配是否合理；逐项说明收益与成本落在谁身上，能够使原本被总体数字遮蔽的问题进入治理。

对于会显著改变某类既有权益的事项，可以依制度设置分类同意、加强审查或限定范围的否决条件。保护措施需要与所保护的权益相对应，并说明触发、行使和复核程序。一般经营分歧与特定权利受损不能始终采用同一处理方式，否则少数保护可能被扩张为对全部组织行动的无条件阻断。

处理僵局时，也应遵守既定边界。补充证据、缩小方案范围、引入独立评估或开展调解，可以帮助寻找可接受方案；不能因为获得同意困难，就临时删除相应群体的表决资格。程序可以修订，但谁有权修订保护规则，本身就是需要受到约束的治理事项。

退出可以为某些主体提供选择，却不能替代全部保护。退出成本可能很高，关系可能无法立即转移，尚未履行的请求也可能继续存在。组织应把退出渠道与信息、参与和救济并列考虑，不能将“可以离开”作为回应所有不合理安排的理由。

利益冲突则要求区分共同利益上的不同立场与可能妨碍履职的特殊关系。员工代表关注工作条件、客户代表关注服务质量，本来就是多方治理需要表达的不同利益，不能因此一律要求他们回避。需要重点识别的是某个主体在履行受托或治理职责时，是否同时拥有会影响其独立判断的个人、关联方或其他特殊利益。

这种关系可能出现于交易审批、薪酬决定、服务商选择、资格确认和争议复核等事项。判断应关注受益、控制和依赖关系，而不只看是否使用同一个账户。同一控制者通过不同组织、地址或代理人参与，不会因为数字标识不同就自然形成独立性；必要核验应与隐私保护和信息访问权限相协调。

G20/OECD《公司治理原则》在董事会职责中强调识别与管理利益冲突、监督相关内部控制，并关注举报渠道的独立性与保密性。这些原则为本章提供了制度参照，但其具体适用对象和本书提出的多类主体治理安排仍需分别判断，不能将公司治理原则中的某一角色要求直接套用于全部参与者。OECD：董事会职责与利益冲突管理〔3〕

冲突处理应从及时披露开始，并进一步确定如何参与。有关主体可以提供必要事实和解释，但是否参与评价、表决或执行，需要结合冲突程度与有效规则决定。单纯公开关系并不当然消除影响；同样，存在关联也不自动证明方案不合理，仍需要对交易条件、替代方案和组织利益进行实际审查。

回避安排必须能够落实到计票与执行。谁判断需要回避，相关权重是否计入门槛分母，由谁接替必要职责，以及对判断有异议时怎样复核，都应提前说明。回避后没有足够合格主体作出决定，应进入相应的替代审查程序，不能由程序静默降低门槛或重新计入本应回避的权重。

监督者和复核者也需要接受同类检查。由被质疑决定的直接受益者控制全部证据、选择审查者并决定是否执行纠正，难以形成可信处理。组织应尽可能提供独立报告与复核路径，并记录审查者的任命、权限和相关关系。独立性应当表现为能够实际调查和提出不同结论，而不只是名称中出现“独立”二字。

表达异议的主体还需要避免因合理质询而遭受不当报复。对于举报、少数意见和受托代表履职，应建立适当保密、回应与保护安排，同时保留核验事实及处理恶意行为的程序。公开账本适合保存某些程序依据，并不意味着应公开所有举报者身份或个人争议明细。

自动执行增加了及时复核的重要性。制度若允许在明确条件下暂停有争议的操作，应同时限定暂停对象、期限与恢复程序。没有约束的暂停权同样可能被滥用。保护措施既要能够阻止不可挽回的损害，也要使行使保护权限的人说明依据并接受监督。

面向未来，本书提出一种需要检验的治理方向：让技术系统持续呈现权限的来源、代表关系、委托集中程度、事项影响与尚未解决的异议，使参与者能够检查权力在何处形成、怎样行使及如何受到纠正。评价这一方向，应观察受影响主体是否更容易进入程序、决定理由是否更充分、救济是否可达，以及治理成本是否与效果相称。更多投票记录，并不足以证明更多主体真正参与了决定。

从技术共识走向多方治理，意味着把共同可核验的记录进一步连接到有依据的权力与责任。协议维护账本秩序，治理安排共同事业的方向和边界，监督与救济则使决定持续接受检验。三者相互支持，才能让共同创造中的不同主体不仅被记录，也能够有关事务中被听见、获得回应并追索责任。

下一章将讨论制度的制定、执行与修订，进一步展开提案怎样经过审议成为有效规则，参数与版本怎样受到授权约束，以及自动执行、人工裁量和例外处置怎样共同维持组织的连续性。

定稿补强：代表生命周期与委托集中

利益相关者代表不是一个永久标签，而是一段可追责的授权关系。制度应说明代表如何产生、代表哪些群体和事项、任期与利益披露、协商和报告义务、投票说明、罢免、空缺补位及卸任后的资料交接。代表可以运用判断，但必须能解释其判断与授权范围的关系。

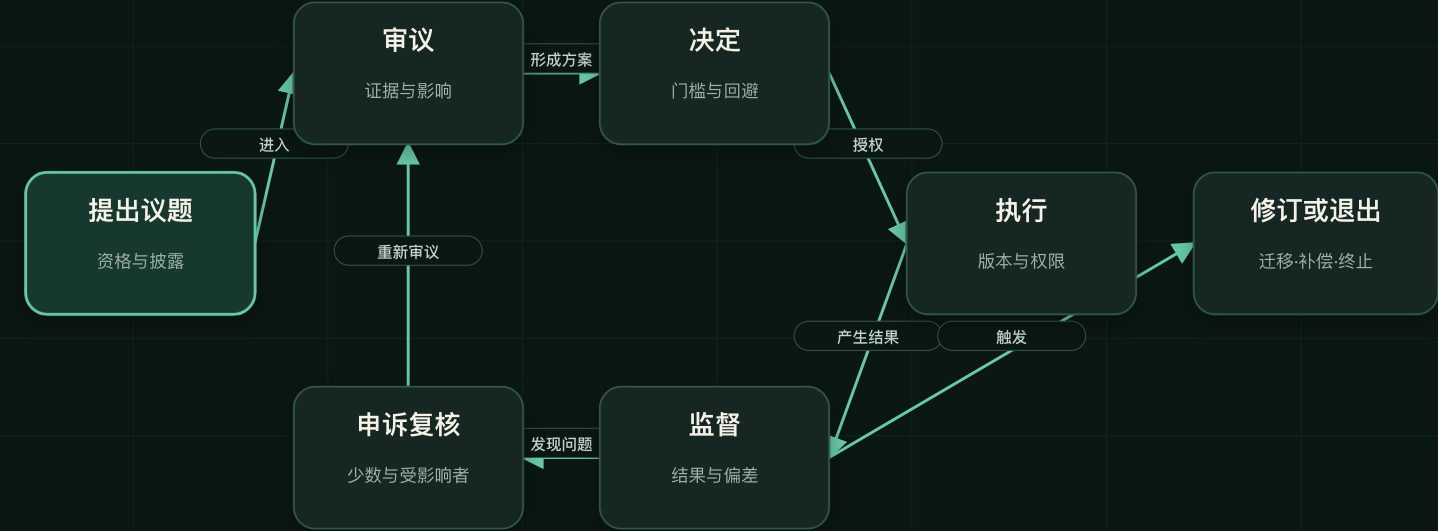
委托能够降低参与成本，也可能重新集中权力。系统应允许清晰撤回，规定是否可以再委托，并监测单一代理、关联方和投票联盟的集中度。委托上限、关联方合并计算、异常投票复核和法定人数防操纵，可以作为具体控制。界面应同时显示自有权重与受托权重，使参与者看见实际权力结构。

本章工具与图表

本章的制度关系可结合[附录八](#)、[附录十一](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

图21-1 多方治理的提案、监督、申诉与修订闭环

验证权与治理权分别配置；少数保护、回避和救济贯穿全过程



《区块链——利益相关者资本论的底层技术》V1.0 · 可编辑SVG

图21-1 多方治理的提案、监督、申诉与修订闭环

图21-1 多方治理的提案、监督、申诉与修订闭环。验证权与治理权分别配置；少数保护、回避和救济贯穿全过程

本章注释

- [SRC-044] Ethereum.org：协议治理与参与主体。[原文或官方页面](#)
 - 本章引证：Ethereum：协议治理与参与主体。
 - 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：以太坊治理说明、Ethereum：协议治理与参与主体、Ethereum：协议分歧与分叉。
 - 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-020] OpenZeppelin：链上治理的权限、计票与执行配置。[原文或官方页面](#)
 - 本章引证：OpenZeppelin：链上治理的权限、计票与执行配置。
 - 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：OpenZeppelin：链上治理的权限、计票与执行配置。
 - 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
 - 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-065] 经济合作与发展组织（OECD）：董事会职责与利益冲突管理。[原文或官方页面](#)
 - 本章引证：OECD：董事会职责与利益冲突管理。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：OECD：董事会职责与利益冲突管理。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：官方来源存在访问限制，已保留人工复核标记，核验日：2026-10-08。

第二十三章 制度的制定、执行与修订

共同创造需要稳定的规则，也需要在事实、能力与协作关系变化时修订规则。区块链可以使一部分规则以程序形式执行，使参与者核验决定与状态变化；它无法自行决定一项规则应当由谁提出、经什么程序获得承认，或何时可以改变已经形成的承诺。制度技术要发挥作用，必须把规则从形成到退出的全过程连接起来。

上一章区分了账本验证权与企业治理权，并讨论了代表、表决与利益保护。本章沿着这些权力关系继续追问：提案如何成为适用的规则，参数改变怎样取得权限，自动执行与人工判断怎样配合，出现根本分歧时组织如何继续承担责任。技术确认的对象是某个版本下的有效操作；制度需要解释这个版本为什么有效，以及它对谁有效。

本书把制度规则理解为包含主体、行为、权利义务、程序与责任的安排。规则可以写在章程、协议、专项制度或业务流程中，其中适合形式化的部分可以进入软件与智能合约。文件、程序和现实行为必须相互指向，才能让共同创造者知道自己应遵守什么、可以请求什么，以及遇到错误时由谁处理。

一、提案、审议、授权与规则形成

规则形成首先要有明确的问题。提案不应只写“优化分配”或“提高效率”，还应说明现行安排在哪些事实下不足、拟改变哪些关系、受影响者是谁，以及如果维持原状会发生什么。只有目标与问题清楚，参与者才能比较不同方案，事后也才能检验修订是否实现了原来承诺的效果。

提出问题与起草条款可以由不同主体完成。实际承担工作、提供资源、使用服务或监督执行的人，可能最早发现制度漏洞；具有起草能力的人则负责将问题转换为清楚的权利义务和操作条件。制度应为前者保留提出问题的渠道，同时要求后者说明取舍，避免起草权悄然变成独占议程的权力。

一项完整提案至少应说明适用对象、拟改变的规则、现实与技术执行方式、生效安排、资源和成本影响，以及对原有承诺的处理。若涉及计算方法，还需提供可复核的口径；若涉及身份或数据，还应说明核验与访问边界。条款正文和解释材料可以分开，但不能让关键限制只留在参与者难以发现的技术说明里。

审议需要兼顾可比较性与充分性。不同参与者应尽可能基于同一份文本讨论；提出实质修改时，应展示变化及其后果。对资源、代表资格或收益条件具有不同影响的方案，不宜只给出一个笼统的“赞成或反对”。审议可以通过书面意见、专业复核与正式会议展开，但意见的收集、回应和未采纳理由都要留下可以检查的联系。

多方参与并不要求所有人对所有事项拥有相同表决权。有关主体至少应能了解对其关系有重大影响的调整，在既定范围内表达意见，并在需要时使用异议或复核渠道。审议程序的要求应与事项重要性相称：日常技术修补不必重复制定基本规则的全部程序；改变参与边界、分配依据或责任承担，则不能用日常维护的程序快速通过。

程序中还需要识别利益冲突。提案发起者、负责测算的人与直接受益者可以参与说明事实，但是否有权作最终审查或计票，仍需依据有效安排判断。披露并处理这些关系，有助于提高理由的可信度；若只记录投票数而不记录明显的利益影响，形式上的多数可能掩盖问题。

规则获得授权，至少需要回答四件事：作出决定的机构是否有权处理该事项，参与和计票是否符合既定程序，决定内容是否越过已有权利与适用制度的边界，以及有无还必须取得的同意或批准。某一环节通过，不能代替其余环节。组织希望采用一项规则，与该规则已经对特定主体发生效力，也可能相隔多个步骤。

尤其应注意修订权限本身的来源。现有规则可以规定自己的修订程序，但持有一般事务决策权的人，不能仅凭一次普通决定降低基本权利的保驾护航门槛，再以新门槛处理同一议题。若保护条款需要改变，应依其当时有效的修订条件处理，并说明受影响主体的参与方式。这样才能避免通过先改程序、再改内容的顺序安排绕开原有约束。

规则形成可以用一条状态链描述：问题被提出，文本进入审议，有权主体作出决定，必要条件得到满足，规则在确定范围内生效，执行结果接受复核。各环节可能退回或终止，不应因为提案获得关注就把它展示为“已获批准”。账本可以保留文本摘要、决定记录与状态变化，但真实授权仍需要与身份、权限和程序证据核对。

以太坊的 EIP-1 将提案、审阅、最后征求意见和最终状态区分，并强调技术规范要说明动机、取舍及安全影响。它是协议改进提案的程序资料，可以启发本书对提案版本和审议记录的设计；企业中的制度效力仍应由其自身的授权关系和适用规则决定。EIP-1：提案目的与流程〔1〕

形成规则以后，应把规范性文本与解释、操作手册和程序代码建立对应关系。规范性文本说明应当怎样做，操作手册说明由谁按何步骤办理，代码执行其中可明确表达的条件。三者出现差异时，需要事先规定由谁发现、怎样暂停有风险的执行以及如何修正，不能简单让“运行中的代码”替代所有人的权利依据。

参与者还需要可达的规则入口。只公布一串摘要值或合约地址，无法使大多数人理解期限、资格和救济条件；只公布文字而不给出当前执行版本，也不能让人判断实际系统遵守什么。有效发布应指明完整文本、适用范围、生效时间、执行版本与负责解释的主体，重大变化还应有适当通知。

形成规则不是结束治理。组织应保存当初的目的、重要反对意见与预期影响，安排实施后的复核节点。如果某项新规则没有改善它要处理的问题，或者让新的负担集中于未充分参与的主体，后续修订就有了可讨论的证据，而不必把早期决定视作无法质疑的终局。

二、参数权限、版本管理与生效程序

制度中的可变内容并不具有相同性质。结算周期、信息通知期限、贡献评价权重、可分配资源口径、表决门槛和紧急暂停条件，可能都被写成系统参数，但它们改变的权利关系不同。参数是否容易在界面上修改，不应决定它需要哪一级授权；真正重要的是修改后谁的行动空间、权益或风险发生变化。

本书建议按作用范围区分参数。纯粹的显示或性能设置，可以在明确运维职责内调整；影响个别业务流程但不改变基本权利的设置，需要业务负责人与必要复核；涉及资格、计量、分配和决策权重的设置，应进入相应制度审议；改变基本原则或保护机制的事项，则需适用更严格的修订程序。这是分析框架，不是替任何组织预设具体机构和门槛。

每项参数应有可识别的名称、含义、单位、适用范围、允许的取值、责任主体及变更方法。孤立地记录“权重从二变成三”，不足以解释它是比例、评分系数还是表决权重，也无法说明影响哪些期间。参数登记应指向其上位规则，使执行人员和参与者可以知道某个数值究竟在实现哪项制度决定。

关键在于权力不能自我扩张。能调整分配比例的人，不应仅凭该权限改变“哪些主体有资格分配”；能延后执行时间的人，也不应因此获得取消已经成立请求的权力。对于新增参数、扩大取值范围或改变参数解释，应判断是否构成规则修订，而不是一概交由原参数管理员处理。

组织制度版本、计算规则版本与程序代码版本应分别编号并保持映射。一次代码修复可能不改变既定权利；一次制度修订也可能需要多个系统协同更新。版本关系应说明采用哪份制度文本、哪组参数、哪份执行程序以及哪个数据口径。若它们不同步，不能只用“最新版本”四个字掩盖差异。

版本或状态	主要回答的问题	应保留的连接
制度文本版本	哪一项权利义务和程序获得了授权	决定主体、适用对象、生效条件
参数集合版本	哪些可变规则取何数值	上位依据、变更权限、适用期间
程序执行版本	哪段系统逻辑实际处理操作	测试、部署、核验与回退记录
业务数据口径	哪批事实和资格进入计算	来源、截止时点、复核及更正记录

生效应当与批准、公布和部署分别记录。制度可能已经获批但仍待通知或约定条件；程序可能已部署，却尚未被授权用于正式分配；旧程序也可能在过渡期继续处理旧期间的请求。系统界面若只有“在线/离线”状态，就难以表达这些关系。需要明确哪个版本在何时、对哪些人和哪些事项开始适用。

时间规则应尤其注意跨期承诺。对新加入主体适用的新条件，与调整已经完成贡献、已经形成资格或已经成立的支付请求，属于不同效果。制度应说明旧规则下的事项如何结算，哪些环节进入新规则，必要时设置并行处理和过渡期限。不能通过回填生效日期，使新规则看起来从过去就一直存在。

版本并行需要确定一个归属规则。同一主体在一段过渡期内可能同时拥有旧期间形成的请求和新期间适用的资格，系统必须按请求来源和生效范围分别计算，而不能只根据当前账户显示的版本处理全部余额。对于尚未完成任务，也需要说明采用开始时、完成时还是其他有依据的规则；其选择影响各方预期，应在改变发生前说清。

公开计划也未必等于已对每个主体成立的安排；但一旦组织已依据有效程序作出承诺，就需要判断修订是否触及该承诺。不能把“规则可以升级”解释为管理者永远有权单方重写一切。既有权利是否可变、由谁同意和如何补偿，应回到具体权利依据与适用法律制度。

有些变更可以通过延迟执行提供检视时间。OpenZeppelin 对 TimelockController 的说明表明，特定管理操作可以经过预设等待期再执行，并区分提案与执行角色。等待期提供发现问题和采取行动的机会，但是否适用、等待多久以及如何处理中止，仍是组织需要决定的制度问题。

OpenZeppelin: 延迟执行控制 [2]

参数变更还需要检查执行前的条件。应验证有权决定是否已经完成、拟部署版本是否与审议文本一致、相关业务系统能否使用新口径、数据是否可以读取，以及重要的未了事项如何处理。代码通过技术测试，不能证明其业务结果符合授权；只通过一次投票，也不能证明代码准确实现了决定。

生效后需要持续对照实际运行。发布记录应让参与者查到当前版本和历史版本、变更理由、影响范围以及相关过渡安排；内部则要核对真实程序与已公布安排是否一致。发现配置错误时，纠正应保留原状态与处理依据，不能悄然覆盖历史。版本管理最终服务于权利可解释，而不仅是工程管理。

三、自动执行、人工审批与例外裁决

规则能够自动执行，通常意味着条件、输入、权限和结果已经形式化。资格在指定时点符合要求、金额按固定口径计算、审批签名齐备或某项资源在范围内转移，都可以设计为由系统直接处理。这样做能够减少重复核算和选择性执行，却只能覆盖规则已经准确表达的部分。

自动执行首先需要可靠的输入。业务事实、服务质量、损失归因和对现实资产的控制，不会因为进入共享账本就自然变真。系统可以核验输入来自被授权的主体、格式是否正确以及是否与已有记录冲突；事实判断仍需要证据、责任和可质疑的程序支撑。

本书将执行路径分为三类。第一类是条件清楚、风险可控的事项，由程序自动执行并保留结果；第二类需要人确认事实或授权，系统在取得有效审批后继续执行；第三类涉及例外和冲突，由有权主体作出理由明确的裁决，再让系统落实可执行的部分。这种分类取决于事项性质，而不是技术是否能够写出一个判断条件。

自动执行应受适用范围约束。分配程序能够为某类已确认资格计算份额，并不表示它可以处理没有证据支持的特殊贡献；支付程序能够按有效清单划转资源，也不表示它可以自行决定资源不足时的权利顺序。对未知情况，系统应清楚地返回“待核验”或“需裁决”，不能靠默认值制造已经通过审查的外观。

人工审批也不是任意决定的许可。审批人应有明示权限、必要资料和说明理由的责任。涉及多个职责时，需要区分事实确认、资源授权与支付操作，不能让一个人通过连续点击同时产生证据、批准方案和完成支出。多人签署可以降低单点控制风险，但只有在签署者确实履行不同职责时，才形成制度上的相互约束。

审批的证据应能够被追溯。何人以什么身份、依据哪份规则、核验了什么材料、批准了哪个范围和额度，决定了日后能否复查。系统可以核验签名和时间，却不能从签名本身推断审批人已经看过材料。对重大事项，制度可以要求材料摘要、审查结论与必要的独立复核相互对应。

在链下审批、链上执行的安排中，还需要避免批准对象与执行对象脱节。审批材料所指的收款主体、金额、资源用途或截止时间，应该与实际发起的操作建立可核验联系。若执行前相关事实发生实质变化，应回到原权限范围判断批准是否仍然适用，而不能把一份旧批准当作任何后续操作的通行凭证。

例外裁决处理的是一般规则无法充分覆盖的情形，例如身份被冒用、证据矛盾、服务中断、紧急风险或两项既有承诺冲突。例外程序的目的，是在特定事实下给出可以说明的处理，而不是让管理者绕开平常规则。启动条件、受理主体、可采取措施、期限和事后复核，应在例外发生之前确定基本边界。

例外记录至少应说明触发事实、受影响者、临时措施、裁决理由、所依据的权限和后续救济。需要迅速处置时，可以先采取范围受限的止损行动，再在限定时间内补充复核；若事后未获得有效确认，应明确怎样恢复和补偿。紧急措施可以暂时改变操作状态，但不能自行改写事实，也不应自动成为永久的新规则。

自动化与人工裁量之间需要一条可见的回路。人工确认产生可核验的输入，系统执行有范围的结果，异常再次返回有权程序。只有在这个回路里，参与者才能知道是算法计算了一个已定金额，还是有人判断某种事实成立。混淆两者，会使错误既难归于代码，也难归于作出判断的人。

执行情形	适合的处理方式	核验重点
明确且重复的条件	自动核验与执行	输入来源、规则版本、结果一致性
需要事实或资源确认	有权审批后执行	审批权限、证据范围、职责分离
出现冲突或特殊调整	例外裁决并记录	启动依据、比例适当、理由与复核

执行情形	适合的处理方式	核验重点
无法确定适用条件	暂停相关操作并补充事实	保全状态、通知、责任与处理期限

若例外不断重复，就说明一般规则可能已不适用。组织应分析例外的类型、成本和对不同主体的影响，再决定是否进入修订程序。不能通过一连串个别裁决，实际上建立一套没有公开审议的新规则；也不能为了减少例外数量，强迫不同事实进入同一个失真的自动判断。

参与者所见的界面，应如实显示事项所处的执行阶段。申请已提交、证据已确认、人工审批已通过、链上操作成功和现实履行完成，各自含义不同。能够看见责任主体和下一步处理，往往比只看一个“完成”标记更有助于建立可持续信任。

四、分歧、分叉与组织连续性的维护

制度会遇到分歧。参与者可能不同意目标、权重、资源配置或对旧承诺的解释；技术参与者也可能对协议升级和安全措施有不同判断。分歧不是账本核验失败的同义词。一个共同承认的历史记录，可以同时成为不同制度主张所引用的事实基础。

处理分歧应先判断争议对象。若是事实或计算错误，应通过证据和复核纠正；若是现行条款含义不清，应通过有权限的解释程序处理；若是未来制度方向不同，则应让各方依据既有提案和修订机制表达立场。将所有分歧都称为“技术问题”，会使真正需要协商的权利变化失去讨论空间。

对重要争议，应保留原问题、不同意见、所依据的证据和形成决定的理由。系统可以记录提交与回应，但若没有让持不同意见者得到公平表达的程序，公开记录也可能只放大已有权力差距。对仍能继续履行的无争议事项，组织应尽量维持处理，使局部分歧不至于使所有参与者的日常合作停摆。

分叉有多种含义。网络协议可能因各方采用不同规则而形成不同链；应用可以迁移到新合约或新账本；组织也可能因目标与权益安排分歧而分立。这些变化的对象、控制者和后果不同。技术上复制数据或启动另一套系统，不会自动复制现实资源、合同、品牌、人员义务或对外承诺。

以太坊的治理资料说明，当重大协议变化无法取得共同接受时，技术网络可能形成不同版本。这个事实帮助我们理解分叉作为一种技术与社会协调结果，但企业或多方组织的分立，还必须另行解决资产、权利与责任的归属。Ethereum：协议分歧与分叉〔3〕

因此，组织在迁移或分立前应建立事项清单：哪些资源由谁控制，哪些权益与支付请求已经形成，哪些服务仍须继续提供，哪些数据可以转移，以及各方怎样获知并选择。尤其要确认对尚未作出选择的参与者负有什么义务。一个新系统把历史余额复制过去，并不意味着原系统中的请求已经履行或消失。

历史事实也需要保持可核验。迁移时可以将旧记录的证据链和必要状态映射到新系统，但应说明映射原则、未完成事项与异常处理。复制两份记录可能用于连续审计，不能让同一项资源或义务在两个系统中被无依据地重复兑现。技术兼容与经济清偿，应分别核对。

维持组织连续性不等于要求所有主体永远采用同一个技术平台。关键是角色和责任能否在更换系统时延续：谁承担未付请求，谁有权确认新系统，谁能恢复必要服务，谁负责保存和开放历史证据。系统迁移应服务于这些已有关系，不能把技术停机解释为制度关系已经终止。

对于重大升级，本书主张事先准备有限的连续性安排。它应包括触发条件、临时负责者、可动用的资源范围、最长处理期限、通知方式、原有决定的延续性，以及事后审查和交还权限的办法。安排越容易在紧急状态下启动，越需要防止临时权力因缺少退出条件而固化。

连续性还取决于外部关系。支付服务、数据保管者、合作组织和实际资产管理者，可能并不会因为内部系统完成迁移就同步接受新安排。组织应核对通知、授权更新和服务交接的实际结果，并为暂不能迁移的事项保留可履行路径。由此可以看出，技术部署只是迁移中的一个环节，组织是否继续有效履约，需要在各类关系中分别确认。

共同规则失去广泛认可时，可以通过补充协商、限定范围的试行、独立评估或依有效程序作出修改，争取恢复合作基础。无法继续共同运行时，也应尽量有序处理分离和退出。维护连续性既包括让愿意继续合作的人可以协作，也包括让不愿继续的人能按适用安排结清关系，而不是被迫接受未获授权的新条件。

本书进一步提出一个有待检验的研究方向：将制度的提案、授权、生效、执行、异议、修订与退出构造成相互引用的公开责任链，让参与者不仅看到当前数值，还能追问“是谁、根据什么、对谁改变了什么”。这种安排是否改善治理，需要观察规则误用是否减少、变更是否更容易被理解、例外能否及时纠正以及弱势参与者的救济是否真正可用。记录更完整只是检验的起点。

制度技术的成熟，不表现为所有判断都被永久写死，也不表现为任何变化都可以由少数人即时推送。它表现为稳定承诺与必要修订之间有清楚的程序，执行能够服从有效授权，异常能够回到负责的人，分歧出现时组织仍能面对历史和现实义务。这样的制度才可能让共同创造在变化中保持合作。

下一章将继续讨论审计、纠错与责任追溯，具体检验从业务证据到权益结果的链条，以及当数据、代码或操作发生错误时，如何标注、修正、补偿并说明责任。

定稿补强：规则层级与紧急权力期限

制度规则应至少分为四层。基本规则保护主体资格、基本权利、代表结构和修订权限；政策规则决定资源与行为的一般安排；参数规则在授权范围内调整数值；操作指令处理日常执行。每一层分别规定提出者、审议门槛、冷静期、生效方式和复核渠道。参数权限不得被用于绕过基本规则。

紧急权力只能在明确证据和有限范围内启用。启动记录应写明事件、权限、受影响对象、替代方案和最长期限；到期自动失效，续期需要更高门槛。事后必须完成独立记录、治理追认、损失与补偿审查、恢复验证和临时权限撤销。紧急状态不能成为长期改变权利结构的便捷通道。

本章注释

1. [SRC-023] Ethereum Improvement Proposals: EIP-1: 提案目的与流程。[原文或官方页面](#)

- 本章引证：EIP-1: 提案目的与流程。
- 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：EIP-1: 提案目的与流程。
- 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
- 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-018] OpenZeppelin: 延迟执行控制。[原文或官方页面](#)

- 本章引证：OpenZeppelin: 延迟执行控制。
- 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：OpenZeppelin: 延迟执行控制。
- 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
- 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。

3. [SRC-044] Ethereum.org: 协议治理与参与主体。[原文或官方页面](#)

- 本章引证：Ethereum: 协议分歧与分叉。
- 支持范围：用于说明特定协议或项目在当前文档中的运行机制与工程约束，本书引用主题包括：以太坊治理说明、Ethereum: 协议治理与参与主体、Ethereum: 协议分歧与分叉。
- 使用边界：项目文档描述特定系统，版本、参数与实现可能变化，不能直接外推为所有区块链的一般性质。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第二十三章 审计、纠错与责任追溯

共同创造进入制度系统后，每一项权益结果都应能够回答三个问题：它根据什么事实形成，依据哪一版有效规则计算，由谁作出必要确认并承担后续履行责任。共享账本可以保存部分答案，却不能单独保证答案正确。事实可能被误报，计算可能采用错误版本，签名也可能出自无权操作的人。制度的可信度，取决于这些问题被发现后能否说明、纠正并落实责任。

上一章讨论了制度从提案、授权到执行和修订的过程。本章把视线移到执行结果：组织怎样追溯从业务证据到权益凭证的每一步，怎样在保留历史的同时处理错误，以及当合约或人员操作导致损害时，怎样划分责任、暂停风险并恢复正常治理。

审计并非事后给账本盖章。它从事前的证据设计开始，在运行中核对规则与操作，出现争议时重建事实，最后检验纠正是否真正到达受影响者。能够留下痕迹，是审计的条件；能够解释痕迹的意义，才是制度审计的任务。

一、从业务证据到权益结果的审计链

利益相关者资本治理中的审计对象，是一条从共同创造活动到权益安排的可追溯关系。承诺与任务规定参与边界，投入和交付形成业务事实，验证和复核决定哪些贡献得到确认，计量与资本判断决定它们能否进入后续安排，授权规则再决定是否生成具体权益，最后由履行记录说明请求获得了什么结果。任一环节缺少依据，终端凭证都不能替上游环节补证。

审计链首先需要稳定的对象标识。任务、交付、证据、确认、评价、权益决定、支付请求与执行操作，应当能够彼此引用；同一任务有多项交付，同一项贡献影响多个结果，也要保留一对多或多对多的关系。若系统只展示参与者的最终分数，审查者就很难查明数字来自哪些事件，更无法区分重复记录与真实的共同贡献。

证据的来源、形成时间、保管者和证明范围，应在进入审计链时说明。一份签收记录可能证明某项材料已交付，未必证明质量合格；一项使用数据可能显示有人使用成果，未必证明使用的经济价值完全由单个贡献者创造。审计应检查证据被用来支持的具体判断，不能把“有证据”当作对全部结论的通用认可。

业务事实还需要独立于系统录入状态。记录被接受，说明它符合当时的输入和确认程序；如果原始资料错误、核验人失职或相关主体串谋，系统可能一致地接受错误结论。美国国家标准与技术研究院将区块链描述为具有篡改可见性与抗篡改性的共享账本，其说明针对记录的改变难度，并不能推导出链下输入天然真实。NIST：区块链技术概述〔1〕

因此，审计至少需要分别检查记录完整性、事实可靠性和制度适用性。完整性关注记录是否被替换、遗漏或重复；可靠性关注输入是否有独立来源和必要交叉核验；适用性关注采用的规则是否有效、确认者是否有权，以及计算范围是否正确。三类检查相互支持，但不能互相代替。

涉及贡献计量时，还应能重建计算。采用哪一版权重、哪个期间、哪些已确认事件，是否存在合格上限或时间调整，都需要可核对。最终分数相同的两个人，可能经历了完全不同的证据质量和裁量程序；审计不能仅以结果相同判定过程一致。

资本形成更需保留独立判断。贡献被确认，不代表它已成为跨期使用的资源或能力；被记录为资本来源，也不代表贡献者自动取得所有权。审查者应检查资源是否确被组织吸收、能否持续作用、相关风险由谁承担，以及任何权益是否另有授权依据。这些判断应分别留有责任主体与支持材料，避免用一张凭证覆盖全部经济和制度意义。

权益审计则从结果反向追问：谁是权利主体，谁承担相应义务，权益覆盖什么对象，何时成立，是否附带条件，以及转移或终止依照哪份安排。持有账户的控制者、实际受益者和代理操作人可能不同。若只审计通证余额，便无法判明一项收益请求是否已经成立或由谁实际兑现。

对于收益分配，审计还要连接资源来源、资格名单、计算规则、支付清单与真实支付。已发放单位、已登记应付、已提交转账和已完成履行，是不同状态。即使总额相符，也要核查个体层面的漏付、重复支付、错误地址与退回款项，才能判断制度承诺是否落到具体参与者身上。

审计环节	关键依据	容易误认的结果
业务与贡献	承诺、交付、来源及确认记录	已录入即等于事实真实
计量与资本	规则版本、计算输入、持续使用与风险依据	分数即等于资本或企业价值
权益形成	授权决定、主体、义务、条件和生效记录	持有凭证即拥有全部权利
分配履行	资源来源、资格、金额、支付及对账证据	标记已分配即已经收到回报

审计链需要分层开放。受影响者应能核验自己的依据与结果，具有授权的审查者需要足以复核总体关系的材料，公众或其他协作方则可在适当范围内看到汇总和必要证明。不是把所有合同、身份与账户明细都放到公开链上，才能实现可核验。重要的是证明与原始材料能以受控方式对应，且有人负责保存和提供。

审计结果还应标出不确定性。资料暂缺、来源相互冲突、规则解释有争议和已经确认错误，是不同状态。审查者应说明已完成哪些核验、哪些范围未被覆盖，以及结论依赖什么条件。审计不能让一枚“通过”标记掩盖尚未核查的重要链下事实。

一条有效的审计链，允许审查者从一个权益结果向上查到其事实和授权，也允许从某项被推翻的证据向下找出受影响的全部计算与支付。前者解释制度为何作出结果，后者决定纠错能否完整展开。制度技术提供连接和留痕，审计则赋予连接以可复核的判断。

二、错误数据的标注、冲正与补偿

错误不只有一种。原始事实可能不准确，证据可能属于错误主体，评价可能重复计入，参数可能取错版本，账户可能映射失误，支付也可能转至错误路径。修正前应先确定错误位于哪一环节、影响哪些下游结果。若只改终端余额，上游仍保持错误，下次计算就可能再次产生同样的偏差。

发现疑似错误时，应先保全现有记录和相关证据，再标注其争议状态。标注不是立即认定参与者有过错，而是告知后续使用者该项资料需要核验。对于可能继续触发分配的记录，可以在有效权限内限制相关操作，并说明限制范围、起始时间和复核责任。无关权益不应因局部疑点被一并冻结。

确认错误需要受影响者有机会了解问题并提供材料。自报、他人举报、系统检测和独立审查都可能启动核验，但启动方式不能替代最终证明。若错误由组织自身录入或程序造成，也应如实记录，而不能默认由领取者承担全部证明与损失。调查中应区分事实争议、规则解释争议与已发生的执行差错。

链上记录难以按传统数据库方式无痕改写，纠错应保留原记录并添加有依据的更正联系。冲正适合表达某项先前计入结果在后续核算中被撤回或抵消，但需要同时指向原记录、原因、批准者与影响范围。保留历史不是持续展示一个明知错误的当前余额；当前有效结果应能清楚反映更正后的状态。

冲正也有层次。更正贡献事实与重算评价、调整资本记录、修改权益账户和追认支付结果，分别属于不同环节。上游事实改变后，应沿审计链检查下游是否确实依赖它；有些权益已经独立成立，未必随某次评价修正自动消灭。是否能够撤销或调整已成立请求，要看其有效依据、适用规则和必要的处理程序。

若错误涉及多个期间，应保留跨期影响。旧期间的记录可加更正说明，新期间的核算则纳入经确认的调整；任何回填处理都应让人分辨当时实际采用了什么结果、后来为何改变。不能把新规则伪装成旧规则，也不能用重算结果覆盖已经完成的支付事实。

已经执行的错误支付，需要分别处理多付、少付和未能交付。少付部分应确认责任和补付路径；多付部分若需追索或在未来抵扣，必须检查其权利依据、受领者状态和适用程序；支付指令虽已提交但未到达约定对象，也不应被视为已经足额履行。技术上可以增减余额，不等于经济结果已经恢复。

补偿更进一步，关注错误造成的实际影响。被延迟的款项、无法使用的服务机会、因错误停权而错过的治理参与，以及不当披露造成的损害，可能需要不同处理。组织应当先查明可恢复的原状态，再依据有效规则 and 具体事实判断是否需要额外补救；不能把一次补发通证当成所有损害的通用结案方式。

处理阶段	应说明的事项	对外呈现的状态
标注与保全	疑点、发现时间、暂时限制及证据范围	待核验，不预断责任
确认与冲正	原记录、错误事实、授权和受影响结果	已更正，保留历史关联
补付或返还	请求依据、金额或对象、履行进度	已处理部分与未处理部分分列
补偿与复核	剩余损害、补救依据及申诉结果	是否真正结案可被复查

部分纠错可以自动化，例如识别重复编号或在确认新的输入后按同一版本重新计算。但涉及事实取舍、既有权利调整与责任争议时，仍需要有权主体给出理由。自动更正应能说明其触发依据、允许范围和影响对象，必要时提供暂停与申诉途径。

纠错之后还要检查再发生风险。同类错误是否来自身份核验薄弱、审查流程过于集中、参数含义不清，或系统没有处理退款和跨期变更的能力？如果根因仍在，只为当前受影响者补齐差额，制度仍会继续生产新的错误。复核应同时提出程序或技术修正，并说明何时检验其效果。

透明纠错不是让个人错误永久暴露于所有人面前。审计者可以保留必要证据及修订历史，参与者获得与自身相关的说明，对外披露则限定在监督所需范围。记录可追溯与个人信息适当保护，可以通过权限、摘要和受控查询共同实现。

三、合约缺陷、越权操作与责任划分

智能合约可以按照预设条件执行，但同一个错误结果可能来自不同原因。制度文本本身有缺陷，程序错误实现了正确规则，外部输入不真实，操作人超越了授权，或者有效操作与其他系统的记录未能衔接，都可能在链上表现为一个“成功”的状态变化。责任追溯应从原因与职责出发，不能仅看交易由哪个地址发起。

先要区分规则设计与技术实现。若有效规则要求两名独立审批者确认，而程序只检查一个签名，问题主要出在执行条件未准确实现；若程序忠实执行了经批准却明显遗漏受影响群体的规则，技术团队并不能单独解释整个制度选择。两类问题都可能需要及时止损，但责任审查的对象和修订程序不同。

程序缺陷还须进一步确认影响范围。代码中存在一条潜在错误路径，与该错误已经被触发并造成资源损失，不是一回事。审查者需要核对部署版本、可调用权限、触发输入、链上操作、实际资金或权益变化，以及同一逻辑在其他期间是否被使用。技术调查应保存可重现条件，不应靠“合约存在漏洞”的笼统结论代替损害核算。

越权操作关注行为人与授权的关系。某个账户在程序中拥有管理员角色，只能证明它在当时具有相应技术权限；该角色是如何授予、操作者是否受组织委托、此次行动是否落在委托范围内，仍需分别查证。OpenZeppelin 的访问控制文档说明了按角色授予、撤销和检查权限的机制，它有助于限制可执行动作，但不能自行证明每一次角色使用均符合组织制度。OpenZeppelin：访问控制与角色权限〔2〕

多方签署也需要实际核验。多个地址背后可能是同一控制者，签署者也可能在不明白内容时一起签名。因此应审查签署者身份与独立性、请求内容是否清楚、签署前能否看到所需证据，以及异常操作是谁发起和谁审核的。技术门槛可以减少单点风险，制度上的职责分离还需要组织条件支持。

链下输入责任则应落实到提供与确认事实的主体。数据提供者可能只保证资料来自指定系统，业务核验者则负责核查服务确已发生，审批者还需判断该事实是否满足权益条件。把这些职责合并成一个“预言机负责”标签，会使各方在错误发生后互相推卸。每个输入接口都应标明证明范围和负责核验的环节。

责任可以通过一张关系图重建：谁制定规则，谁开发与测试，谁批准部署，谁持有密钥并执行，谁提供事实数据，谁监督异常，谁负有对参与者的履行义务。不同主体可以兼任多个角色，但角色合并不能消除各项职责。相反，若一个人同时控制输入、批准与支付，更需要说明如何避免自我证明和自我监督。

问题来源	先核验的对象	主要责任问题
规则或授权缺陷	决定文本、参与程序、生效边界	谁有权作出并修订该安排
程序实现缺陷	需求、代码、测试与部署版本	谁负责实现、审核和放行
事实输入错误	原始材料、来源、复核与接口	谁负责提供和确认事实
越权或失当操作	身份、密钥、授权范围与具体行为	谁有操作能力，是否得到制度授权
后续处置不当	异常发现、通知、暂停和补救记录	谁有能力减轻损害而未采取行动

责任分析应避免两种简单化：把全部后果归于“代码不会犯错”，或将一切技术故障自动归于开发者个人。实际义务可能来自合同、组织规则、职责安排及适用法律，需要结合具体事实确定。技术层面的缺陷定位有助于说明因果，但赔偿、补救和纪律处理仍须经过有权程序。

在调查中应保全程序版本、参数、相关交易、系统日志、审批材料、密钥权限变更与受影响者的通知记录。保全也要注意接触权限和资料完整性；调查人员不能为了取证而继续扩大风险，不能让被调查者单独控制唯一证据。必要的独立复核能够提高结论可信度，但其权限、范围和与当事者的关系同样应接受说明。

出现实际损害时，先行补救与最终责任认定可以分别推进。组织对参与者已承担的履行责任，不应仅因还未确定哪个承包方写错代码而长期悬置；各责任方之间如何分担费用，可以在证据完整后处理。若补救需要动用共同资源，则仍需说明授权、金额、受益对象与事后追偿安排。

责任还包含预防义务。设计者应说明可预见的失效情形，维护者应监测重要异常，具有暂停权限者应按既定触发条件行动，治理机构应及时处理持续出现的问题。并非每一次意外结果都意味着有人应被归责，但长期忽视已经可见的风险，会改变对其行为的评价。

因此，追溯的终点不只是找出一个“背锅者”，而是让受影响者获得事实解释和有效补救，让制度知道需要修改哪一层安排，并让有权主体对自己的决定承担可检查的后果。代码、密钥、账本和组织职责共同构成责任链，缺一环都可能使问责流于形式。

四、紧急暂停、恢复与治理接管

当错误正在扩大、资金持续流失或资格系统出现系统性误判时，组织需要能够及时阻止进一步损害。紧急暂停是为核验和补救争取时间的临时措施，不是对异常事实或最终责任的裁决，也不是持有暂停密钥者取得长期治理权的方式。

暂停前应界定触发条件与受影响范围。某个自动分配模块发生异常，不意味着所有查询、历史证据和无关业务都必须停止；一项外部数据源不可信，也不必然要求锁住全部已经独立成立的支付请求。暂停的颗粒度应与风险相称，同时考虑过窄的暂停是否会留下继续损害的路径。

第十一章已经说明，暂停模块只有被实际接入的功能才会受暂停状态约束。本章不再讨论实现方式，而把暂停视为事故处置权限：是否配置、覆盖哪些操作、由谁启动、怎样通知和恢复，都必须能够进入审计。

暂停权限可由特定职责主体掌握，并配以多人确认、事后批准或其他约束。紧急情况可能无法等待完整的常规表决，因此制度可以授予范围受限的先行处置权；同时应规定可核验的触发事实、即时记录、通知义务、最长持续时间和续期程序。不能让“紧急”成为没有结束日期的常态治理模式。

启动暂停时，应立即固定当时的状态：正在执行的任务、已提交但结果未明的交易、尚未支付的请求、相关钱包和密钥权限，以及链下服务是否继续运行。技术层面的暂停可能不覆盖外部系统，支付机构或业务部门也可能仍在处理旧指令。应建立跨系统核对责任，避免一边暂停、一边继续产生同类结果。

通知应说明已知事实、尚不确定之处、受影响的功能、可继续办理的事项，以及参与者如何提交证据或取得帮助。及时通知不等于提前宣告全部原因；为避免误导，可以公开事实状态和下一次更新时间。让参与者知道自己的请求是保留、延迟还是需要补充材料，比只显示“系统维护中”更有制度意义。

暂停期间的审查，既要查原因，也要查暂停本身的影响。停止某项转移可能保护资源，却也可能阻碍参与者履行已到期义务或退出某种关系。组织需要识别这些次生影响，必要时安排受控的替代履行或局部恢复，并说明为什么它不会重新打开原风险。

恢复不宜只依据“合约补丁已部署”。还要验证错误输入是否已清理，受影响记录如何纠正，资源是否足以履行原有请求，新版本是否经过授权和检验，操作权限是否重新配置，以及链下系统是否同步。恢复范围可以分阶段扩大，但每一步应说明检查通过了什么、仍由谁承担监测责任。

若原管理者失去操作能力、涉嫌严重越权，或长期不履行处置责任，治理接管才可能成为必要安排。接管应基于事先明确的权限或有效的有权决定，说明启动证据、移交对象、临时管理范围、监督者和退出条件。更换密钥控制者可以改变系统操作能力，却不能凭技术动作直接转移企业资产、合同地位或既有权利义务。

接管还需要双向核验：确认旧权限已经适当撤销或限制，也确认新责任主体确实有能力维护服务、保存证据和处理未了请求。若部分系统由合作方托管，应取得相应交接与确认。没有清楚的移交清单，接管可能在界面上完成，却让数据、资金和责任落在无人负责的缝隙里。

当严重分歧使正常治理机构无法有效决定时，接管程序尤其需要防止自己成为新的争议来源。临时权力应有明确目标和期限，只处理必要的安全与连续性事务；涉及永久改变权益结构的决定，应在恢复有效治理后按相应程序处理。接管者的行动、费用和与受影响者的关系，也应接受独立审查。

暂停与接管期间，原始历史和已有请求仍需保留。系统停止自动执行，不等于承诺消失；计算被暂停，也不意味着贡献事实被撤销。到期义务可能因故暂时无法履行，但状态、原因、负责主体和补救安排应持续可查。维持制度连续性，需要让参与者在困难时仍能知道自己的位置。

本书提出一个有待检验的方向：将事故处置设计为能够逐步证明的责任过程。发现异常、限定风险、保全证据、确定影响、作出更正、完成补偿和授权恢复，各阶段都留下可以复核的条件。评价这种制度，不看暂停开关有多快，而看实际损失能否被及时限制、受影响者能否获得说明和补救、恢复后同类错误是否减少。

审计、纠错与责任追溯共同揭示了制度技术的一条边界：技术能让许多动作留下可靠痕迹，却不能替组织免除辨认事实、解释规则和承担后果的责任。良好的制度让记录可以追问、错误可以纠正、权力可以监督，使共同创造者在系统出错时仍有途径维护自己的合法权益和继续合作的基础。

下一章将把视角扩展到跨组织协作与生态治理。共同事业可能连接多个企业和平台，贡献、结算与争议跨越不同制度边界；审计与责任链能否延伸到这些边界之外，将成为新的检验问题。

定稿补强：技术纠错、现实履行与法律救济分层

纠错应明确发生在哪一层。技术层可以追加更正记录、冲正账户或恢复权限；支付层需要追回、补付或重新结算；现实履行可能要求返还实物、停止使用、继续服务或恢复访问；法律救济还可能涉及确认、赔偿、临时措施和第三人关系。这些后果不能用一次链上冲正统一替代。

系统结案时，应列出哪些结果已经自动恢复，哪些需要责任人继续履行，哪些因第三人权利、不可逆交付或事实灭失无法恢复原状。每项未完成的后果应有义务主体、期限、监督和申诉路径。技术历史保留与现实后果纠正可以同时成立，前者不应成为拒绝后者的理由。

本章注释

1. [SRC-078] 美国国家标准与技术研究院（NIST）：[Blockchain Technology Overview（NIST IR 8202）](#)。[原文或官方页面](#)

- 本章引证：NIST：区块链技术概述。
- 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：NIST IR 8202：第7.3节、NIST IR 8202：第8.1节、NIST：区块链技术概述。
- 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
- 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

2. [SRC-016] OpenZeppelin：[OpenZeppelin文档：延迟操作与时间锁](#)。[原文或官方页面](#)

- 本章引证：OpenZeppelin：访问控制与角色权限。
- 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：OpenZeppelin文档：延迟操作与时间锁、OpenZeppelin：访问控制与角色权限、OpenZeppelin：角色与访问控制。
- 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
- 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。

共同创造并不总在一家企业内部完成。研发、生产、服务、传播与持续维护可能分布在不同组织，客户与供应商也可能参与能力形成和结果改进。参与主体增多，贡献就更需要被理解和核验；但每家组织拥有自己的资源、责任与治理程序，不能因为共同使用一本账，就被视为合并成同一个企业。

上一章讨论审计、纠错与责任追溯。当证据和权益穿过组织边界，这条责任链会遇到新的问题：谁能够证明某件事已经发生，谁有权评价其作用，哪些组织愿意承认该结果，以及出现错误时由谁纠正并履行后果。本章以跨企业贡献、共同规则、系统互认和平台权力为线索，讨论区块链怎样支持协作而又不抹去组织之间真实的制度边界。

生态治理在本书中指围绕共同事业形成的多方规则与责任安排，并不预设所有参与者服从同一中心，也不等于任何平台公开接入后就自然成为共同体。它的质量要由参与者能否明确协作条件、检验相互承诺、处理分歧和有序退出判断。

一、跨企业贡献记录与协作关系

跨企业贡献的起点是共同任务，而不是一份统一积分表。组织可以共同确定某项成果的目的、参与范围、交付条件和验收方式；也可以在已有业务合同之上增加可核验的协作记录。只有先说明参与者各自承诺做什么、如何证明完成，后续记录才知道在描述哪一种共同创造。

贡献事件应分别保留投入、交付、采用和结果。某企业投入研发资源，另一企业完成生产适配，客户实际使用后提出改进要求，都可能与最终成果有关；它们并非一种可以凭次数直接相加的动作。事件记录需要指明发生时间、关联任务、作出者、受领或验证者、证明材料及状态，避免同一事实在多家企业内部被重复登记后又被当作多项独立贡献。

跨组织证据往来自不同位置。交付方可以出具成果与过程资料，接收方可以确认收到及使用范围，第三方可以核查特定质量指标。每种签名证明其签署者作出了什么陈述，不保证所有其他主体已经同意该陈述的完整经济意义。制度应要求证据来源与证明范围一起流转，使之后的评价者看得出还缺哪一环。

面对共同成果，还要区分归因与分配。多方共同设计、反复修改的一项成果，可能无法精确切成各自独立生产的份额。可行的制度可以在事前约定贡献类别、共同贡献的确认程序以及无法分割部分的分配原则；也可以保留未决状态，等待证据充分时再判断。数字记录支持复核，但不会自动解决因果归属的难题。

个人与组织的关系也需分层。员工在企业项目中完成工作，其个人行为、企业承担的资源投入，以及企业对外承诺交付，分别属于不同事实。生态账本可以在必要范围内识别贡献者与所属组织，不应直接把个人业绩改写为对另一企业的债权，也不应因为企业对外结算，就删除实际参与者的历史贡献。

贡献记录与资本形成、权益成立之间仍有制度门槛。某合作方完成了交付，可能取得合同约定的价款；其工作又可能帮助共同事业形成持续能力，但这一判断需要组织吸收、持续使用与风险承担的证据。合作方是否进一步参与未来收益或治理，要依据另外的有效安排。跨企业“贡献分”不能自行转换为所有成员企业的股权或收益权。

共享账本适合维护多方需要共同核对的事件状态，特别是双方都不愿完全依赖对方单独保管记录时。它可以记载提交、承认、异议、修订及相应时间，并让授权主体核对前后版本。但共同记录解决的是证据可得与操作一致的一部分问题，不决定证据是否充分、服务质量是否达到标准，也不代替各企业原有的财务与业务审查。

记录层次	需要共同明确的内容	不宜自动推导的结论
协作承诺	任务、角色、交付和验收条件	已有可分配收益
贡献事件	行动、证据、确认者与争议状态	贡献具有确定市场价值
共同成果	多方作用、采用范围和持续效果	每方都取得同一资产的所有权
权益安排	权利主体、义务主体、条件与期限	一家组织的承认约束所有组织

为了使记录能够跨组织使用，应建立共同的任务与事件标识、签署主体识别和必要的版本关系。标识不只是技术编号，更要让各方分辨同一交付是否在不同系统中重复出现。身份映射发生变化时，也要保留当时哪一家机构、哪位有权代表以何种身份作出确认。

证据共享还受保密与个人信息边界限制。生产数据、定价条件、员工资料和客户行为，不宜因为一方希望“上链透明”就对整个生态公开。各方可以共享必要摘要、确认结果及受控访问办法，对详细材料规定持有人、保存期和审查条件。参与者能核验证据是否对应原始材料，比所有人同时看到全部原始材料更重要。

跨企业记录的最终目的，是降低对共同创造的解释成本。当每方都能说明自己承担了什么、确认了什么、仍对什么存疑，协作才有机会从一次交易延续为跨期的能力与关系。这样的关系可能成为利益相关者资本的组成部分，但其存在和持续作用，仍要在实践中检验。

二、共同规则与各组织自主权的衔接

共同事业需要一组相互承认的规则：谁可以加入，哪些事实可以共享，怎样确认交付，争议由谁受理，系统如何升级，以及退出时怎样处理未了事项。与此同时，每个组织仍要管理自己的人员、预算、商业秘密和法定职责。生态规则要能约束共同协作的接口，也应清楚划出各组织保留自主决定的范围。

共同规则可以按层次组织。基础层约定成员资格、数据与权利边界；协作层约定任务发布、证据提交、验证和评价；结算层约定资源、支付、对账与违约处理；治理层约定提案、表决、监督及修订。分层使参与者知道某项协议改变的是共同接口还是企业内部管理，减少“加入生态即接受全部未来规则”的不确定性。

权力来源不能由平台界面单独决定。平台可以提供发起提案和计票功能，是否有权代表一家企业同意规则，仍须由该企业的有效授权确定。某个员工拥有项目账户，不一定能承诺企业承担新增支付义务；企业代表能够签署协作记录，也不因此取得更改所有成员权益结构的权限。

共同规则还应说明哪些决定需全体成员同意，哪些可以由类别代表决定，哪些可以交由有授权的运营机构执行。业务数据格式更新和改变风险分担方式，影响程度不同，不能只因为两者都可写入“参数”，就使用同一级别的审批。对应的通知期限、异议程序和生效条件，也要与影响范围相称。

组织自主权需要以明确保留事项表达。是否接受某项具体任务、内部由谁参与、如何核算本企业成本、对外承担超过既定范围的义务，通常都需要组织自身的决定。共同规则若拟限制这些权力，应说明限制的目的、内容及得到各方同意的程序。共享基础设施可以降低重复协调成本，却不能替任何企业承担它没有接受的责任。

反过来，自主权也不是随意否认共同承诺的理由。企业已经按有效程序接受的交付、保密、结算或纠错义务，应按其范围继续履行。成员内部人员变更、信息系统替换或预算重新安排，可能影响操作路径，却不自动取消对其他参与者已经形成的请求。生态治理应同时保护成员的决策边界和共同承诺的稳定性。

有些规则需要在不同组织内部转化为各自的操作要求。共同规定由双方向指定材料签收，接收方就需要安排谁有权签收；共同规定错误数据应在一定期间内复核，各企业也需配置相应受理职责。共同文本获批，不等于成员内部已经具备执行能力。生效前应核对身份、预算、流程及数据接口是否就绪。

共同规则可以采用版本管理，但成员采用时间可能不同。过渡期要说明旧任务依旧规则还是新规则处理，哪些成员和业务已正式切换，涉及多个成员的任务怎样避免一方采用新口径、另一方采用旧口径。已成立的请求不能因为某家企业更新得较慢便成为无主状态；必要时应保留兼容期和负责协调的主体。

治理代表性同样需要设计。大企业承担较多资源风险，小企业可能承担关键专业工作，个人参与者又可能缺少正式成员席位。权重可以结合事项和责任配置，但应防止出资最多者或掌握平台者在所有议题上都取得无限决定权。受影响者至少需要适当信息、表达和救济渠道；对于直接改变其既有权益的安排，还需满足相应的有效程序。

一个成员参与多个生态时，可能面临义务冲突、资料重复提交和身份滥用问题。共同规则应允许有依据的保密与最小披露，也要规定哪些共享成果不得被重复承诺给相互排斥的主体。是否允许并行合作，应依具体承诺和竞争关系判断，不能笼统要求所有参与者把全部业务都置于同一平台之下。

共同规则的边界可概括为：在多方确实需要共同核验、协作或履行的事项上形成共享秩序；在各组织依法依约独立承担的事项上保留可识别的自治空间。只有这两部分都清楚，生态才可能在扩大时保持合作，而不以规模增长掩盖权力和责任的模糊。

三、跨系统互认、结算与争议解决

互认首先要说清“认”的是什么。甲企业确认一个人曾参与项目，乙企业可以接受这一历史事实的证明，却仍可依据自己的规则决定该事实是否满足任职资格；丙企业可以接受某项交付确已完成，却不一定承担甲企业对交付者作出的收益承诺。身份、事件、资格、评价和具体权利，处在不同层次，不能因为都能表示为数字凭证便一次性互相继承。

第十三章已经说明凭证角色及其验证边界。跨系统互认在此增加的是组织责任：接收方仍须决定信任哪一签发者、为哪个用途接受哪项声明，以及依赖错误时由谁承担复核与纠正义务。

互认安排需要公布最小必要条件：发行主体是否在授权范围内，凭证对应的对象和任务是什么，状态是否仍有效，证明材料可以在哪里核查，以及接收方采用什么业务判断。某些证明只需核验是否满足阈值，另一些则要查看完整的审查报告。若接收方要求超出用途的全部历史资料，互认可能降低参与者对信息使用的控制。

不同系统对同一词语的理解也可能不同。“完成”在一方系统中表示提交材料，在另一方系统中表示验收合格；“成员”可能只表示平台注册，也可能表示持续承担义务。互操作不应仅靠字段名称相同。各方需要共同的数据定义、状态映射与版本说明，并允许接收方标注“已核验格式、尚待确认业务含义”。

身份互认同样需要识别控制与主体的差别。分散式标识符可以帮助系统定位某个标识及其验证方法，但持有控制手段的人未必就是被标识的自然人或组织；代理、托管和集团关系都可能使两者不同。W3C 的 DID 规范也区分标识所指主体和标识控制者。生态互认应在必要时补充组织授权、代理关系和身份恢复程序。W3C：去中心化标识符规范〔1〕

跨系统状态同步则需考虑时间。甲企业撤回一项错误凭证，乙企业在撤回前已依据它作出决定，后续如何修正，不能只靠让查询接口返回“已撤回”。各方应约定状态更新时间、通知责任、既有处理的复查范围和新的更正记录。无论采用共享账本还是多套互连账本，状态到达各方的时间差都需要被制度承认。

结算比互认更进一步：它改变资源或债务关系。合作方之间可能按任务逐笔支付、定期汇总、在有依据的范围内相互抵销，或由共同资金池按约定条件支付。每种方式都需要明确支付义务人、受领者、计价对象、期间、费用和无法按期支付时的处理。账本能显示“待结算”额度，并不意味着成员企业已经实际交付相应资源。

若共同平台代为清分或托管资源，应区分它是在传递指令、代理收付款，还是自身承担兑付义务。平台展示的余额也需说明是成员间的应收应付、平台保管的资产，还是受其他条件限制的额度。不同关系对风险、监督和审计的要求不同；平台不能只通过统一界面把多个义务主体写成一个没有责任边界的“生态账户”。

跨组织结算要能与各方内部账目分别对接。一项任务在共同账本显示交付合格，付款方仍需核对内部采购或费用依据，收款方还需核对实际收款和自身收入条件。结算单、链上交易和银行回执可以互相引用，但应分别保留证明范围。若发生退款、部分支付或计价争议，双方系统都需要能够找到同一笔原始请求与后续调整。

对不同资产或计量单位的结算，还要说明换算来源和时点。把通证参考价格直接乘以数量，不能自动形成应付法定货币金额；一方愿意接受某种数字单位，也不意味着另一方有权以其替代原约定的支付对象。资源准备、价格波动、手续费与失败重试，都需要通过有效安排分配风险。

跨系统环节	可以共享的核验对象	仍需单独决定的事项
身份与授权	标识、签名、代理凭证及状态	是否承认其代表本组织行动
贡献与资格	事件、发行者、证明范围和版本	是否满足本组织或共同规则的条件
权益与结算	请求、金额、支付及对账记录	谁履行、用什么资源及何时完成
争议与纠错	原证据、异议、更正和通知记录	哪个机构裁决及如何落实后果

争议解决必须在协作开始时有入口。争议可能涉及交付事实、共同贡献归因、凭证真伪、规则解释、结算金额或支付失败；各类问题所需证据和有权处理者不同。可以先由任务双方核对业务事实，再按共同规则进入复核、调解或其他有效程序。若必须由特定机构作出最终决定，应说明其权限来源、适用范围及与各成员既有争议程序的关系。

跨组织争议尤其需要避免任何一方控制全部证据和程序。交付方持有工作过程，接收方掌握使用结果，平台保存状态与接口日志，三者共同构成判断材料。制度应规定必要的保全、提供和保密责任；不提供材料的后果也应有依据。审查者需要能够辨认资料来自哪里，而不是只接受一方生成的单页结论。

结果执行仍需回到各个义务主体。共同机构可以认定某项记录应更正，却需要明确由谁修改各自系统、谁通知下游接受过该凭证的组织，以及谁补付或返还资源。纠错状态应保持跨系统可见，不能在共同账本标记“争议解决”之后，让受影响者继续面对各成员系统中互相矛盾的余额。

互认、结算和争议解决形成一个闭环：先规定哪些证明可被接受，再确定由谁按照何种义务履行，最后使错误或分歧有可执行的处理路径。若只完成第一步，共享记录会提高传递速度，却未必提高合作可靠性。

四、平台权力、基础设施控制与生态退出

生态平台通常掌握加入入口、任务发布、数据格式、证据展示、结算接口和用户联系渠道。这些能力可以降低协作成本，也可能形成新的权力集中。即使平台声称账本由多方共同维护，若只有一家机构能够批准身份、升级协议或关闭关键接口，参与者实际依赖的仍可能是单一控制点。

观察平台权力，不能只看链上治理票数。谁决定哪些组织可以加入，谁能修改贡献评价参数，谁能冻结争议账户，谁掌握原始业务资料，以及谁可以阻止成员读取历史记录，都会改变协作结果。某个操作没有进入智能合约，不代表它对生态没有治理影响。

基础设施控制还可能通过技术设计固化。独占的数据格式、无法替换的身份服务、只在平台内部有效的贡献编号和封闭的结算接口，使成员即使名义上保留退出权，也难以把既有业务带走。评价平台是否开放，应检查接口、数据可携带性、历史凭证的可验证性和替代服务接入条件，而不只检查源代码是否公开。

共享基础设施仍需要运营者。有人要维护节点、更新软件、处理身份争议、承担安全费用并协调不同系统的故障。治理的目标不是假装这些权力不存在，而是公开它们的范围、资金来源、监督方式和更换程序。运营者可以获得与职责相称的报酬，同时必须说明其服务质量、利益冲突和不履责时的替代方案。

平台参与市场交易或自行持有大量权益时，更需把运营职责与自身利益区分。若平台决定评价标准、掌握分配数据又能从发行或交易中获益，就需要特别检查其是否利用信息和程序优势改变分配。必要的披露、独立复核和受影响成员参与，可以降低权力滥用；单纯宣布“规则写在链上”并不足以解决这些关系。

平台费用也要接受共同监督。交易、验证、存储、争议处理和退出迁移可能分别产生费用。参与者应知道收费对象、调整权限与实际服务的对应关系。过高或不可预见的迁移费用，会把退出权变成纸面承诺；将治理成本全部转嫁给较弱成员，也可能让他们无法真正参与共同决定。

生态退出需要同时回答成员与参与者两个层面。企业退出共同平台，可能结束未来任务，但其已接受的交付、保密、结算、数据保存和争议处理义务仍需按有效安排完成。个人在成员企业或平台上停止活动，也不应自动失去已经形成的请求。退出程序要把未来合作终止与历史关系结清分别列明。

迁移时，成员应能取得自己有权保留的业务资料、凭证、审计证据和未了事项清单，并验证导出材料与原记录的对应。平台也要保护其他成员的商业秘密与个人信息，因此“可携带”并不等于复制全体数据库。共同任务的证据若由多方共同维护，应预先规定各方在退出后仍能核验什么、保留多久以及如何请求必要材料。

退出权还需要资源与技术条件。若支付请求只能通过平台内部钱包提出，成员离开后必须有替代办理方式；若某项身份凭证依赖即将停用的服务，应提供适当验证或迁移期限。运营者停止服务、成员不愿继续合作或生态治理发生根本分歧时，也需要保证历史关系可审计、未付请求可追踪、正在进行的任务有明确处置。

对于形成网络效应的生态，成员越多，单个成员退出越困难。共同标准与可替换接口可以降低这一成本，但也可能需要较高的初期协调投入。是否采用统一平台、联盟式基础设施或可互认的多套系统，应由实际协作关系、信任结构和运营成本决定，而不能把“去中心化”当作免于比较的结论。

本书提出一个需要检验的方向：让生态治理具有可迁移的制度连续性。参与者应能够在不抹去历史事实、不重复取得同一项权益的前提下，更换服务提供者并维持可核验的请求。检验这一方向，需要观察真实迁移所需时间、成本、资料完整性、结算不中断的程度以及弱势成员能否使用退出渠道；仅仅开放一个“导出”按钮，还不足以证明退出可行。

跨组织协作真正形成长期资本，依赖的是参与者可以共同维护的能力、相互理解的规则和持续可信的关系。区块链使记录与部分执行跨越企业边界，但共同事业是否正当有效，仍取决于各组织能否清楚承担承诺、分享决定并在分歧中保持可履行的秩序。生态越大，这些制度安排越不能被单一平台的增长指标取代。

下一篇将进入系统构建。第二十五章从整体技术架构出发，讨论业务、证据、规则、权益与治理模块怎样连接，链上与链下如何分工，以及系统如何在保持制度边界的条件下与企业已有设施协同运行。

跨组织协作协议应明确主体、准据法、管辖或仲裁地、送达、证据、临时措施、破产、权利优先和退出后存续条款。技术互认只能说明系统能够读取或验证某种状态，不能保证合同、担保、登记或裁决在另一法域自动获得承认。

生态治理还要识别标准维护者、身份根运营者、接口提供者、预言机、结算入口和软件升级者。共同协议应公开依赖、费用、变更程序、数据可移植格式、替代运营者和退出测试。所谓分叉权只有在参与者能够取得数据、软件、标识映射和运行能力时才是现实选择；制度应披露实际迁移成本，防止互操作接口形成新的基础设施垄断。

本章注释

1. [SRC-073] 万维网联盟（W3C）：去中心化标识符规范。[原文或官方页面](#)
 - 本章引证：W3C：去中心化标识符规范。
 - 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：W3C：去中心化标识符规范。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第六篇 系统构建：从技术架构到有效性检验

第二十五章 利益相关者资本治理的整体技术架构

前五篇分别讨论了制度技术、数字资产、共识执行、贡献确认、资本与权益，以及多方治理。进入系统构建时，需要把这些论证放进同一张能够运行的关系图：共同创造怎样形成业务事件，哪些证据支持对事件的确认，哪一版规则决定后续处理，谁因此获得何种请求，最后又由谁监督结果并修订规则。

上一章把视角扩展至跨组织协作。不同企业可以共用部分记录和核验程序，但仍保有各自的权利义务与现有系统。这使架构设计不能从“把一切放到链上”出发，而应从制度所需的共同状态、事实来源、责任主体和实际履行出发。区块链在其中承担被明确选择的职能，其余工作需要业务流程、数据服务和组织程序共同完成。

本章提出的是一种可检验的整体架构，不是要求所有企业采用同一套产品。判断架构是否有效，应看它能否支持明确的业务闭环、保留权利边界、处理错误与争议，并在需要时替换某项技术而不使参与者失去已形成的请求。

一、业务、证据、规则、权益与治理模块

整体架构可以按五类职责组织。业务模块说明共同创造正在做什么，证据模块保存何以认定相关事实，规则模块确定这些事实如何进入制度判断，权益模块表达由此成立的具体权利和履行状态，治理模块决定、监督和修订这些安排。模块是职责边界，可以由不同软件承担，也可以部署在同一系统中；分开的目的，是让每一步有可核验的输入和有权负责的人。

业务模块应从承诺和任务开始。它记录合作对象、任务范围、交付要求、期间及参与角色，并在工作推进中接收投入、交付、采用和结果信息。企业原有的项目、订单或服务系统可以继续承担大量业务处理；共同架构只需取得完成后续确认所必需的事件和标识，不必另造一套覆盖全部经营活动的界面。

任务与事件需要保持关系。一个交付可能回应多个承诺，数个组织也可能共同完成一个成果；修改、撤回或追加交付时，应能找到原任务与原参与者。业务模块输出的是待核验的事实主张，不应因字段填满便直接输出“贡献价值”或“应得权益”。

证据模块关注来源与证明范围。谁提交了材料，谁签收或核验，材料证明交付、质量还是使用结果，是否存在异议，以及原始资料由谁保管，都应在此得到表达。对不同可信度的材料可以采用不同核验路径，但证据之间的冲突不能靠覆盖旧文件处理。保留原始状态、修订原因和有权复核的结果，是后续审计的基础。

规则模块把有效制度与可执行条件连接。它保存资格、计量、转换、分配和审批规则的版本及适用范围，并指向形成规则的授权决定。纯粹的计算逻辑可以由程序运行，依赖事实评价或例外裁量的事项则应进入相应人工程序。规则模块要能够回答“为什么在这个期间、对这个主体适用这一版规则”，不能只返回一个缺乏依据的数值。

权益模块不能被简化为通证余额。它应区分贡献账户、资本记录和权益账户，并在权益内部说明所有权、收益请求、治理参与、使用资格等不同安排。每项具体权益要连接主体、义务主体、成立依据、限制和兑现条件；若采用数字凭证或通证，还需说明凭证状态与权利变动如何对应。凭证转移不应悄然改写历史贡献或企业已有义务。

权益模块还需跟踪履行过程。已确认资格、已计算金额、已成立请求、已安排支付、链上转移成功和链下实际收款，不能只有一个“完成”标记。若支付被退回、权益遭到争议或部分履行，系统要能保留原请求与后续处理的联系，使余额具有清楚的现实含义。

治理模块负责提案、审议、授权、监督和救济。它管理参与资格、代表与委托关系、表决程序、利益冲突披露，以及规则变更的生效状态。它也接收业务和权益环节中的异常，决定哪些问题可按现行规则纠正，哪些需要重新审议制度。治理模块的输出不是一串抽象投票数据，而是对确定事项有效的决定与相应执行责任。

模块	主要输入	主要输出	必须留下的责任线索
业务	承诺、任务与经营过程	待确认的事件及结果	发起者、履行者与业务范围
证据	原始资料、签收与复核	有证明范围的确认状态	提供者、保管者、核验者
规则	有效制度、授权与参数	适用口径和可执行条件	制定者、生效版本、解释者
权益	确认事实与有效规则	具体请求、限制及履行状态	权利主体、义务主体、经办者
治理	提案、监督信息与争议	决定、修订和纠错要求	代表、表決者、复核者

WISERUNION · V1.0162 / 240

五个模块之间还需要共同的基础能力：身份与代理关系管理、时间和版本标识、事件关联、访问控制、审计日志及通知。基础能力不应变成新的不受约束的权力中心。例如，负责维护身份服务的人可以帮助核验代理权限，却不能因此决定该代理人有权代表企业批准额外的收益分配。

从一条具体流程看，业务事件先进入证据核验；得到确认的事件按适用规则计算；经过必要的人工作出资本或权益判断；权益结果再进入履行与对账；异常、异议和效果评估返回治理程序。这条流程并非每一步都必须发生：已确认的贡献可能没有资本化条件，资本形成也可能没有为该贡献者设立新的所有权。系统应允许流程止步，并解释止步的依据。

流程还应能逆向追踪。审计者从一笔权益或支付，能够查回原业务、证据、规则、授权和实际付款；当某项证据被撤销，系统则能找到受其影响的评价、请求与支付。设计阶段若只关注顺向发放，不考虑逆向查找，后续纠错就可能必须依赖人工逐页搜寻。

模块化的最终目的不是画出整齐的系统图，而是阻止概念在接口处被悄然合并。投入不自动成为贡献，贡献不自动成为资本，资本不自动成为所有权，收益权也不自动赋予治理权。每一次跨越这些边界，都需要对应的制度条件、事实依据和有权程序。

二、链上链下的数据与执行分工

把哪些信息写入链上，首先应看参与者是否需要共同确认同一状态、对单方修改是否存在实质争议，以及维护分布式核验是否具有足够价值。数据规模、敏感性、更新频率和删除需求也会影响选择。共享账本、签名日志或普通数据库各有作用，不宜以“重要数据一律上链”代替逐项判断。

链上更适合保存多方共同需要核验的状态转换：某项授权是否已经满足，某笔数字资产控制是否转移，某个规则版本何时被共同采用，以及某次更正与原记录如何关联。在具体设计下，也可以保存可验证的凭证状态或证据摘要。链上存储的位置并不决定权利是否成立；若对象是现实资产或服务，仍须检查链下关系与履行。

链下通常保存容量较大、需要频繁修改或受访问限制的业务资料，包括合同、交付文件、人员信息、财务细目、质量报告和争议材料。链下并不意味着无法审计。资料可以保留来源、版本、签名与必要摘要，通过受控查验与链上记录相互印证。若原始文件已经遗失，链上的摘要只能证明某个文件曾被对应记录，无法替代丢失的内容。

执行也需要分工。条件明确且输入可靠的状态转换，可以由智能合约或其他规则引擎自动处理；事实核验、例外裁量、现实资产交付和跨机构支付，则需要相应业务与组织程序。链上交易执行成功，只能证明在该协议条件下完成了对应动作，不能统一解释为链下服务已经提供或义务已经清偿。

数据进入链上前，最重要的是输入责任。谁可以提交业务结果，谁复核材料，提交者的签名证明什么，以及发现错误后怎样标注和更正，应比选择哪一种预言机或接口更早确定。只把错误资料以更可靠的方式保存，会增加错误长期存在的影响范围。

链上链下连接还要处理不同的时间。交付完成、审核确认、链上记录被确认、付款发起与现实到账，可能发生在不同日期。系统应保留各自时间与状态，避免因链上确认较早就把付款显示为已到达，或因业务系统尚未更新而重复生成相同权益。

敏感信息不宜为了透明而公开复制。对个人身份、薪酬、商业秘密和未公开争议，可以只开放必要的资格证明、总量核验或经过授权的审计查询。W3C的可验证凭证数据模型提供发行者、持有者与核验者之间交换陈述的结构，并讨论凭证状态和数据最小化；这种结构可以服务于某些跨系统证明，但能否相信陈述内容仍取决于发行者和实际证据。W3C：可验证凭证数据模型 2.0〔1〕

跨系统操作可能出现一边成功、一边失败。链上已锁定额度，银行支付却被退回；链下服务已交付，链上凭证却尚未生成。架构应提供稳定的业务请求标识、可重试的操作记录和差异处理队列，使各方知道哪一步完成、哪一步待查。不能因为跨系统无法像单一数据库事务那样同时完成，就把某一边强行改写为已经发生的结果。

选择链上范围还需要考虑长期成本与治理。网络费、读取方式、合约升级权限、历史数据保留和节点运营，都影响参与者未来能否核验自己的请求。某一时期成本低，不保证长期适用；若网络或运营方发生变化，制度仍应能解释存续的权利、取得必要证据，并安排迁移或替代履行。

因此，链上链下的分工应接受一项朴素检验：将某项数据或操作移到链上后，究竟改善了什么共同问题，谁承担新增成本，以及何种事实和权利判断仍需链下完成。只有答案清楚，共享账本才成为制度技术的一部分，而不是给旧流程增加一层难以解释的记录。

三、与财务、人事、客户及供应链系统的连接

利益相关者资本治理并不是企业经营数据的唯一来源。财务系统维护收入、成本、应付和实际收付；人事系统管理劳动关系与岗位变更；客户系统保存使用、反馈及服务记录；供应链系统追踪订单、交付、验收与退回。治理架构应从这些既有系统获取经授权、可核验的信息，再按自身制度生成相应结果。另建一份互不对账的“治理数据”，只会增加冲突。

连接前应识别每类事实的权威来源。财务部门确认某笔款项已到账，不等于它确认了某参与者符合收益分配条件；人事部门确认某人曾任职，不等于它确认此人在某项目上的贡献分值。一个系统可以对部分事实具有记录优势，但不能因其被称为“主系统”，就获得对所有制度判断的最终解释权。

财务连接应围绕资源与义务建立映射。本书前面区分了收入、利润、现金流和可分配资源，架构也应保留这些分类。分配模块从财务系统取得经过适当核验的核算结果和资源状态，形成候选分配范围；有权主体作出方案决定后，支付指令再回到实际支付路径，并将回执与原请求逐项对账。治理系统不能用自己展示的通证价格或账户余额替代组织的真实履行资源。

财务系统还需接收治理侧的有效请求。权益成立后，是否构成应付、何时结算、金额怎样调整，应由有关制度和适用核算要求共同确定。系统接口应传递请求来源、期间、义务主体和更正记录，避免把一项尚待条件满足的奖励显示为已经到期的货币支付，也避免支付已发生却未更新权益状态。

人事连接的重点是身份、角色与代理关系。员工入职、调岗、休假和离职可能改变参加未来任务或代表企业操作的资格，但对过去已经确认的贡献和已经成立的请求，不能由人事状态变更自动抹除。治理系统应区分“当前有权执行某项操作”与“历史上是谁完成了工作”，并给离岗人员保留适当的结算与异议渠道。

客户系统可以提供使用、服务和反馈证据，却不应将点击、停留或购买次数直接换算成资本。某项客户反馈是否构成有效贡献，需要事前说明任务目标、证据质量与使用结果。客户资料还有明确的访问目的和保密边界；将行为明细全部复制到共享账本，只会扩大与评价无关的信息暴露。

供应链系统连接更强调多方确认。订单发出、货物送达、质量验收、安装使用和售后退回，代表不同状态。供应商提交的发货记录可以与采购方的签收、检验记录互证，但一方“已发货”不能自动改成双方“已完成履约”。若出现部分交付或退货，贡献评价和结算安排都要能找到原事件并保留调整依据。

这些系统之间通常采用不同编号和时间口径。一个人可能在项目系统有参与者编号，在人事系统有员工编号，在支付系统有收款对象编号；同一订单也可能拆成多个交付与付款批次。连接层需要维护受控的对应关系，并记录每个编号的来源与有效期间。跨系统统一身份，不等于公开暴露所有内部标识。

来源系统	可提供的主要事实	治理系统仍需作出的判断
财务	核算结果、资源状态和支付回执	哪些资源可按何种授权进入分配
人事	任职、岗位、代理与变更记录	对具体事项是否具有参与资格
客户	使用、服务和反馈记录	反馈是否符合贡献与评价条件
供应链	订单、交付、验收和退回状态	共同成果如何确认及如何结算

接口接收事件时，应区分新增、更正与撤销。财务冲回、人员身份纠错、客户撤回错误反馈或采购退货，都可能改变已有计算。连接层应把变化送入有权复核的流程，标出受影响的下游权益；不能静默覆盖原始事件，也不能机械地把每次更新当作一份新的贡献。

重复消息和迟到消息也需要处理。同一来源系统可能重发交付事件，网络中断后旧消息又可能晚于新状态到达。稳定的业务标识、来源版本、事件时间与接收时间，可以帮助系统识别重复和先后关系。技术上阻止重复导入只是第一步；若业务本身确有两次相似交付，还需要回到任务和证据判断其是否属于不同事件。

连接责任应落到接口两侧。来源部门负责什么数据质量，治理系统负责什么规则解释，技术服务商负责什么传输与运行，都应清楚。发现差异时，应能说明谁核对原始记录、谁决定是否重算、谁通知受影响者。接口越自动化，越需要避免“系统之间传过去了，所以没有人负责”的空白。

架构也要允许企业现有系统暂时不具备标准接口。起步时可以采用有权限、有版本和有复核的批量导入，只要来源和校验条件清楚，仍可以建立可审计的流程。是否进一步实时连接，应根据业务变化速度、错误成本和实施资源判断，而不是把系统集成程度直接当作治理质量。

四、数据标准、接口边界与系统可替换性

要让不同模块和组织长期协作，首先需要共同理解数据。主体、角色、任务、贡献事件、证据、规则版本、资本记录、权益请求、履行结果和异议，至少应各有明确定义。数据标准不只是字段格式，还包括一项状态何时产生、由谁确认、可在哪些场景使用，以及何种变化必须产生新记录。

“已确认”尤其不能成为跨模块的模糊通行证。业务已验收、贡献已确认、资本已形成、权益已成立和支付已完成，分别指向不同对象。标准要求记录写明所确认的内容、依据、权限、时间和版本；任何模块引用它时，还要说明该确认是否足以支持当前动作。

共同标识使跨系统记录能连接，但标识策略应考虑合并和分离。两条记录后来被证实属于同一主体，或一个组织发生业务拆分，都不能只靠删除其中一个编号解决。系统应保留映射的依据和有效期间，使历史请求仍可追溯。标识符本身也不应被当成对现实身份或代理关系的充分证明。

接口边界需要写成双方可以检验的约定。接口提供什么事实，接收方有权怎样使用，哪些字段为必填，错误如何返回，多久可以取得更正，以及旧版本停止支持前如何通知，都应有明确规则。对于会产生经济请求的接口，还要注明重复处理、超时和重试后的核对办法，不能让传输成功自动代表制度判断成功。

数据标准与组织规则需要同步管理。增加一项“贡献类型”看似只是扩充选项，却可能改变评价口径；调整“已履行”的定义可能影响应付与对账。对数据含义的变更应有相应制度授权，并明确新旧数据如何比较。否则，程序仍能运行，结果却可能已经失去可解释性。

可验证凭证、签名日志或共享账本可以为部分记录提供一致的交换与核验形式。标准形式仍须配合可信发行者、业务定义和接收方的判断。技术互通解决的是机器能否识别一份声明；制度互通还需要各方同意它在何种范围内具有作用。因此，选择标准时要同时检查规范是否清楚、各方是否能实现，以及退出后是否仍能核验历史声明。

系统可替换性应落实到具体对象。更换证据存储，不应丢失原始文件与版本关系；更换规则引擎，不应改变已生效规则对旧期间的适用；更换钱包或账本服务，不应让已成立请求失去主体对应；更换平台运营者，不应使监督者无法读取必要审计材料。没有这些验证，所谓模块化只是部署图上的分隔。

替换需要可导出的资料、可读的规则、可核验的历史以及可执行的交接。导出不仅是下载一份表格，还应说明字段含义、记录之间的关系、签名或摘要怎样验证、未完成事项处于什么状态，以及由谁继续履行。涉及其他主体的材料，还要按权限和保密条件处理，不能为了可迁移性任意扩大数据复制。

接口替换也需要兼容期。新旧系统可以在限定时间内并行核算，对相同业务给出结果并解释差异；正式切换则应明确截止时点、未完成请求的处理者和回退条件。若并行过程中发生实际支付，必须指定唯一的执行路径，以免两套系统分别把同一请求当作待付。技术切换不应变成权利内容的隐蔽修订。

为了验证架构是否真正可以替换，可以定期选取有代表性的任务，从业务事件重建证据、规则、权益和履行结果，并在备用系统中复算。差异应能解释，而不是靠修改备用数据消失。这种演练也能暴露对某个供应商、某把密钥或某个没有文档的内部判断的依赖。

架构治理还要为接口留有更正和申诉入口。自动导入会提高处理量，也会放大来源错误；模块一旦互相引用，错误可能快速进入贡献评价、权益和支付。系统应能把有疑问的输入隔离出来、查找受影响结果、在有权程序下重算，并为已履行部分提供后续处理路径。可替换性与可纠错性在这里相遇：两者都依赖清楚的来源和版本。

本书提出的整体架构，可以从一个范围有限的闭环开始验证：明确参与角色和一项共同任务，保存必要证据，应用已授权规则，形成可解释的权益结果，核对实际经营与履行，再将异常和反馈带回治理。这样的起点能检验模块之间是否真的连接，也能让组织看清哪些工作需要继续人工判断，哪些共享状态值得采用区块链。

技术架构最终要服务于共同创造持续形成的资源、能力与合作关系，而不是以模块数量或上链比例证明成功。只有业务、证据、规则、权益和治理之间的责任能够被理解、核验并延续，制度技术才可能成为利益相关者资本治理的基础设施。

下一章将进一步讨论安全、隐私与系统持续运行，检验这套架构在合约缺陷、密钥风险、错误输入、数据保存及灾难恢复面前，能否继续维护参与者的权利和组织的行动能力。

定稿补强：三类可用性与财务接口控制

整体架构应把协议数据可用性、证据可取回性和业务连续性配置到不同责任模块。链上状态层负责可验证的共同状态，证据层负责在权限和保留期内提供材料，业务系统负责持续履行与恢复。接口必须标明权威来源、版本、失败模式和降级路径。

治理子账进入财务系统时，还需要总账接口控制。每一批次应具备子账到总账映射、借贷或余额平衡、截止日期、币种、异常队列、关账责任、会计凭证链接和审计抽样路径。贡献或权益事件完整，不表示会计分录已经完整；跨期差异、失败支付和后续冲正必须进入关账程序。

本章工具与图表

本章的制度关系可结合附录二、附录六使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

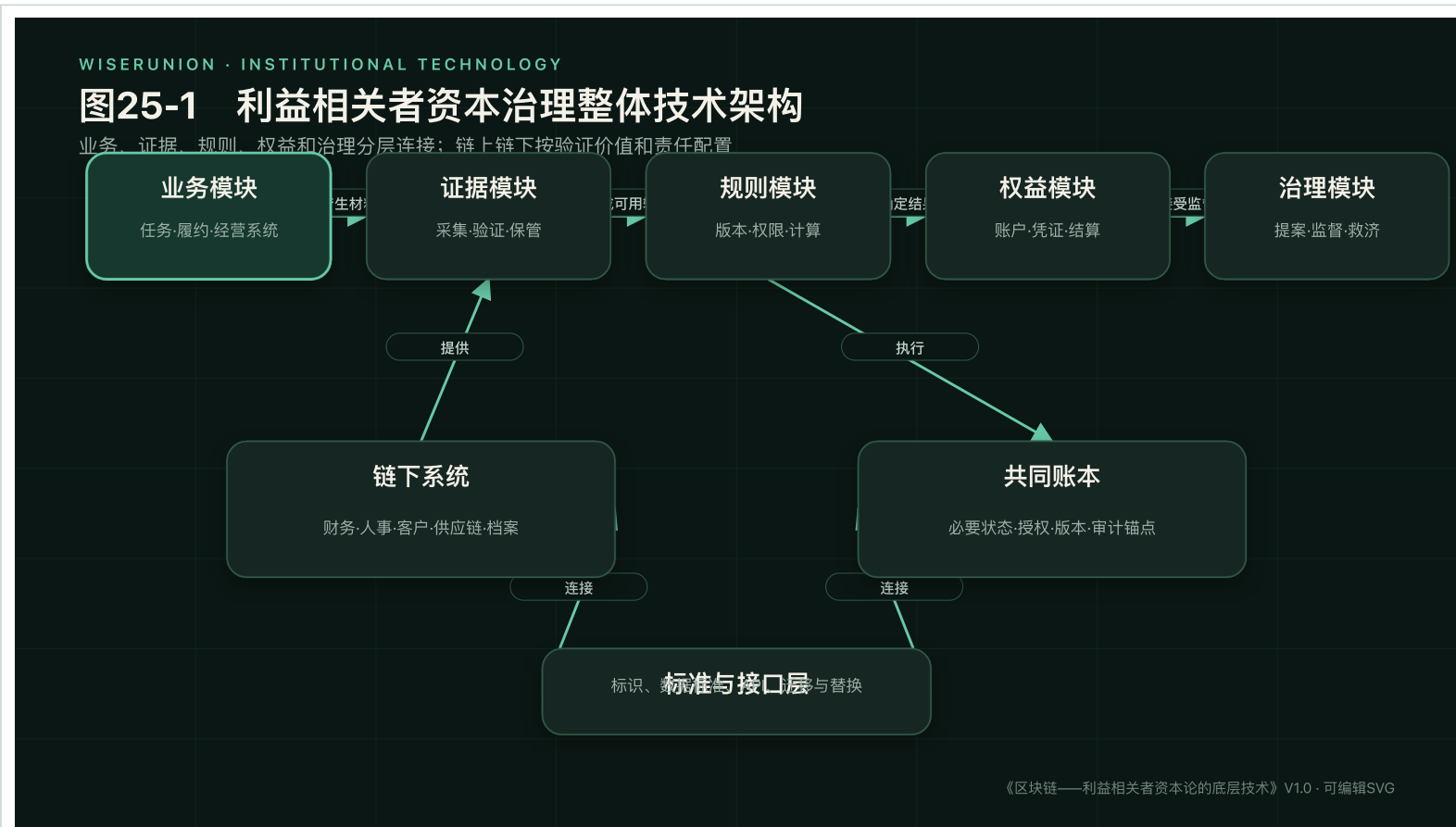


图25-1 利益相关者资本治理整体技术架构

图25-1 利益相关者资本治理整体技术架构。业务、证据、规则、权益和治理分层连接；链上链下按验证价值和责任配置

本章注释

1. [SRC-076] 万维网联盟 (W3C) : Verifiable Credentials Data Model v2.0。原文或官方页面
 - 本章引证：W3C：可验证凭证数据模型 2.0。
 - 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：W3C：可验证凭证数据模型 2.0、W3C：可验证凭证中的选择性披露与隐私考虑、W3C：可验证凭证的参与角色与验证边界、W3C：可验证凭证的验证与业务判断、W3C：可验证凭证与数据最小化。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第二十六章 安全、隐私与系统持续运行

利益相关者资本治理一旦依赖数字系统，系统出错就可能改变参与者的现实处境：贡献证据找不到，权益余额错误，支付被阻断，管理权限被误用，或者本应只供特定主体查阅的资料被长期公开。安全因此关乎资产、记录与服务，也关乎谁能够继续行使权利、质疑决定并获得补救。

上一章把业务、证据、规则、权益与治理组织为相互连接的模块。本章进一步检查这套架构在攻击、故障和长期运行中能否维持其制度承诺。技术防护可以降低特定风险，隐私安排可以限制信息使用，持续运行机制则使故障不至于使历史关系和未履行请求消失。三者需要一起设计。

本章不会把“区块链难以篡改”当作安全的总答案。不可随意改写的账本，仍可能保存错误输入；自动执行的合约，仍可能忠实执行不合适的规则；多个节点仍可能共同依赖同一把管理密钥。应当从要保护的关系出发，逐一说明可能失去什么、由谁控制、怎样发现异常以及失败后如何恢复。

一、威胁模型与关键资产识别

威胁模型首先要确定保护对象。资金和链上资产容易被看见，但关键资产还包括原始业务证据、身份与代理关系、有效规则版本、分配资格、未履行请求、审计日志和能够恢复服务的密钥。某一记录虽然没有市场价格，若它是证明贡献或请求的唯一依据，丢失后仍可能给参与者造成重大损害。

保护对象应按其作用区分。数字资产需要防止未经授权的转移与重复兑现；证据需要完整、可得和正确关联；规则需要保持版本与生效范围；个人资料需要限制披露；支付和申诉渠道需要保持可用。不同对象有不同失败方式，不能用一次链上交易成功证明整套制度已经安全。

威胁还要识别谁具有能力接近这些对象。外部攻击者、恶意参与者、越权员工、被盗用账户的操作者，以及虽无恶意但会误操作的维护者，可能从不同入口造成相似后果。协作企业、云服务商和外部数据提供者也掌握部分事实与运行能力。建模不应假设所有组织都诚实可靠，也不应把每个参与者预设为敌人；需要识别各方实际可以改变什么。

权限关系比组织名称更能揭示风险。谁能够签发身份凭证、提交业务事实、修改评价参数、升级合约、暂停系统、提出支付指令、访问个人资料，以及批准恢复运行，应逐项列出。多项权限集中在同一主体时，控制链会缩短，但独立核验也会减少；分散权限则可能降低单点风险，却增加协调时间。选择要结合后果和可恢复性。

风险评估应沿业务过程进行。设立任务时可能发生虚假身份或越权承诺；提交贡献时可能重复报送或伪造交付；评价时可能采用错误权重；形成权益时可能跳过授权；支付时可能错付或重复执行；争议时可能隐藏关键材料。每个环节都应问：错误能否被发现，何时发现，能够阻断多少后续动作，以及谁负责通知受影响者。

安全还包含可用性。一项服务即使没有资产被盗，只要参与者持续无法查看证据、提出异议或领取已成立回报，制度履行也可能受到损害。需要识别哪些功能必须连续运行，哪些可以临时停用，以及中断期间怎样保存申请时间和原有请求。维护系统的能力，是权利兑现条件的一部分。

隐私风险则不止“数据库泄漏”。公开地址与身份资料之间的关联、多个系统共用同一标识、访问日志被用于推断工作关系，均可能让原本分散的信息被重新拼接。若一个贡献者只有通过公开自己的客户、薪酬或合作网络才能证明贡献，制度设计本身就在制造不必要的暴露。

关键对象	典型失效方式	应保留的恢复条件
资产和支付请求	越权转移、重复支付、余额错误	独立对账、未了请求与授权记录
证据与贡献历史	丢失、伪造、错误归属	原始来源、版本、异议及复核路径
规则与治理权限	未授权升级、参数篡改、集中控制	有效文本、决定记录与权限交接
身份和个人资料	冒用、关联推断、越界披露	代理核验、访问记录与限制机制
运行能力	节点中断、服务商退出、密钥遗失	备份、替代办理和恢复责任人

威胁模型需要区分发生概率与损害程度，也要考虑风险会否沿模块扩大。一份错误证据可能通过自动接口进入贡献评价、权益配置和支付；一次管理密钥失陷可能影响所有后续规则。优先保护的不是最显眼的功能，而是可能造成重大、难以逆转后果的连接点。

美国国家标准与技术研究院的网络安全框架将网络安全管理置于组织风险管理之中，强调用系统化方法理解和改善风险。本书借其风险视角说明：技术控制需与治理责任、持续监测及恢复能力一起安排，而不是以一份安全认证代替具体制度判断。NIST：网络安全框架 2020〔1〕

模型还需随着实践修订。新增合作组织、改变资金托管方式、引入新的身份服务或调整治理门槛，都可能产生新的控制点。一次演练或审查通过，只证明当时的特定范围；应记录前提、未覆盖部分和下一次复核条件，使安全判断能够随着制度变化更新。

二、合约、密钥、预言机与治理攻击面

智能合约风险首先来自规则与程序之间的差距。规则文本要求的限制如果没有进入代码，程序会允许制度不认可的动作；代码中多出未经授权的限制，又可能阻碍合法请求。审查应同时对照有效制度、测试输入和实际部署版本，不能只检查代码能否在理想条件下执行。

合约还可能在边界条件下出现意外行为。精度处理、跨期状态、批量操作失败、外部合约调用及升级兼容，都可能影响权益或资金。上线前应有适当测试和独立复核；上线后应监测异常金额、权限调用和状态变化。审查范围必须包括被调用的外部组件和管理员能够改变的配置，否则一份“代码已审计”结论可能遮蔽最重要的动态权限。

不可升级与可升级都存在代价。不可升级有助于使执行逻辑更可预测，但发现缺陷后可能难以修复；可升级使纠错更灵活，也给掌握升级权的人更大影响力。选择前应说明升级条件、批准机构、等待期、可核验的变更说明、回退能力与未了请求处理，避免技术架构先于治理决定确定权力边界。

密钥保护的是操作能力，密钥控制不等于现实权利归属。资产转移、参数变更、合约升级与紧急暂停若使用不同权限，应分别配置并记录授权。高风险操作可以增加多人参与、时间间隔或独立复核；同时需要确认多把密钥是否由不同主体实际保管，以及遗失或人员变动时如何安全交接。

私钥被盗、签名设备故障或继任人员无法接手，会以不同方式造成中断。系统应在日常运行前建立权限清单、恢复程序和撤销路径，规定谁可以启动恢复、怎样核验身份、旧权限如何失效。未经有效审查的“找回密钥”机制也可能成为夺取控制权的入口，因此恢复能力与滥用限制应同时设计。

预言机及其他外部输入会把链下陈述带入自动执行。报价、履约状态、身份资格或客户使用结果，都可能依赖外部提供者。系统能核验消息来自被指定接口，却未必能判断来源事实准确。重要输入需要明确采集方式、提供者、复核者、更新时间和异常值处理；若一个输入源被操纵便能触发大额分配，应限制其单次影响或增加独立核验。

外部数据中断也要有明确后果。报价停止更新时，不能默默沿用旧值完成一项原本依赖实时价格的兑现；业务系统暂时无法确认验收，也不能把“没有反对”解释为已验收。对于有条件的自动执行，应预先规定过期数据、来源分歧和校验失败时进入什么待审状态。

治理攻击面经常隐藏在技术权限之外。少量主体可能通过掌握提案入口、代表授权、投票权重或议程安排改变基本规则；也可能利用紧急权限长期暂停异议者的领取。治理程序应核查资格来源、权重集中、利益冲突、修订门槛以及恢复正常程序的途径。一次形式上有效的投票，若超越适用权限，仍需要制度审查。

智能合约中的角色控制可以限制某个地址可执行的操作，但无法独立判断地址背后的组织授权是否持续有效。OpenZeppelin 的访问控制资料区分角色及其授予、撤销过程；在利益相关者资本治理中，这些技术角色需要映射到可核验的职责、代理和交接记录。OpenZeppelin：角色与访问控制〔2〕

各类攻击面之间还可能形成连锁。虚假数据进入贡献确认，随后利用管理员权限降低审查要求，再通过自动分配转移资源，最后借助日志访问限制阻碍追查，任何单点防护都难以覆盖全过程。系统需要让异常信号在模块之间相互印证，并使监督者能够及时取得必要材料。

防护措施也可能增加新权力。能够冻结账户、替换预言机或接管系统的人，需要受到授权、记录和复核约束。安全措施的意义，是让风险可被限制并使责任可追溯；若处置者完全不受监督，系统可能以防护之名引入新的治理风险。

三、数据最小化、保留期限与删除需求

治理系统需要保存证据以便确认贡献和处理争议，也可能必须回应个人资料的访问、更正与删除需求。二者不能靠一句“全部上链”或“全部删除”解决。设计之初就应问每项数据为何收集、谁会使用、需要保存多久、到期后如何处置，以及出现请求时由谁判断是否仍有保存依据。

数据最小化从任务开始。证明某人符合参加项目的年龄条件，未必需要复制其完整证件；确认某项交付按时完成，也不一定需要公开整个内部工作记录。业务处理者应只取得完成当前判断所必需的资料，并说明若需进一步复核，怎样在授权范围内访问更详细的来源。

W3C《可验证凭证数据模型》在隐私讨论中建议发行者限制凭证内容，核验者也应只请求完成特定交易所需的信息。该原则适用于本书的身份和资格接口：能证明限定条件时，不应默认披露全部身份与履历；即使采用可验证凭证，接收方仍须决定如何使用与保存取得的信息。W3C《可验证凭证与数据最小化》^{〔3〕}

最小化还包括限制重复复制。个人资料如果在业务、人事、证据、链上索引和审计库中各存一份，任何一处泄漏都会扩大影响，后续更正也难以同步。系统可以保留受控的来源位置和必要引用，让授权审查者按需获取；不必为了接口便利把所有原始材料传播到每个节点。

公开链上的数据尤其需要审慎选择。即使只上传摘要，若摘要对应低熵或容易猜测的个人信息、与公开标识持续关联，仍可能支持推断或匹配。加密内容放在可长期复制的链上，也不能仅凭当时无法解密就保证未来永不暴露。应先判断某项可核验需求能否由链下保存、选择性披露或受控查询满足，再决定是否上链。

保留期限应按数据类别与用途确定。身份材料、项目原始文件、分配依据、支付回执和审计日志可能具有不同期限与访问要求。期限不宜只有一个全系统默认值，应说明起算事件、延长保留的条件、到期审查与删除方式。过期数据若仍被用于新评价，也需检查是否超出原定用途。

制度中的历史请求可能要求在较长时间内保留必要证据。若参与者尚未领取已成立权益，或者仍存在真实争议，过早销毁唯一依据会损害其复核能力。另一方面，不能因为“未来可能有人争议”就无限期保存全部个人明细。可按证据重要性和开放权限分层保留，并定期检查继续保存的理由。

删除请求需要区分对象和位置。原始资料可以在满足条件时从受控存储中删除，公开账本的既有记录往往无法同样处理；因此应在设计时减少个人信息进入难以修改的共享层。对已经进入账本的记录，可在有依据时停止继续展示、取消不再必要的索引关联、修正当前状态并限制链下材料可得性，但不能向参与者保证已经发生的公开复制会随之消失。

加密、失效密钥或断开映射可以降低某些数据继续被识别的可能性，其效果仍取决于其他副本、公开关联和未来技术条件。把密钥删除称为“绝对删除”，可能夸大控制能力。组织应向相关主体解释采取了哪些措施，哪些痕迹因系统特性仍可能存在，并据此改进未来的数据收集方式。

更正需求与删除需求也不一样。贡献者指出身份归属错误时，可能更需要保留原证明并更正当前归属；对无关的私人材料则可能需要彻底移除可控副本。制度应提供可以区分两类请求的受理程序，记录决定依据并允许必要复核，而不是让技术管理员按一个“删除按钮”处理全部情况。

访问控制须随角色变化更新。项目负责人离任后，不应继续读取原项目全部个人资料；审计者完成特定任务后，也不应永久持有材料副本。权限授予与撤销、访问目的、必要日志和异常提醒共同构成使用边界。防止未经授权访问，并不意味着监督者必须被排除在所有必要证据之外；可核验监督可以通过范围受限的查验实现。

隐私与透明不是非此即彼。参与者可以了解自己的贡献依据、规则和权益结果，治理机构可以审查总量与异常，公众可以了解制度的基本安排，而不必让所有人看到每个人的薪酬、健康、客户或争议明细。衡量隐私设计是否有效，应同时看过度披露是否减少、必要的纠错和问责是否仍能进行。

四、灾难恢复、系统迁移与长期维护

持续运行意味着在事故发生后仍能恢复关键服务和制度关系。节点、云平台、身份服务、密钥保管或支付接口都可能中断；更换运营者和长期维护经费不足也可能让系统逐渐不可用。恢复方案需要面对这些原因，而不是只保留一份数据库备份。

恢复目标应由业务后果确定。何时必须让参与者重新查询请求，多久内要恢复支付，允许哪些操作短暂停止，以及在中断期间怎样受理异议，需要有明确安排。不同功能可有不同优先级：停止新增发放可能可以接受，丢失已成立请求或关闭全部申诉渠道则会给参与者带来不同性质的影响。

备份要覆盖制度所需的全部状态。账本数据、业务证据、规则文本和程序版本、身份映射、未完成操作、权限清单及外部支付回执，应能在恢复时互相核对。只有区块链节点的副本，不能重建已经丢失的合同或原始交付材料；只有业务库的备份，也可能解释不了链上状态何以变化。

恢复演练应验证可用性，而不仅检查文件存在。应能在隔离环境中读取备份，重建某项任务从业务到权益的关系，复算金额，并核对迁移后的未付请求。若演练依赖一位已经离任的工程师记住不成文的密钥和操作步骤，就说明组织还没有真正取得恢复能力。

密钥恢复尤其要兼顾连续性与控制。重要操作密钥可以采用适当的分散保管与交接程序，记录谁能在何种条件下启动恢复，以及旧权限怎样失效。过于集中的备份可能变成新的单点风险；完全没有可操作的恢复安排，则可能让正常离任或设备损坏变成永久失权。技术形式应服从已确认的授权关系。

事故期间应保留单一的业务状态判断。旧系统可能还在处理请求，新系统又可能根据备份再次执行；若两边同时支付或生成权益，同一义务就可能被重复处理。恢复程序需明确停机边界、最后可信状态、仍在途的链上与链下操作，以及何时由新系统取得唯一执行权。对结果未明的交易，应先核查实际结果再决定重试。

迁移并非仅仅复制数据。采用新的账本、合约或服务商时，需要保证身份、证据、规则版本、权益请求及历史支付之间的关系能够延续。迁移方案应说明旧记录如何验证、哪些状态映射到新系统、哪些请求仍由原义务主体履行，以及未同意迁移的参与者如何取得必要服务。旧系统停止运营不能自动消灭旧制度下的承诺。

迁移中的技术签名也不能替代组织授权。运维人员可以证明某份数据从旧系统导入新系统，是否有权改变权益内容、延长锁定或更换支付义务人，是另外的问题。重大迁移应采用有权决定，公开对比新旧结果，并为差异提供复核和纠正渠道。

长期维护需要持续的资金、人员和治理安排。合约依赖的组件可能需要更新，密钥管理与安全监测要有人承担，数据存储和审计取用也有长期成本。收益模型或业务规模变化时，应再次核对这些成本由谁支付；若仅靠一次开发预算而没有维持资源，系统最初运行成功并不能说明它可以支持跨期资本治理。

服务商替换应能实际演练。组织要能导出有权限的材料、独立核验历史状态、接通替代服务并维持必要功能。合同中写有“数据归客户所有”，如果原始证据格式不可读、签名验证依赖已停用接口，或停机期间无人接收异议，制度上的退出仍然难以实现。

对于系统最终不再适合继续运行的情形，也应提前设计结束程序。停止新任务、清理在途操作、保存必要历史、结清未了请求、通知参与者和安排后续查询，是有序退出的组成部分。系统停服可以是经营决定，权利义务是否终止仍要依据具体制度判断；不能让服务器关闭成为事实上的单方免除。

本书提出一个需要检验的方向：将安全与持续运行能力作为制度有效性的组成部分，而不是上线之后附加的技术指标。应观察故障能否被及时发现、损害能否限制、个人资料是否按用途使用、备份能否重建实际请求，以及更换系统时参与者是否仍可取得证明和救济。只有这些能力与共同创造的长期关系相匹配，制度技术才具有可持续的基础。

下一章将讨论实施路径与制度迁移，进一步说明组织怎样从制度界定和历史数据核验开始，形成一个范围有限、能够验收的运行闭环，并安排试运行、人员培训和退出条件。

定稿补强：跨攻击面的持续运行控制

持续运行需要把密码、密钥、预言机、数据、治理与恢复放进同一威胁模型。算法退役、恢复权滥用、来源同谋、隐私泄露、暂停权限失控和迁移失败可能相互放大。控制清单应记录资产、攻击者能力、依赖、检测、限制损失、恢复和责任人，而不能只列技术漏洞名称。

灾难恢复应验证的不只是服务重新启动，还包括检查点来源、历史验证环境、密钥和权限更新、链下证据可取回、子账和总账对账、临时权限撤销及受影响者通知。数据恢复也应遵守最小化、保留和删除安排；从备份恢复不能使已经到期或应删除的数据无期限复活。

本章工具与图表

本章的制度关系可结合[附录九](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

图25-1 利益相关者资本治理整体技术架构

业务、证据、规则、权益和治理分层连接；链上链下按验证价值和责任配置



《区块链——利益相关者资本论的底层技术》V1.0 · 可编辑SVG

图25-1 利益相关者资本治理整体技术架构

图25-1 利益相关者资本治理整体技术架构。业务、证据、规则、权益和治理分层连接；链上链下按验证价值和责任配置

本章注释

- [SRC-060] 美国国家标准与技术研究院（NIST）：网络安全框架 2.0。[原文或官方页面](#)
 - 本章引证：NIST：网络安全框架 2.0。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：NIST：网络安全框架 2.0。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-016] OpenZeppelin：OpenZeppelin文档：延迟操作与时间锁。[原文或官方页面](#)
 - 本章引证：OpenZeppelin：角色与访问控制。
 - 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：OpenZeppelin文档：延迟操作与时间锁、OpenZeppelin：访问控制与角色权限、OpenZeppelin：角色与访问控制。
 - 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
 - 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-076] 万维网联盟（W3C）：Verifiable Credentials Data Model v2.0。[原文或官方页面](#)
 - 本章引证：W3C：可验证凭证与数据最小化。
 - 支持范围：用于确认标准或技术规范对数据结构、验证条件、协议流程及接口语义的明文规定，本书引用主题包括：W3C：可验证凭证数据模型 2.0、W3C：可验证凭证中的选择性披露与隐私考虑、W3C：可验证凭证的参与角色与验证边界、W3C：可验证凭证的验证与业务判断、W3C：可验证凭证与数据最小化。
 - 使用边界：符合技术规范只说明相应格式或过程条件，不自动证明链下事实真实、权利合法或制度正当。
 - 证据等级：A（原始法律、正式标准、原始研究或正式规范）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第二十七章 实施路径与制度迁移

一项制度技术真正进入组织，不是因为已经部署合约或开通账户，而是因为原有业务和权利关系能够以可理解、可核验的方式进入新程序，并在运行后仍有人负责判断、履行和纠错。共同创造涉及人的贡献、持续使用的能力和不同性质的权益；这些关系不可能通过一次数据导入全部重新定义。

上一章讨论了安全、隐私和持续运行。本章把这些要求放回实施过程：先界定制度的对象与权限，再核验历史记录，选择一个能够闭合的运行范围，经过试运行验证，最后安排长期成本、人员能力和退出条件。实施路径的每一步都应有能够审查的结果；扩大规模应依赖结果，而不是依赖上线日期。

本书不预设某一家企业已经批准了相关规则，也不将现存积分、通证或草案自动当作有效的权益安排。制度迁移的任务，正是把已经存在的事实、已经成立的权利与拟议中的新规则区分开，再决定哪些关系能够被新系统承接。

一、先明确制度，再选择技术架构

实施的第一项工作，是写清楚要解决的协作问题。多方是否需要共同核验同一任务、交付和权益状态？现有单方记录在哪些地方缺乏可信的复核？争议是来自事实没有被保存、规则含糊、履行责任不清，还是来自已有系统之间不能对账？问题不同，合适的制度和技术也会不同。

制度界定至少包括主体、对象、权利义务、资源和程序。谁参与共同创造，谁承担任务，谁可以确认事实，谁评价贡献，谁有权把一类记录纳入资本安排，谁承担收益或服务义务，以及谁处理异议，都需要明确。没有这些答案，就无法判断系统中的“确认”“发放”和“完成”究竟应当产生什么效果。

尤其需要划清贡献、资本与权益之间的条件。组织可以记录某人的投入和交付，也可以评价其作用，但这不自动形成可持续的资本；资本被组织吸收并持续使用，也不自动赋予该人所有权。收益资格、治理参与和使用权要分别有依据，不能因为旧表格只有一个“积分”字段，就在新系统中把所有关系合并成一个通证余额。

每项新规则都需说明其授权来源和生效边界。业务负责人可以安排本部门试行任务记录，却未必有权改变企业对员工、供应商或客户已承担的支付义务；技术负责人可以部署测试环境，也不能因此替组织宣布新的分配制度已经生效。要先确定有权决定者、审议与通知程序、适用期间、过渡安排和申诉路径，再为其选择执行工具。

资源来源是同样重要的起点。拟向参与者分配什么、由谁提供、何时可以使用、是否已经为其他义务预留，需要在制度文本和财务处理中对齐。一个智能合约可以预设比例，却不能创造可分配利润或保证兑现资产。若资源尚未形成，系统就应把相关安排表达为有条件的资格，而不是到期必然到账的金额。

架构选择可以从四个问题进入：各方是否需要共享状态，是否存在单方记录难以解决的信任问题，规则中有多少部分能够明确表达，以及系统失败时如何恢复权利与服务。在单一组织内部已经具有可靠核算、审计和授权条件时，普通数据库或签名日志可能足够；跨组织需要共同验证控制状态与顺序时，共享账本才可能提供额外作用。选择应以可检验的收益和成本为依据。

先确定的制度问题	需要取得的证据或决定	随后才能选择的技术能力
谁对何种事实负责	任务、提交、核验和复核职责	业务接口、证据与签名方式
哪些关系具有权益效果	权利主体、义务主体、条件和期限	账户、凭证或通证形式
谁能制定和改变规则	授权、参与、门槛及生效程序	权限配置、版本和治理工具
如何履行与纠错	资源来源、支付路径、申诉和补救	合约、对账、暂停与审计功能

制度设计还应给技术能力划出边界。自动计算适合稳定、可说明的条件；事实审查和个别争议需要有人负责；系统的共享状态可帮助各方看到同一结果，却不替代不同组织的法律和合同关系。若一项设计只能通过把这些区别消除才能运行，应先重新检查制度，而不是进一步增加程序复杂度。

架构方案本身也应可替换。在正式选择前，应比较系统建设和运维成本、数据访问与隐私、升级权力、网络中断风险、证据保存及成员退出条件。所有方案都要能够说明异常时谁接收申请、谁有权暂停、谁承担数据恢复费用。技术选择是治理选择的一部分，因为它会重新配置参与者的行动能力。

最初的制度文本不穷尽未来所有场景，但必须覆盖当前准备运行的范围。可以对暂未解决的事项标注不纳入试行，保留人工程和修订入口；不能在关键权利未确定时先发行可流转凭证，寄望后续讨论自然补齐义务。受限而明确的安排，更适合成为扩展的可靠起点。

二、历史数据核验与初始权益确认

许多组织进入新系统前，已经有项目记录、绩效评价、付款清单、合同、账户余额和口头形成的协作预期。这些材料具有不同效力。迁移的目标，是让历史能够被正确理解和继续使用，而不是把所有既有数字统一改写为一种新制度下的权益。

盘点应先明确数据来源和保管状态。某条记录由谁建立，记录的是投入、交付、验收、评分、应付款还是已付款，覆盖什么期间，能否找到原始材料，以及是否曾被更正或提出异议，都需要标记。缺少来源的汇总数，可以成为查找线索，不能仅因它保存在旧系统里就成为新制度的确定事实。

主体映射必须考虑身份和代理变化。企业部门改名、员工离职、项目账户与个人账户混用，可能让同一人出现多个编号，也可能让不同主体被错误合并。迁移需要保留旧标识与新标识的对应依据、适用期间及复核人；对于无法确认的归属，应进入待核验状态，而不是为赶进度强行指定受益者。

历史贡献应按其证明范围分类。业务系统显示“已提交”，未必表示质量合格；签收单说明已收到，不一定说明成果产生了长期价值；某项评价分数可能只用于当时的绩效讨论，不自动包含未来收益的承诺。若新制度准备引用历史贡献，应说明采用哪些事实、按哪种规则重新判断，以及是否取得了相关主体对回溯处理的有效授权。

已有权利则需要另一套确认。尚未支付的工资、合同款、有条件的分配资格和已经到期的收益请求，性质不同。迁移清单应写明权利主体、义务主体、来源依据、已履行部分、剩余条件和争议状态。新系统生成一份数字凭证，可以帮助表达和核对，不能单方面改变原债务或让原义务人因旧账户关闭而免责。

对已履行记录也要核实。旧系统标为“已分配”可能只是内部核算，实际支付还需对账；已经发生的银行付款也可能尚未从权益账户扣减。若将这种差异直接导入，系统可能重复支付或漏付。迁移前应把计算、清单、指令和现实收款分别映射，再决定哪些请求仍处于未履行状态。

初始权益确认需要一个可审查的基准时点和清单。基准时点决定哪些历史事项纳入首次转换，清单说明每项请求的来源、状态和计算依据。清单应让相关主体在必要范围内查阅并提出异议，组织则需有受理、核验和修订程序。没有异议并不等于所有人已经看见清单；通知是否到达和理解是否可能，也需纳入程序评估。

对于证据不足或关系存在争议的条目，可以暂列“待核验”，同时明确调查责任、期限和不确定性对后续操作的影响。不能把待核验项目显示为已成立权益，也不能因资料缺口就悄然抹除参与者的全部历史请求。是否暂缓特定支付或转移，应有对应的制度依据与影响范围。

迁移过程应保留旧数据的原貌、清洗后的版本与决定之间的联系。修改重复记录、纠正身份归属和剔除无效评价，可以改善质量，但应记录为何修改、由谁批准，以及下游金额怎样变化。初始余额若无法追溯到来源和有效规则，就很难在运行后区分历史错误与新系统错误。

一次性“创世确认”还须防止权力集中。负责导入数据的人不宜同时独自决定疑难条目的归属、批准初始权益并操作资源转移。重要清单可以经过业务复核、权益审核和执行校验的分工，确保技术上成功写入的初始状态，具有制度上可说明的依据。

完成初始确认后，也需要保留后续纠错。历史资料可能迟到，原收款回执可能被发现有误，参与者也可能提供新证据。系统应以有依据的更正关联原条目，分别处理未付与已付结果。设置一个基准时点，是为了有序启动系统，而不是宣布所有历史争议从此不再受理。

三、最小可行系统、试运行与阶段验收

最小可行系统应选择一条确有共同需求、能够走完责任闭环的业务过程，而不是挑选最容易展示链上交易的功能。适当范围可以是限定参与者、明确任务和交付、能够取得原始证据、有权确认贡献，并且具备实际权益或反馈处理路径的一组协作。运行规模可以小，但承诺、证据、规则、结果和救济应当完整。

本书建议用“承诺、投入、交付、确认、回报、评价、修订”观察闭环。承诺说明组织和参与者各承担什么，投入与交付留下可核验事实，确认使贡献进入规则判断，回报需要资源和义务主体，评价检查结果及成本，修订则根据证据调整下一周期制度。这条链不要求每项贡献都获得相同回报，也不要求所有环节自动化；它要求每次转换能解释。

最初版本应缩小制度和技術变量。只选择少数明确的贡献类型与权益安排，限制可以自动执行的条件，把有争议或事实难以验证的事项保留给人工审查。若先同时引入复杂通证流转、多层激励、跨企业结算和持续变化的权重，试运行出现问题时难以辨认究竟是哪一项安排失效。

试运行可以先经历无经济后果的影子计算。用真实业务资料在受控条件下验证身份映射、证据流转、规则复算和账本状态，不立即根据计算结果支付或发行可流转凭证。影子结果要与现行业务记录对照，列出差异原因。只有相关主体看得懂差异，才有条件决定是否让结果承担正式作用。

接下来可以让有限的正式任务进入新程序，同时保留必要的人工作业和对账。对于成立的请求，执行路径、支付资源和应急操作应当事先就绪；对未满足条件的事项，则如实显示待核验或待决定。试运行不应把全部参与者当作接受尚未成形制度的测试对象。哪些安排仍为试验，哪些已经对特定主体有效，要能够明确区分。

阶段验收应采用事先确定的观察项目。身份和授权是否准确，原始证据能否找到，计算是否可复现，权益是否有对应义务主体，支付是否能够与链下结果对账，异议是否在约定期限内得到答复，数据是否按权限访问，系统中断后能否恢复，都应有相应责任人和验收材料。界面运行流畅，只能覆盖其中一部分。

阶段	必须形成的结果	未满足时应采取的行动
制度准备	有效的参与、权利、资源和申诉边界	继续审议，不将试算结果当作权益
数据准备	可追溯的初始清单和待核验条目	补证、分开处理争议与无争议部分
影子运行	可复算流程与差异报告	修正数据或规则后重新演练
有限正式运行	可履行请求、对账与异常处置	限制新增范围并处理未了事项
扩展审查	效果、成本、参与和纠错证据	决定扩展、调整、维持或结束

验收不能只由建设团队自评。业务负责人可以核对事实与服务结果，财务人员核对资源和支付，权益或治理负责人检查授权与申诉，技术人员报告系统行为；受影响参与者的实际使用反馈也应进入判断。必要的独立复核应能看见原始记录和差异，而不是只阅读团队总结的成功率。

出现严重偏差时，试点应能暂停扩大、限制有风险操作，并把已经成立的请求继续纳入处理。回退不是把数据库恢复到较早日期就算完成；它还要检查这段时间内发生了哪些链上转移、链下支付和对外承诺。哪部分可以恢复，哪部分需要新的补救决定，应分别说明。

阶段通过后也不自动证明区块链优于其他方案。试运行可以证明特定条件下的记录一致性、复算与履行是否达到预先要求，却还需要与其他可行工具比较成本、速度和治理质量。若协作问题主要由制度不明确引起，即使系统改进了留痕，也可能无法改善共同决策。下一章将专门讨论这些效果怎样检验。

扩展范围时，应一次增加可解释的变化。可以先增加参与类别，再增加跨组织任务；或者先稳定内部权益对账，再引入可转移数字凭证。每一步都应核对旧规则是否仍适用、资源是否足以履行新增承诺、人员能否处理更多异议。扩展不是复制成功界面，而是复制已经被证明能够承担责任的制度关系。

四、成本承担、人员培训与退出安排

实施成本不止于开发和部署。业务梳理、证据核验、历史数据清理、身份管理、程序审查、接口维护、节点或服务费用、财务对账、争议处理、备份与迁移，都会持续消耗资源。预算应区分一次性建设与长期运营，说明费用承担者、受益者和资源来源，避免通过发放数字单位把真实成本暂时隐藏。

成本分配需要与控制权和收益相联系。某个平台要求成员企业承担验证费用，却由平台单独掌握升级权与数据出口，应解释这种安排是否合理；组织要员工无偿完成额外的证据录入和治理工作，也应检查新增负担是否与原有承诺相符。技术减少某个部门的工作，可能同时把工作转移给参与者或合作方，不能只按系统运营者的支出评价总成本。

培训应围绕不同角色的实际决定。参与者需要知道怎样提交证据、查看结果、提出异议和安全保管操作凭证；核验者需要理解每种材料能证明什么；审批者应知道权限范围和利益冲突规则；财务人员需要能区分内部余额、应付款与实际收款；技术人员则必须能够解释版本、权限与异常状态。用一场面向全员的“区块链原理”讲座，难以替代这些岗位训练。

培训还需要让人知道什么时候停下来。遇到资料不一致、重复请求、身份无法确定或收款结果未明时，经办者应知道如何标注、通知与转交，而不是为了维持自动流程把未知填写为“通过”。通过演练具体异常，比背诵正常操作步骤更能发现制度和界面之间的断裂。

可达性应进入培训和产品安排。不是每位贡献者都持有同样的设备、语言能力或数字经验。必要的授权代理、替代提交与人工支持，可以帮助不同参与者行使已成立的权利；这些通道同样需要记录身份、权限和操作结果，防止“线下协助”成为不受审计的例外。

实施期间要明确沟通责任。参与者应能知道旧流程何时停止，新流程何时对哪些事项生效，旧权益怎样继续查询，以及提交问题后从哪里获得回应。公告一次不足以证明所有受影响者已经理解变化；对于将改变实际请求或履行路径的事项，需要更明确的通知与反馈渠道。

退出安排应在系统上线前准备。试运行可能被终止，供应商可能停止服务，成员企业也可能退出合作。组织应决定如何停止新任务、处理在途操作、导出有权限的材料、保留证据、核对未付请求和移交申诉渠道。技术服务结束不能自动结束已经成立的权利义务，尤其不能让没有系统管理权限的人承担信息消失的后果。

退出的成本也要提前说明。迁移数据、继续验证历史凭证、维护最低限度的查询和支付服务，可能需要持续费用。若退出后只能支付高额费用才能取得自己的证据，所谓可退出便缺乏实际内容。费用标准、保存期限和替代承接者，应在关系尚能协商时形成清楚安排。

制度迁移也可能需要渐进停止旧程序。旧系统可在限定期间继续处理旧请求，新系统处理新任务，但两边不能同时独立发放同一项权益或支付同一义务。应指定唯一有效的执行来源，保留双方的对照记录，并在切换完成后核对尚未关闭的请求。历史可查询与旧系统继续决定新权益，是两回事。

本书提出一个需要检验的实施原则：每次扩大技术能力之前，先证明该能力所承载的制度关系已经能够被理解、复核、履行和纠正。若系统只能展示贡献分数，尚不能说明资本形成和权利依据，就继续完善证据与判断程序；若已能确认权益，但无法处理支付差异，就先完成对账能力。这样的推进可能不够迅速，却能使扩展建立在真实的责任能力上。

实施成功不是上线后也不需要修改，而是组织拥有了持续学习的程序。它能看见共同创造中的事实，承认计量和制度选择的边界，依据经验修订规则，并在必要时换用更合适的工具。制度技术由此成为组织能力的一部分，而不是一次性的软件项目。

下一章将讨论如何检验区块链对资本治理的真实作用。资产转移是否可靠、协作成本是否下降、治理质量是否改善，以及这些效果是否确由区块链而非其他制度改变带来，都需要进一步用可比较的证据回答。

第二十八章 如何检验区块链对资本治理的真实作用

本书把区块链理解为一种可以承载部分制度安排的技术。这个判断若要超出概念解释，就需要接受经验检验：共同账本是否使资产控制转移更可靠，是否降低多方协作中的核验成本，是否让贡献、权益与治理关系更清楚，最后是否改善共同创造的持续能力。仅凭系统上线、交易数增加或通证出现价格，不能回答这些问题。

上一章提出了从制度界定到阶段验收的实施路径。本章进一步把验收转化为可比较的研究设计。需要预先确定研究对象、结果指标、观察期间、对照方案和失败条件，并如实记录制度与技术同时变化的部分。这样，即使某个试点没有达到预期，也能知道是工具选择不适合、规则设计不足，还是组织尚未具备必要条件。

本书不把单一案例的成功宣传为普遍规律，也不因为某次实施失败便否定所有区块链用途。技术效果、制度效果与经营效果处在不同层次；一项系统可能在其中一个层次取得改进，却在另一个层次没有明显作用。只有把层次与边界区分清楚，研究才可能持续推进。

一、资产转移可靠性、协作成本与治理质量的评价

评价应先定义“可靠”指什么。对于链上原生资产，可以观察经有效授权的转移是否在既定规则下正确完成、重复支出是否被拒绝、交易在适用时间内是否达到预期最终性，以及异常发生后能否核验和恢复。对于现实资产的数字映射，还需另查链下对象、登记或交付与链上状态是否对应。协议上的控制转移成功，并不自动证明现实权利已经转移。

可靠性不能只看成功交易占比。被错误拒绝的合法请求、未经授权却被接受的操作、错付后迟迟无法更正的结果，也属于系统质量。需要说明观察单位和分母：是每笔提交、每项有效请求，还是每笔最终履行的义务；重试和批量交易应如何计数。没有分母与状态定义，“99%成功率”可能掩盖参与者真正遭遇的问题。

可用性同样进入可靠性评价。参与者能否取得必要凭证、提出异议和领取已成立请求，不能仅靠节点正常运行率表示。应记录业务流程中断的持续时间、受影响人数、未履行请求数量与恢复后的核对结果。系统稳定运行但现实支付接口长期不可用，在参与者看来仍是不可靠的安排。

协作成本要覆盖完整过程。原有方式下，各方需要多少次对账、重复录入、补证与争议处理；引入共同账本后，这些成本是否减少？同时还要计入合约开发、身份核验、节点维护、密钥保管、隐私处理、人员培训和技术迁移。把企业内部工作转移给供应商或个人参与者，不应记作生态总成本的消失。

成本既有货币部分，也有时间和权力部分。等待交付确认的天数、从异议提出到得到理由答复的时间，可以反映流程负担；受限于某平台独有接口、必须依赖少数密钥持有人，虽然短期费用不高，也会增加退出成本和未来谈判的不对等。评价应说明成本由谁承担、谁获得效率收益，避免只报告平台运营者的账面支出。

治理质量比交易数量难以测量，却不能因此省略。应观察受影响主体是否及时获知规则，能否提出议题，代表与委托是否真实有效，决定是否明确理由，少数意见和利益冲突是否得到处理，执行是否遵守授权，以及申诉后是否存在可见的纠正。投票数、参与账户数和提案数只是程序活动量，不能单独证明治理更正当或更有效。

还应关注共同创造是否持续。被确认的贡献是否转化为组织能跨期使用的资源、能力和合作关系，参与者是否愿意继续承担有价值的任务，兑现是否可靠，以及维护性工作有没有因单纯追求可计数行为而被挤压。资本形成不能以“发了多少凭证”替代，企业价值也不能以通证市场价格替代。

评价维度	可观察的证据	需要防止的误读
转移可靠性	授权结果、错误接受或拒绝、最终性与恢复	链上成功即法律权利完整变动
协作成本	全流程时间、核验次数、费用与退出成本	成本转嫁后被当作节约
治理质量	知情、代表、理由、执行和救济结果	投票活跃即制度正当
长期能力	持续交付、资源吸收和关系维持	积分或通证数量即形成资本

指标还需要适当分组。大组织与小组织、拥有数字工具与缺少工具的参与者、承担高风险与低风险任务的主体，可能经历不同效果。总体平均时间下降，不代表少数群体的申诉更容易；平台费用下降，也可能伴随合作方被迫承担更多审核工作。分组结果帮助发现效率收益和制度负担的分配。

在正式评估前，应确定数据如何取得及谁有权复核。链上数据能证明某些操作顺序和状态，不能直接告诉研究者原交付是否真实、客户是否获得服务或合同是否履行。评价需要结合业务资料、财务对账、访谈或申诉记录，同时在数据使用中保护个人和商业信息。证据的可信程度应随来源和核验方式说明。

最终要把结果与预先提出的命题对应。如果目标是减少跨组织对账争议，却只测到链上吞吐量提高，仍未检验原命题；如果声称参与者更有发言权，却只统计了通证持有人投票，则遗漏了没有通证但受到决定影响的人。可解释的评价始于目标与指标的对应，而不是从容易获取的数据倒推希望得到的结论。

二、与非区块链方案进行同条件比较

声称“区块链带来改进”，需要有可信的对照。如果旧系统缺少清楚规则、身份核验与申诉程序，而新系统同时增加了这些安排，效果可能来自制度改进本身。比较对象应包括经过合理改造的中心化数据库、签名日志或多方定期对账方案，而不是故意保留缺陷的旧流程。

同条件比较需要尽量固定业务任务、参与主体、有效规则、证据要求、观察期间和服务目标。不同方案可以选择各自合适的实现方式，但应承担同样的授权、纠错和隐私责任。若链上方案获得额外预算和专人培训，对照方案却无相应支持，则差异不能仅归因于技术结构。

一个有用的比较可以分出两种变化：仅改善制度与流程，和在相同制度基础上进一步引入共享账本。前者告诉我们规则清晰、职责分离和对账机制本身产生了什么效果；后者才有机会识别分布式共同验证的增量价值。这是研究设计上的分层，并不要求每个组织在现实中同时部署四套完整系统。

观察前后变化可以作为起点，但不能直接给出因果结论。业务规模、参与者构成、经济环境和管理者经验都可能同时变化。世界银行与美洲开发银行的《影响评估实务》强调使用可信的对照和反事实分析，避免把本来会发生的变化归因于项目。本书借此提醒：上线前后指标不同，只能提出进一步调查的线索。世界银行与美洲开发银行：《影响评估实务》〔1〕

若有条件在相似任务之间分阶段采用新系统，可以比较先行与后行单位的变化，并检查采用前的差异及其他同时发生的政策变化。若有条件随机分配某些低风险的操作路径，也需要确保参与者的既有权利、重要履行和救济不因研究而受到不当影响。实验方法可以提高识别能力，却不能替代组织对参与者的责任。

无法开展严格实验时，可以使用平行记录、影子计算、历史流程重建和相似组织比较，明确哪些因素无法控制。比较结果应附上限制条件：成员为何选择参与，哪些任务因难度不同而进入不同方案，哪些费用未能充分估算，以及小规模试行的效果能否延续到长期运行。证据有限时，结论也应保持有限。

还应防止把分布式系统的成本藏在其他组织账上。多个节点各自承担设备与人员成本，可能换来更强的共同核验和退出能力；如果这些能力实际并未被使用，额外开销就缺少对应收益。反过来，单一数据库表面成本低，却依赖中心运营者解决所有争议、批准所有访问，也可能产生难以看见的制度成本。两边都要记录真实控制结构。

对照还要覆盖极端条件。正常交易量下，两种方案都可能顺利运行；在节点断连、合作方退出、管理员失联、错误输入被确认后，能否维持历史证据和已成立请求，可能出现重要差别。应设计可重复的故障演练，并按相同恢复目标评价，不宜只比较理想状态下的平均处理速度。

研究对象可以是“一项任务从承诺到结算的全流程”，而不是单独的一次写入。这样才能看到某项技术减少了手工对账，却可能增加身份管理或争议处理；也才能观察参与者是否得到更稳定的权利解释。可比较的单位确定以后，指标和成本才有同一尺度。

同条件比较并不是预设区块链必胜，而是决定何时值得使用它。若经过清楚设计的签名日志已经足以满足共同核验，且成本更低，制度设计者应接受这一结果；若多方确有不能委托单一运营者的状态确认需求，分布式账本的额外成本可能有可说明的价值。技术选择因此成为可以被证据修正的判断。

三、技术效果、制度效果与经营效果的区分

技术效果回答系统能否在设定条件下正确运行。签名核验是否可靠，重复支出是否被拒绝，共享状态是否及时形成，记录能否在参与方之间保持一致，服务中断后是否能恢复，都属于这一层。美国国家标准与技术研究院将区块链描述为具有篡改可见性与抗篡改特征的分布式账本；这

说明其记录机制具备特定技术能力，却不能单独证明任何企业的贡献判断或分配决定正确。NIST：区块链技术概述〔2〕

制度效果回答技术是否使有效规则得到更清楚的表达与履行。不同角色能否识别自身的权限，贡献证据是否经适当确认，权益是否指向明确义务主体，规则改变是否经过授权，错付是否能追查并补救，都是这一层的观察对象。制度效果可能借助技术得到改善，也可能因为原规则不公平、监督不足而没有改善。

经营效果则关注组织是否创造和维持更有用的能力。协作是否更稳定，质量是否改善，必要资源是否得到持续投入，客户是否获得有价值的服务，组织是否具备履行长期承诺的能力，都需要经营与财务资料支持。经营成果也受市场需求、管理能力、资金条件和其他技术影响，不能从链上活动量直接推出。

三层之间可能存在机制链：可靠的共同状态降低争议与重复核验，较好的证据和规则执行提高协作可信度，可信协作帮助资源、能力与关系跨期积累，最后在一定条件下改善经营成果。这条链的每一环都需要观察；任何一环断裂，后续结果就不能沿着预设故事自动发生。

例如，交易最终性提高可以减少同一链上的重复支付风险，却未必减少业务事实争议；贡献确认变得迅速，可以减轻等待，却可能因核验仓促增加虚报；权益分配透明，可以提高理解，也可能在资源不足时把未能履行的承诺更清楚地暴露出来。某一指标改善有实际意义，但不能直接被升级为全部层面的成功。

资本形成尤其需要较长观察期。项目结束后留存的知识、可重复使用的工具、稳定的协作关系和承担未来风险的组织能力，不会在一次发币或一季度的参与数据中完整显现。评价应预先确定观察窗口，辨别暂时活动与跨期能力，并说明窗口过短时不能作出的结论。

市场价格也应放在正确位置。通证价格可能反映市场预期，也可能受流动性、供给、投机和交易条件影响；它既不等于参与者的实际可得回报，也不等于企业价值。若本书研究的是利益相关者资本治理，就应把实际贡献、权益履行和持续经营与交易价格分别记录，检查它们是否存在可说明的联系。

研究还要留意负向效果。共享记录可能提高可审计性，也可能扩大个人数据暴露；自动执行可能提高一致性，也可能使规则错误迅速影响更多人；通证化可能强化某些激励，也可能把长期合作转成追逐短期价格。制度评价需要同时报告受益与损害，不能把不利结果统统归入“实施不够完善”而不进入结论。

责任归属是区分三层效果的另一条线。协议验证一项交易、组织承认某种事实、义务主体完成支付，分别由不同机制和主体支撑。即使最终履行成功，研究也应查明它依赖了多少人工补救；即使链上操作失败，仍可能通过有效的链下程序维护参与者请求。只看最后余额，会错失制度真正起作用或失效的位置。

若某项试点同时修改贡献标准、增加员工代表、换用账本和重新设计收益安排，评价结果只能初步说明“整体改革”的效果。要归因于区块链，需要观察它相对于其他变化的独立贡献。做不到时，应明确写出证据界限，而不是为了形成单一结论忽略同时发生的改革。

技术、制度与经营三层最终应形成一份可复核的结果图：每层提出何种命题、使用何种证据、发现何种变化、仍有哪些替代解释。研究的价值不在于必然得出肯定结论，而在于使未来的建设者知道哪些条件值得保留、哪些因果关系还没有被证明。

四、失败条件、适用范围与后续研究命题

一本提出制度技术命题的书，应当说明什么观察会使自己的判断受到挑战。若在同样的规则和审计条件下，区块链方案对资产转移的错误处理、跨方核验成本和退出能力没有可辨认改善，却带来更高的持续费用或更强的权限集中，就不能继续宣称其对该场景具有额外制度价值。研究应允许“无需使用区块链”成为严肃结论。

另一些失败来自更早的制度前提。各方未就证据标准达成一致、权利义务没有明确、资源不足以支持回报，或者少数主体控制全部参数，区块链都难以通过自身机制补齐。此时说“系统还需要更多用户”或“再提高交易速度”并未对准原因；应先改变制度安排或缩小应用范围。

还应识别安全和隐私边界。若个人资料必须被广泛公开才能运行，若管理密钥失陷便会不可恢复地改写大量权益，若参与者无法在退出平台时保留对历史请求的证明，那么技术所增加的可核验性可能不足以抵消新风险。适用性判断要把这些影响与正常运行时的效率一起计入。

适用范围可以按关系结构描述。多方长期协作、彼此需要核验同一资产或权益状态、难以接受单方随意改写记录，且有能力共同承担网络、证据和治理成本时，区块链较有可能提供额外价值。若主要是单一企业内部的记录管理、事实来源高度依赖唯一机构，或者组织尚无法界定权益内容，则其他工具可能更合适。这些是待检验的条件，而非普遍有效的使用清单。

研究命题应具体到能被反驳。第一，若共享账本确有作用，在控制规则与参与者构成后，多方之间对同一权益状态的核对时间与争议率应下降；若没有下降，则要查明账本是否缺少共同认可的输入。第二，若制度执行更透明，参与者对资格和分配结果的理解、可申诉性与纠错速度应改善；若只是记录变多而解释能力没有提高，则不能认为治理质量提升。

第三，若贡献记录有助于形成长期资本，应能在足够期间观察到资源复用、能力持续和协作关系稳定，而不是只有提交事件或奖励次数增加。

第四，若通证机制承担明确制度功能，它相对于普通账户或数字凭证应在流转、互认或履行方面产生可辨认的增益；若主要变化只是产生市场交易价格，则不应将这种价格直接归因于共同创造的改善。

这些命题还需要反例。多组织协作可能因共同账本降低对账争议，却因治理门槛过高延误必要决策；一项贡献机制可能提高参与率，却排挤难以量化的维护工作。研究应保存这种混合结果，说明效益在何处出现、代价由谁承担，以及修订制度后效果是否仍然存在。

后续研究可以从比较不同权力结构入手。同样使用共享账本，节点、数据输入、提案和升级权限分布不同，制度效果可能相差很大。单纯比较“链上”与“链下”会遗漏更关键的治理变量。应研究哪些权限配置真正支持共同验证与有效纠错，哪些只是在技术上分布、在组织上重新集中。

还可以研究不同时间尺度。短期内可能观察到对账效率，较长时期才看得到资本形成、承诺履行与退出能力。研究设计应同时记录短期操作指标和较长周期的组织结果，防止用容易取得的即时数据替代重要但缓慢出现的效果。

任何未来命题都应保留证明责任。本书关于可编程权利义务、可组合制度和可演化治理的设想，尚需具体制度设计、工程实现与独立经验验证。提出研究方向，不等于已经证明其原创优先权、普遍适用性或实践效果。能够明确指出尚未被验证的条件，本身就是制度技术研究走向成熟的一部分。

至此，本书完成了从制度技术到系统构建的论证，并把自己的中心主张交给可比较的证据检验。区块链若要成为利益相关者资本治理的技术基础，必须在特定条件下改善共同状态的确认和有效规则的执行，并让这种改善最终有助于权利兑现与共同创造的持续能力。若做不到，应诚实修订主张或选择更合适的制度工具。

下一篇将进入未来制度的讨论。第二十九章从资产控制转移出发，进一步考察权利义务怎样随贡献、责任、风险和时间变化，同时保留清楚的授权、稳定预期与救济边界。

定稿补强：工作负载、总拥有成本与可比口径

技术比较必须固定工作负载和故障条件。报告应说明数据规模、交易结构、并发、节点分布、隐私要求和观察期间，同时报告中位数、P95/P99延迟、错误率、网络分区、节点故障、冷启动、恢复时间和重复试验。平均吞吐量不能代表拥堵和故障中的真实体验。

成本比较应覆盖建设、基础设施、密钥和身份、预言机、合规、审计、治理、升级、故障、迁移、培训和机会成本，采用适合项目周期的总拥有成本模型。不同方案使用相同功能单位、期间、规模、币种、汇率与通胀基准；长期比较说明折现方法，并对关键参数做情景和敏感性分析。

效果和成本都要标记数据质量。缺少同条件数据时，可以形成待验证假设，不能来自不同规模、不同时间或不同合规要求的数字得出确定优劣。第二十八章的任务，是使技术效果、制度效果和经营效果分别接受反证。

本章工具与图表

本章的制度关系可结合[附录二](#)、[附录十](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

图28-1 区块链与非区块链方案的同条件评价

先固定制度目标、参与者和工作量，再比较技术、制度与经营效果

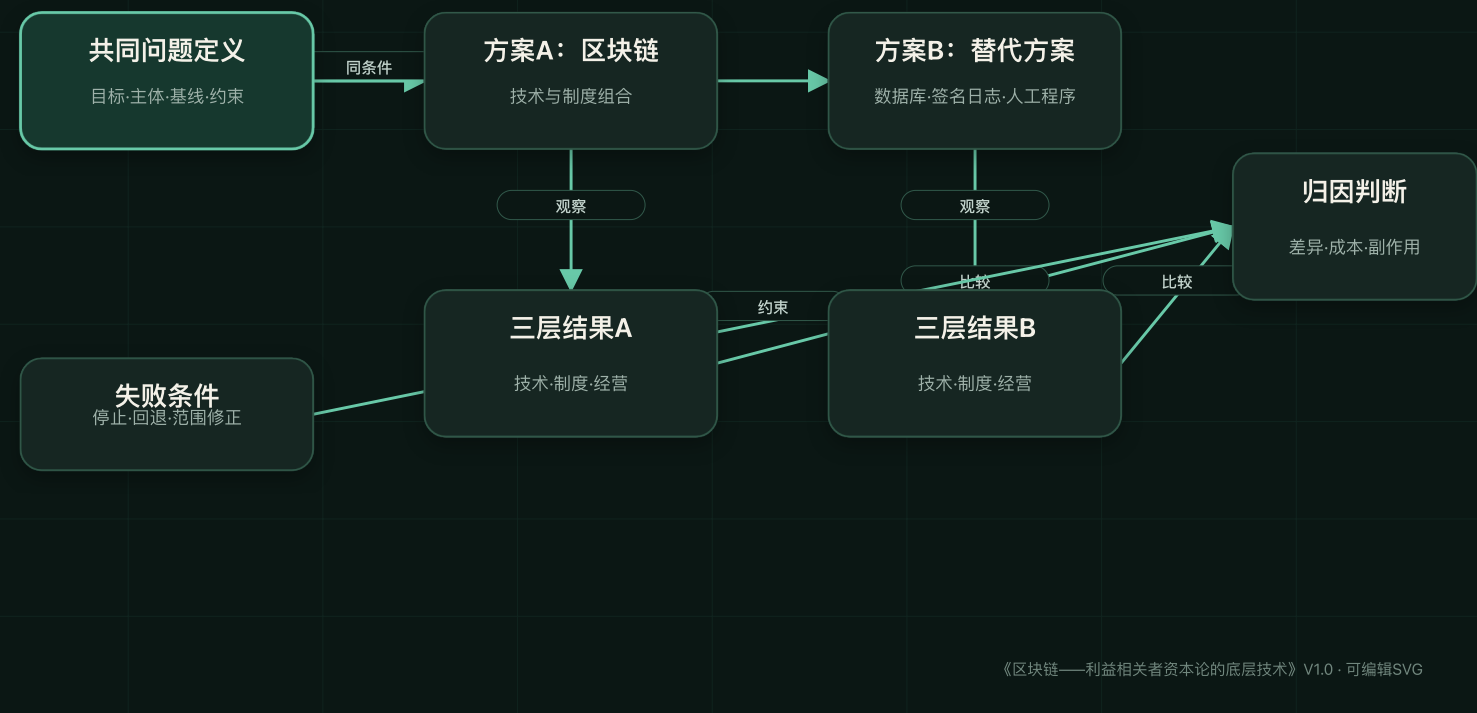


图28-1 区块链与非区块链方案的同条件评价

图28-1 区块链与非区块链方案的同条件评价。先固定制度目标、参与者和工作量，再比较技术、制度与经营效果

本章注释

- [SRC-077] 世界银行：Impact Evaluation in Practice。[原文或官方页面](#)
 - 本章引证：世界银行与美洲开发银行：《影响评估实务》。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：世界银行与美洲开发银行：《影响评估实务》。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-078] 美国国家标准与技术研究院（NIST）：Blockchain Technology Overview（NIST IR 8202）。[原文或官方页面](#)
 - 本章引证：NIST：区块链技术概述。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：NIST IR 8202：第7.3节、NIST IR 8202：第8.1节、NIST：区块链技术概述。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第七篇 未来制度：从可 编程资产到可演化的共同 创造秩序

第二十九章 从资产转移到可编程的权利义务关系

区块链最容易被看见的能力，是让一项数字资产的控制状态从一个地址转向另一个地址。然而，利益相关者资本治理面对的并不只是“谁持有一个东西”。共同创造会持续发生：贡献需要核验，组织承担兑现责任，参与者承担约定风险，既有成果随时间投入生产，新的事实又可能改变未来的合作条件。一个静态余额无法充分表达这些关系。

因此，本章提出一个有待设计和检验的方向：在有效的制度授权下，把部分权利义务关系表示为可核验、可执行、可修订的状态。所谓“可编程”，不是把人的判断交给代码，也不是凭一次技术部署创造法律上的权利；它指已经形成的规则可以规定事实怎样进入程序、条件怎样触发、哪些状态可以变动、谁负责履行以及错误如何救济。技术能够提高执行的一致性，但权利的正当来源、链下事实和争议裁决仍要由相应的组织制度承担。

这里必须坚持本书已经建立的区分：贡献记录不自动成为资本，资本记录不自动产生所有权，收益请求不自动附带治理权。可编程关系的价值，恰恰是把这些不同层次分别表达，再说明它们在何种条件下发生联系。

一、权利如何随贡献、责任、风险与时间改变

权利的变化，首先要回答“变化的是什么”。一份交付通过确认，可以使尚待核验的贡献变为已确认的贡献；它未必同时使报酬到期、资本形成或表决资格成立。某项收益请求可能已经成立，但支付日期尚未到来；治理资格可能因任期届满而终止，既已取得的报酬请求却依然存在。把这些状态压成一个可升可降的“权益分数”，既掩盖责任归属，也容易使参与者无从预期。

制度设计可以对每项关系记载权利主体、对应义务主体、标的与范围、取得依据、触发条件、证据来源、生效时间、有效期限、可转让性和救济路径。技术记录的是这些要素的当前状态及其变更依据，而不是给每个人贴上一项无条件的“价值”。同一人可在不同任务中同时处于贡献者、审查者或收益领取者的位置；同一项成果也可能对应多个主体的不同请求。

贡献改变关系，须经过预先说明的确认程序。投入工时、提交成果、成果被使用以及产生经营结果，是不同事实。制度可以约定交付被接受时产生固定报酬，持续使用达到条件时产生后续收益，或者只有组织吸收某项能力并承担相应义务后才进入资本记录。每种安排都需要说明证据、确认者和异议期。不能因贡献容易被链上记录，就推断所有记录均具有相同的经济意义。

责任也会使权利的行使方式变化。担任项目负责人可能附带审批权限、保密义务和对超出权限行为的说明责任；职责解除后，未来审批权限应停止，但此前依法依约完成的劳动或交付不应因此被一并抹去。责任与权利的关联应限于具体职务和事项：没有事先约定和适当程序，不能凭事后评价任意扣减已确认请求。

风险的处理尤其需要克制。承担资金损失、质量担保或履约延期风险的人，可能要求相应回报、风险准备或退出条件；但“共同承担风险”不是把企业经营失败自动分摊给所有贡献者。应区分自愿承担的、可识别的风险与无法由个人控制的系统性风险，明确承担上限、期限、信息取得权及补偿规则。若风险状态由外部数据触发，还要说明数据提供者、复核权与错误输入的纠正办法。

时间可以影响归属，却不应成为含混的剥夺工具。持续服务、分期交付和长期合作可以对应不同的归属进度；归属前的期待与归属后的请求，在稳定性上应受到不同对待。对于已经完成的贡献，是否仍须经过等待期才能行使收益权，应在事前清楚约定。既有请求与未来资格不能只因系统内同属一个账户，就被同一个“离开组织”按钮同时清零。

由此可形成多维状态模型：贡献事实有“待核验—已确认—已修订”，收益请求有“附条件—已归属—到期—已履行”，治理资格有“申请—有效—暂停—终止”。这些状态并非必须排成一条统一的升级阶梯。每次转换都应保留对应证据、规则版本、确认或批准主体，以及变动前后的结果。这样的记录能帮助参与者理解“为什么变”，也为审计和纠错留下依据。

二、收益、治理、使用与退出条件的分别编排

“获得一份权益”在口语中方便，在制度中却过于笼统。收益权回答可以请求什么经济给付、由谁给付、何时到期以及给付来源；治理权回答谁能提出、审议、表决或监督哪些事项；使用权回答谁能在何种范围内接触资源、数据或基础设施；退出权回答如何结束参与、结清既有请求并处理仍在持续的义务。四者的标的、相对方和生效条件并不相同。

收益规则需要把“有资格参与分配”与“已有确定金额可请求”分开。前者可能取决于年度可分配资源、预定计算方法和身份条件；后者还需经过核算、批准及到期等环节。可以预先编排计算周期、资格快照、扣除事项、对账和支付顺序，但账本中的计算结果仍应与真实资金和有权负责的主体相对应。没有可分配资源时，程序不能凭记账动作制造兑现能力。

治理权更不能由收益权机械推导。治理资格可以依据成员身份、任职关系、代表授权或风险承担确定，并按事项配置提案、表决、回避和复核权限。某人获得收益，并不意味着自动取得企业全部决策权；某人不再承担职务，也不意味着他已形成的收益请求消失。治理程序可把通知期、法定或约定门槛、利益冲突申报、委托有效期编排到执行流程中，但谁有权制定和修改这些程序，仍是先于代码的制度问题。

使用权通常与任务、保密和容量相连。供应商为完成交付取得某些数据接口的限期访问权限，与获得该数据的所有权不同。使用范围应按最小必要原则界定：用途、对象、次数、期限、再授权条件和停止访问的触发事实均可分别规定。权限到期可以由系统关闭入口，但已取得的数据副本、持续保密义务和违法滥用的责任，不会因关闭入口自动消失。

退出是检验制度是否公平的关键场景。退出可以停止未来贡献资格、解除尚未开始的任务或结束受托治理权限；对退出前已确认的贡献、已归属但尚未支付的收益和未完成的保密、担保、纠错义务，则应逐项清算。合理的制度应说明提前通知、交接、估值或结算方式、支付期限、争议期间的临时安排，以及参与者获取自己记录的方式。若系统只能将一个地址“停用”，却不能生成清楚的结算说明，所谓可编程退出并未真正实现。

技术上可以把权利编排为条件与状态转换，但制度上还必须区分三种事件：事前约定条件自然成就，具有权限的人依程序作出决定，以及对既有记录的错误进行更正。第一种可以有较高的自动化程度；第二种需要可核验的授权和理由；第三种还需要保留原记录、标明冲正依据并处理已发生的履行。把三者混为“合约自动执行”，会隐藏重要的裁量和责任。

分期归属是一个直观例子。OpenZeppelin 的 VestingWallet 文档〔1〕展示了按时间表释放资金的技术机制，同时提示合约所有权可能被转移。这说明时间条件可以由程序实现，却不意味着受益人身份、基础权利的可转让性或现实中的给付义务也由程序自动决定。制度须另行约定并核验这些问题。

三、可转让权益与不可转让关系的协同

资产可以转移，不等于围绕资产形成的一切关系都随之转移。一笔已经确定的应收款，在适用规则允许且满足通知或同意等条件时，可以由新主体请求履行；产生这笔请求的历史贡献仍属于原贡献者。某个成员的个人信誉、审议经历或受托代表身份，也不会因转让收益凭证而成为受让人的履历。可编程治理必须允许“权益的某一部分变化”，同时保留“关系的其余部分不变”。

判断一项权益能否转让，至少要依次问：转移的究竟是收款请求、使用许可、治理资格，还是包含多种内容的组合；谁是履行义务人；原安排是否允许转移、是否要求同意或通知；受让人需要具备何种资格；原主体的未履行义务是否继续存在。若只设计一个可发送的通证，却没有回答这些问题，链上持有人变化最多表明技术控制状态变化，不能独自说明全部权利义务已变动。

不可转让也有不同理由。有的关系基于个人身份、专业资格或代表信任；有的访问权限仅为执行特定任务；有的贡献记录是对历史事实的署名。它们可以被证明、撤销资格或更正错误，却不适宜像无记名资产那样随意交易。另一方面，“不可转让”不应变成永不纠错。主体失去密钥、更换合法代表、组织合并或身份信息被误记时，应有经授权的恢复与更新程序，并保留连续的责任记录。

第十九章已经讨论身份绑定通证及其转移限制。把某项凭证在协议接口上锁定，只能限制合约所定义的转移操作，不能证明持有人身份真实、没有代持安排，或相关经济利益绝无其他转让路径。相反，可转让的凭证也不能单凭程序设计保证受让人取得所有现实权利。技术状态与制度关系之间需要持续核对。

因此，较稳妥的表达不是为每个人铸造一个包含全部权利的“身份通证”，而是为不同关系设置各自的记录和变更条件：历史贡献与确认者相连；收益请求与权利人、义务人和给付条件相连；治理资格与角色及授权期限相连；访问权限与具体用途相连。需要转移时，只移动允许转移的部分，并在关联记录中说明原权利人、新权利人、变更依据、通知结果和仍由谁承担既有义务。

这种拆分还应防止以形式上的“不转让”掩盖实质控制变化。若持有不可转让凭证的账户由他人实际控制，或可转让的载体把收益与投票权重重新打包，制度设计原本保护的身份关联就可能落空。核验不能只看合约能否执行某个函数，还要观察托管、代理、授权委托和链下合同怎样改变实际控制。相应的治理规则可以要求披露、限制特定委托或设置利益冲突处理程序，但必须说明执行成本和隐私边界。

四、动态权益的预期稳定、变更授权与救济

如果权利随事实和时间变化，参与者首先需要知道自己在何种条件下会得到什么、失去什么。动态权益不是让组织拥有随时改写承诺的自由，而是把可预见的变化写入清楚的条件。应特别区分“按照既定公式输入了新事实”与“有人修改了公式”：前者属于原有安排的履行，后者可能改变原安排本身，必须接受更严格的授权和程序审查。

预期稳定要求规则在参与者作出投入之前可获得、可理解，并有明确的生效时间。系统应保存规则版本及其适用范围：某项贡献适用交付时的规则，还是确认时的规则；某次分配适用周期开始时的资格，还是支付时的资格；跨版本任务如何过渡。版本选择应由事前规则确定，不能等结果出现后再选择对一方有利的版本。尤其对于已经归属或到期的请求，若拟作不利变更，应明确其依据、授权范围和可能需要的个别同意；不能靠一次合约升级悄悄追溯改变。

规则变更的授权应与影响范围相匹配。日常参数调整可以交给限定权限的运营者；改变收益计算方法、治理资格或退出清算方式，则可能需要更广泛的提案、审议、通知和表决。利益冲突中的决策者应回避，受明显不利影响的群体应有表达和申诉机会。授权不只是链上多签人数达标，还包括有权主体、议题范围、程序期限和法律或章程约束是否满足。

异常情况下可能必须暂停自动执行，例如外部数据显著错误或合约漏洞正在造成损失。紧急权限应限定触发条件、作用范围和持续时间，要求记录理由、及时通知、事后复核，并安排必要的临时给付或人工处理。暂停不等于否定所有既有权利；恢复也不等于把暂停期间的损失视为从未发生。若没有补偿或责任分配，紧急按钮就可能成为对参与者单方面变更规则的工具。

救济必须进入设计本身。参与者应能查询自己的权利由何种事实和规则形成，谁提供了证据，谁批准或否决，何时发生状态变化；也应能申请更正事实、质疑规则适用、请求暂停争议部分的执行，并取得有理由的答复。链上记录难以直接擦除时，可以通过标注争议、冲正、追加更正记录及线下补偿处理错误。不同救济针对不同问题：事实错误需要重新核验，程序越权需要撤销或重新决定，给付错误需要追回或补偿，规则本身失当则需要制度修订。

这类制度设计是否比传统账户和合同管理更有价值，不能仅凭构想判断。可检验的命题包括：参与者能否更准确地预测未来请求；多方是否更容易核对权利依据；争议发生后能否更快查明变更链条；退出时是否更容易结清请求；自动执行有没有把错误或权力不对称扩大。应在相近的组织条件下比较不同技术方案，并把规则质量与技术效果分别评价。

五、动态权益状态机与不可越过的约束

要把上述原则转化为可检查设计，需要把“权益”拆成多个相互关联却不互相替代的状态机。状态机不是为了把人的关系机械化，而是强迫制度说明：哪一项事实正在变化，谁有权确认，变化影响哪一种请求，什么事项必须保持不变。

制度对象	典型状态	允许触发的依据	不得由该变化自动推出	错误时的主要救济
贡献主张	待提交—待核验—已确认—争议中—已修订	任务、交付证据、确认决定	已形成资本、已取得收益或治理权	补证、复核、追加更正
资本对象	候选—已吸收—有效—减损—终止	组织承接、持续使用、维护与风险审查	特定主体已经拥有该对象	重评、减损说明、维护责任调整
收益请求	附条件—已归属—已核算—到期—已履行	有效安排、可分配资源、核算与支付证据	自动取得所有权或治理权	重算、冲正、补偿、支付追索
治理资格	申请—有效—回避—暂停—终止	身份关系、代表授权、任期与事项条件	历史贡献或收益请求随之消失	资格复核、决定撤销、重新表决
使用许可	待批准—有效—受限—到期—撤销	任务目的、最小权限、保密与安全条件	获得标的所有权或再许可权	权限关闭、数据处置、损失补救
退出清算	通知—交接—核对—结清—持续义务存续	退出申请、未结事项、争议和交接证据	所有历史责任或既有请求归零	临时保护、分项清算、争议裁决

这个模型至少应满足五项制度不变量。第一，没有可识别的义务主体，系统不得把一项期待显示为可立即兑现的请求。第二，没有相应授权，任何人不得因掌握升级密钥而改变他人的权利状态。第三，事实更正可以改变依赖错误事实的结果，却不能无说明地覆盖历史。第四，转移只能作用于制度允许转移的部分，不能把人格、代表关系或持续义务一并打包。第五，争议应当冻结或标记受影响范围，不能借局部争议清空全部无争议请求。

还要区分三种看似相同的“状态变化”。新事实进入既定公式，是规则的正常适用；有权主体对开放性标准作出判断，是受程序约束的裁量；改变公式、权限或标准本身，则是制度修订。三者的日志形式可以相似，授权强度和救济方式却不同。系统若只记录“参数从A变成B”，而不记录变化属于哪一类，就无法判断参与者原先的预期是否受到不当改变。

动态权益的最小试验，可以选择一个边界清楚、周期有限的共同项目：使用一套普通业务系统保存原始证据，以版本化规则模型同步生成贡献、收益、治理和退出状态；另以现有合同与数据库流程作为对照。试验只处理事前明确的有限请求，不发行可自由交易的通证，也不把实验状态包装为正式财产权。任何无法说明依据的状态变化、无法完成的退出清算或超过预定损失上限的错误，都应触发暂停。

六、未来命题卡：受约束的可编程关系

项目	本章命题
可检验命题	在贡献跨期发生、权利类型多元且规则需要版本管理的协作中，分别建模贡献、资本、收益、治理、使用与退出状态，并保存每次变化的事实、规则和授权，能够提高权利依据的可解释性，减少因状态混同造成的争议。
适用对象	多阶段研发、长期服务、联合项目及其他需要持续确认贡献并分期兑现请求的组织关系。
成立条件	基础权利义务已经有效形成；状态定义能够被参与者理解；链下事实有责任主体；规则版本和救济程序真实可用。
主要风险	组织借“动态”追溯改变承诺；复杂模型使参与者更难理解；错误输入被快速扩散；升级控制集中于少数技术人员。
反证情形	与清楚合同和普通数据库相比，参与者预测自身处境的准确度没有提高，争议反而增加，或退出与纠错成本显著上升。
最小试验	在一个季度、一个项目和有限参与者范围内运行完整的确认—归属—履行—退出闭环，并保留人工处理路径和可回退基线。
观察指标	状态解释正确率、规则版本误用率、争议定位时间、错误影响范围、退出结清时间、参与者理解度及总治理成本。
人的最终责任	有权组织批准权利模型和规则版本；事实确认者对输入负责；治理机构处理例外和修订；义务主体承担实际履行与补救。

这项命题若成立，区块链提供的新增价值不是让权利“天然可编程”，而是使多个主体能够围绕同一版本和变更链核验关系状态。若集中数据库在相同制度条件下已经提供更低成本、更好救济的结果，就没有必要为形式上的链上表达增加复杂性。

从资产转移迈向权利义务关系的编排，区块链才可能进入共同创造更复杂的时间结构。但这条路径的前提始终是：权利有可识别的来源，义务有可追究的承担者，变更有有效授权，错误有实际救济。下一章将进一步讨论，当协作主体包含人工智能体时，贡献证据、代理权限与责任归属会面临怎样的新问题。

定稿补强：动态权益中的稳定承诺

可编程不意味着可以随意追溯改变。动态权益需要区分已经完成并取得的结果、仍在持续满足的条件和只适用于未来的规则。既得结果原则上不因普通规则更新被重新计算；确需调整时，应有明确授权、重大理由、受影响者陈述、过渡、补偿、申诉和退出安排。

基本权利、禁止歧视、程序参与、救济和已经明确承担的义务，应构成制度演化的边界。规则可以改进，承诺的稳定性也必须能够被参与者合理信赖。每次变更应说明是否追溯、影响哪些群体、为何没有更温和替代方案，以及谁承担变更成本。

本章注释

1. [SRC-017] OpenZeppelin：OpenZeppelin 的 VestingWallet 文档。[原文或官方页面](#)

- 本章引证：OpenZeppelin 的 VestingWallet 文档。
- 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：OpenZeppelin：归属钱包及时间安排、OpenZeppelin 的 VestingWallet 文档。
- 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
- 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。

第三十章 人与智能体共同创造的资本制度

共同创造的参与结构正在发生变化。一个人可以借助人工智能完成资料整理、方案生成、代码编写与结果检查；组织可以部署持续接收任务、调用工具并与其他系统交互的智能体。过去由一个岗位完成的工作，可能变成多人、多组织与多个智能体接续完成的过程。若仍以“谁最后提交文件”认定全部贡献，就会看不见任务设计、数据供给、授权、验证和风险承担；若把智能体每次输出都记作独立贡献，又会制造大量没有对应价值的记录。

本章把“AI智能体”用作制度建模中的操作性称谓：它是能够在设定目标和权限范围内执行若干任务、调用工具并产生可观察结果的软件系统。这里不预设它具有自然人或组织的法律地位，也不以技术标识直接赋予其财产、收益或治理请求。它可以成为贡献链中需要识别的行动节点，权利义务仍须依据具体制度、适用法律和真实主体的授权来安排。这个未来制度构想是否提高协作质量，还需要在具体场景中检验。

前章讨论了权利义务如何随条件变化。本章要追问更基础的问题：当部分行动由智能体完成时，谁提出目标，谁允许它行动，谁验证结果，谁承担损失，谁有资格主张收益？区块链能够保存部分授权和状态变化的可核验记录，但记录完整不等于贡献真实，更不等于责任已经得到分配。

一、人、组织与AI智能体之间的贡献链

“人与智能体共同创造”首先是关系命题，不是关于产出数量的口号。一个有用的成果可能依次涉及需求提出者、任务分解者、数据与知识提供者、模型或工具提供者、部署与维护组织、具体操作者、审核者、实际使用者。智能体在链条中生成内容、检索信息或执行操作，但它的行动条件来自其他主体：有人给定目标和权限，有人配置模型与工具，有人提供可用资料，有人决定是否接受结果。共同创造的记录应让这些环节可区分，同时避免把每个环节机械折算为一份独立收益。

贡献链至少需要区分三种关系。第一是因果参与：某个输入或行动在事实上影响了结果。第二是制度认可：事前规则将哪些参与界定为可评价贡献，并要求什么证据。第三是权益形成：经确认的贡献在何种条件下转为报酬、资本记录或其他请求。三者不能画等号。模型提供者可能是按服务合同取得费用，而非分享每次使用成果的权益；操作者可能仅履行雇佣职责，也可能依特别安排取得项目收益；一段自动生成的中间文本即使被记录，也未必满足组织对可用成果的要求。

可以从“任务—行动—验证—吸收—结果”的链条建模。任务记录说明谁设定目标、为何需要完成、允许使用哪些资料 and 工具；行动记录说明智能体调用了什么权限、生成了何种可复核中间成果；验证记录说明谁检查了事实、质量与适用性；吸收记录说明组织是否真正采用并把结果纳入工作能力；结果记录说明采用后产生了什么影响，以及影响如何与其他因素区分。链条中的每一项都可以有状态、证据和异议入口，不应把最后一项的经济结果倒推为所有上游环节都已形成资本。

同一智能体也可能代表不同主体行动。由企业部署的采购智能体、由供应商部署的报价智能体，即使采用同类模型，其授权来源、利益方向和责任承担者都不同。一个智能体服务多个项目时，需要按任务或组织划分记录和权限，不能用统一技术身份替代具体代理关系。相反，同一组织更换模型或工具版本，仍可能保持组织责任的连续性。链上标识记录“哪个系统实例执行了操作”，并不自动回答“它代表谁、根据什么授权、谁有权撤回”。

共同创造中的“人”同样不能被淡化为提示词输入者。界定公共目标、识别真实需求、作出取舍、承担照护与信任关系、处理受影响者异议，都可能是关键贡献，却不总表现为可计数的数字产物。制度若只奖励高频、标准化的机器可见事件，会把难以记录的协调、维护和责任承担挤到边缘。贡献链因此要保留人工说明、共同确认与争议复核，而不是追求每个行为都自动计分。

二、任务授权、行动证据与责任归属

智能体能够调用工具时，最重要的问题不是给它一个独立账户，而是限定它能够代谁做什么。任务授权应包含委托主体、任务目的、可访问的资料与系统、可采取的操作、金额或资源上限、持续时间、需要人工批准的节点、禁止行为和停止条件。权限应能被撤回或到期失效；委托主体、系统运营者和被授权执行者之间的关系应在记录中保持可追溯。授权范围越大，对审批、监控与恢复能力的要求越高。

“允许生成建议”和“允许作出承诺”是不同权限。智能体可以整理报价、提出合同草案，但是否可以向外签订合同、转移资产或确认他人贡献，必须单独授权。对重大权益变动，可以要求由具有相应权限的人复核并签署；对低风险、可逆的小额操作，可以在预定限额内自动执行。这样的分层不是在所有环节形式化地加入一个人工点击，而是让不同风险对应实际有效的控制。

行动证据也不能只保留最终答案。可核验记录应能够关联任务编号、授权版本、智能体与工具版本、关键输入来源、调用的外部资源、操作时间、输出摘要、人工审查和后续修改。敏感数据及完整过程不必全部上链，可以在适当受控环境中保存原始材料，在共享账本上记录摘要、签名、状态与访问规则。哈希只能帮助检查材料此后是否被改动，不能证明输入本来真实，也不能证明智能体推断正确。

证据保留需要比例原则。为每个低风险动作保存完整推理轨迹，可能增加隐私、商业秘密与运营负担，且未必提高可解释性。制度应先明确争议时必须回答的问题，再确定保存哪些输入、工具调用和人工决定；对高影响操作提高记录粒度，对日常低风险操作允许抽样检查。记录的目的在于复核授权、事实与结果，而不是用一份庞大的日志制造“责任已经可追溯”的外观。

责任归属应沿实际控制与义务来源追问。委托人若给出不当目标，不能把后果完全推给执行系统；部署组织若赋予过宽权限或忽略明显异常，应说明其管理责任；数据提供者若违反其保证，需要依据其承诺处理；审核人若只形式签字，也不能因“人工在环”就当然解除责任。多个主体可以分别承担不同环节的义务，不能因为存在多个参与者就出现无人负责的空档。具体责任及救济仍须按照适用制度和法律判断，账本只能保存支持判断的事实链。

这种区分与现有风险治理研究相接。NIST 的 AI 风险管理框架〔1〕强调人机配置中的角色、责任与监督应被明确规定和记录；其关于智能体身份与授权的概念文件〔2〕也把身份、权限和可核验行动列为需要解决的问题。这些资料为制度设计提供问题清单，并不代替具体组织对授权与责任的决定。

三、自动化成果如何影响贡献评价与收益安排

自动化改变了产出成本，也改变了“贡献”的可比性。一个人用智能体一天生成上百份文本，不应仅因数量大就获得上百倍贡献；另一个人花时间核验事实、识别错误并承担发布责任，也不应因输出件数少而被忽略。评价对象应从动作量转向经确认的有用成果及其形成条件：它是否解决真实任务、是否达到质量要求、是否被实际使用、是否减少重复劳动、是否产生新的可持续能力，以及是否造成额外的核验与风险成本。

需要分别记录自动化程度与人类贡献性质。自动化程度可以描述任务中哪些环节由工具完成，但不能直接推出人的贡献比例。任务设计、领域判断、异常处理、复核和长期维护的价值，并非用“人手敲了多少字”衡量。反过来，使用高成本工具也不当然意味着更高贡献；工具费用是成本，组织吸收的有效能力才可能与长期资本形成有关。

收益安排应先明确制度目标。若目标是补偿已完成劳动，可以规定成果验收后的报酬；若目标是激励持续维护，可以把部分收益与后续可用性或服务义务相连；若目标是分享长期共同创造的增量，则需要说明可分配资源、风险承担、归属周期和受益资格。模型供应商、平台、员工与客户可能各有合同价格、服务费用或合作分配，不能把所有关系都塞进一个“AI贡献积分”。更不能因智能体在账本上拥有地址，就推论它应直接取得资本份额或治理席位。

在共同使用工具的团队中，还应防止双重归因。某项自动化成果可能依赖组织购买的模型、团队长期积累的资料、个人提出的问题和另一组人的复核。制度可以给不同环节建立贡献事件及证据关联，规定哪些投入已由工资、采购价或服务费覆盖，哪些新增成果允许另行参与分配。若同一成本或成果在多个账户中反复计入，不仅扭曲收益，还会夸大已经形成的资本。贡献分配可以依事前约定加上复核程序，不宜由系统根据调用次数自动推定“公允比例”。

自动化也可能使原有岗位价值下降或工作内容迁移。制度不能只讨论效率收益归谁，还应讨论培训、转岗、过渡期、已有承诺和退出安排。对因共同知识、历史数据与员工经验训练或配置而成的能力，要明确使用授权、保密、补偿及持续维护责任；对被替代的具体劳动，不能凭一条新规则追溯取消已取得的报酬或贡献记录。共同成长的含义，是把新能力带来的收益与调整成本纳入可审议的制度，而不是假定技术进步会自动公平分配。

因此，智能体的成果进入资本记录要经历更严格的区分：输出被生成，不等于任务已交付；交付被接受，不等于成果可跨期使用；被持续使用，不等于特定个人拥有相应资产；形成长期能力，也不自动确定收益权或所有权。每一步都需要对应的事实、制度条件和责任主体。这与本书对贡献、资本和权益的基本界定保持一致。

四、防止规模化虚假贡献、代理串谋与责任空缺

智能体降低了生成记录的成本，也降低了制造“看起来像贡献”的成本。同一控制人可以批量创建账户、相互提交任务与评价；多个智能体可以交换内容、循环引用并制造使用量；组织内部也可能为了完成考核，把无需求的产出写成已交付成果。共享账本能够保存这些记录，却不会因记录不可轻易修改而使其变真。规模化虚假贡献是制度输入端的问题，不是账本最终性能够单独解决的问题。

防范应从任务来源开始。贡献事件需要关联真实需求、授权预算或资源、可验收标准与受益方；评价不能只由生产者控制，必要时引入业务使用者、独立复核或抽样审计。重复、近似和循环交易可作为异常线索，却不能仅凭相似度或同一网络地址宣告作弊。系统应允许解释、复核和申诉，避免反欺诈模型把合法的团队协作误判为串谋。

代理串谋往往跨越技术身份。两个表面独立的智能体可能受同一运营者控制；一个审核智能体可能由成果提供方配置；人工批准者也可能只按智能体建议机械签字。应披露实质控制、资金关系和角色冲突，设置相互独立的审查路径，并对关键环节实施职责分离。独立性不是多设几个地址，而是使提出、验证和裁决权不能由同一利益方向无约束地掌握。

安全威胁还会改变“是谁行动”的判断。外部文本可能诱导智能体偏离原任务，过宽的工具权限可能使其执行本不应执行的操作，凭证泄露可能让他人冒用其身份。防护应包括权限最小化、输入与工具调用隔离、异常监控、限额、停机与恢复，以及对高影响操作的独立确认。OWASP关于智能体应用风险的资料〔3〕把工具误用和身份权限滥用列为重要攻击面；本书据此提出的治理要求仍需按具体系统的威胁模型验证。

责任空缺则是另一类风险。组织可能把任务交给外部智能体，外部服务商又调用其他工具，最终人人声称只是提供通用技术。制度应在部署前确定对外负责的主体、内部追责与追偿路径、事故报告义务、证据保全责任及受影响者的申诉入口。跨组织合作时还须明确谁能暂停系统、谁能纠正错误权益记录、谁承担已发生给付的处理成本。技术链条可以很长，面对受影响者的责任通道不能无限后移。

对于高风险或大规模自动化，治理还需要总量边界。每个主体可自动提交多少待核验贡献、自动获得多大额度权益、在何种异常阈值下转入人工复核，都应事前设定并定期审议。限制既不能只靠模型自报“我有信心”，也不宜一律以产出数量处罚高效率协作。应综合任务价值、证据质量、历史错误率、风险规模和纠错能力，并公布规则改变的授权与救济方式。

最终要检验的不是智能体是否“像人一样拥有贡献账户”，而是制度能否更准确地把真实需要、有效行动、持续能力和可兑现承诺连接起来。可比较的指标包括虚假或重复贡献的发现率、误伤合法贡献的比例、从异常出现到责任确定的时间、审核成本、被采纳成果的长期可用性，以及参与者对收益规则的可理解程度。只有当这些指标相对于可行的非区块链方案有所改善，且成本与权力集中风险可接受，才有理由认为共同账本提供了额外价值。

五、行动证明、风险分级与责任密度

人机协作要进入资本治理，不能只证明“某个智能体做过什么”，还要证明该行动处在何种委托关系中。一个可复核的行动单元至少应关联九项内容：任务目的、委托主体、被授权智能体、模型与工具版本、可用数据范围、实际操作、人工审查、组织采用和异常处置。它们共同形成行动证明，但并不要求全部原始内容公开或上链。

记录层	必须回答的问题	可以采用的证据	不能据此单独推出
任务层	谁提出真实需要，允许解决什么问题	任务单、预算或资源授权、验收标准	任务合理或目标正当
委托层	智能体代表谁，在何时拥有哪些权限	授权版本、限额、有效期、禁止事项	委托人免除监督责任
行动层	使用何种模型、数据与工具实施了什么操作	版本标识、工具调用、输入来源摘要、签名日志	输出事实正确或质量合格
审查层	谁以何种资格接受、修改或拒绝结果	审查意见、差异记录、复核与回避信息	形式上的人工点击即构成有效审查
吸收层	成果是否被实际采用并形成持续能力	上线、使用、维护和业务结果记录	全部结果都应归于最后生成者
责任层	错误由谁说明、停止、补救和赔偿	事故记录、责任分工、补偿与追偿依据	存在日志就代表责任已经履行

记录深度应当与风险匹配。低风险、可逆、影响范围小的任务，可以保留任务、版本、结果与抽样审查；中等风险任务需要明确数据来源、工具权限和独立验收；涉及资产转移、对外承诺、人员权益或不可逆影响的高风险任务，应要求事前批准、限额、双重确认、实时监测和可执行的停止机制。分级的意义在于把稀缺的人类注意力放在高影响节点，而不是让“人工在环”沦为对所有结果的机械盖章。

本书进一步提出“责任密度”这一设计指标：在一段自动化流程中，能够改变他人权利、资源或机会的每个关键节点，都应当找到至少一个有能力采取行动、具有明确义务并可被追究的人或组织。责任密度不是责任主体越多越好。主体过多却没有首要回应者，会形成扩散；只有一个名义责任人却没有权限和信息，也只是形式承担。需要检查的是责任是否覆盖风险节点，以及受影响者能否沿一条有限路径获得说明和补救。

防止规模化虚假贡献，还需要把容量控制放在身份数量之前。即使每个智能体都有独立标识，同一实际控制人仍可能批量行动。制度可以按委托主体、任务预算、可核验需求和审核能力设置提交容量，对异常关联、循环采用和自我评价提高复核强度。容量限制应有明确理由和申诉路径，避免用反欺诈名义排斥高效率但真实的贡献。

最小试验可以选择一种不会直接处分重大资产的知识任务，让人工团队与人机团队在相同目标、资料和验收标准下工作。试验预先规定授权边界、审查抽样、错误分级和停止条件，同时记录生成数量、实际采用、复核负担、错误修正及责任定位。若自动化组只提高产出量，却显著增加无用结果、审核成本或责任查明时间，就不能把活动规模当作资本形成。

六、未来命题卡：可追责的人机共同创造

项目	本章命题
可检验命题	在智能体能够调用工具并影响业务状态的协作中，以任务授权为起点、以行动证据连接模型和工具版本、以人的最终责任结束，可以提高有效成果的识别率并缩短事故责任定位时间。
适用对象	组织内部AI助手、跨组织智能体服务、自动化研发与内容生产，以及有限权限的交易或运营代理。
成立条件	委托主体可识别；权限可限制和撤回；关键行动能够留证；审核者具备实际能力；对外存在首要责任通道。
主要风险	日志过度收集侵犯隐私；人工批准形式化；多层外包造成责任扩散；模型与身份服务形成新的基础设施依赖。
反证情形	行动记录增加却不能改善责任判断；虚假贡献发现率未提高；参与者无法理解自动化对评价和收益的影响；非区块链日志方案表现更好。
最小试验	在单一、低不可逆性任务中比较人工流程、人机流程及不同记录方案，运行从授权到采用、异常和申诉的完整闭环。
观察指标	有效采用率、重复或虚假贡献率、误伤率、人工复核时间、事故发现时间、责任定位时间、补救完成率和单位有效成果总成本。
人的最终责任	委托组织对目标和权限负责；部署者对配置与监测负责；审核者对其确认范围负责；对外义务主体不得以智能体或供应链条拒绝响应。

若这项命题只能在持续扩大监控、集中身份和强制使用单一平台的条件下成立，其制度代价可能超过效率收益。未来研究必须把生产率、参与者权利、责任可达性和基础设施权力放在同一评价框架中。

人与智能体的协作可能扩展共同创造的规模，却也使代理链、证据链和责任链更加复杂。制度技术的任务不是把智能体拟制为一个无需人负责的新资本主体，而是让每一项重要行动都能回到有效授权、真实成果、明确义务与可行救济。下一章将把视野移向多个组织之间：当不同制度的身份、贡献与权益记录需要相互解释时，如何保持协作，同时避免共同基础设施变成新的控制中心。

定稿补强：智能体安全、人类批准与责任主体

智能体应被视为具有可识别身份和有限能力的技术行动单元，而不是因能够自主执行就取得当然法律人格。每项高影响任务都要登记部署者、授权人、受益人、模型或服务供应者、数据与工具来源、许可和最终责任主体。责任主体不能因任务由多个模型、插件或代理链完成而空缺。

智能体威胁模型应覆盖提示注入、工具滥用、数据投毒、模型与供应链漂移、身份冒用、代理串谋和规模化虚假贡献。控制包括任务沙箱、最小工具权限、输入隔离、模型与工具版本、行动限额、运行监测、熔断、证据保留和定期再授权。可追踪身份只是追责条件，不能代替运行时限制。

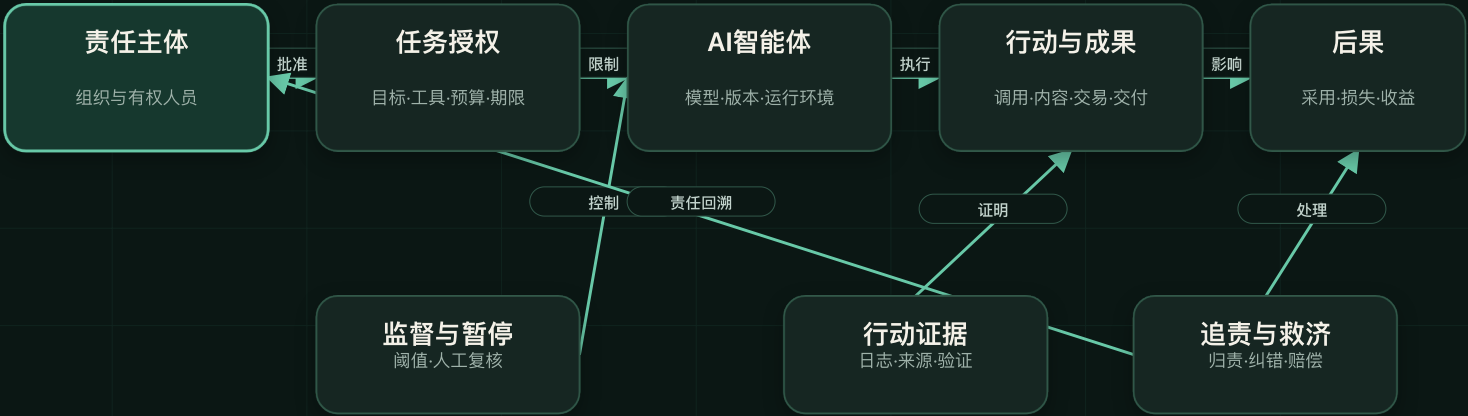
自动推荐、自动评价和自动执行不得形成自我批准闭环。基本权利变化、大额分配、身份或资格取消、重大规则升级、例外裁决和对外不可逆履行，应由具名的人或有权组织批准；高风险事项配置双人复核。人类批准也必须是实质审查，系统应保留意见分歧、拒绝理由和复核时间，而不是用点击确认转移责任。

本章工具与图表

本章的制度关系可结合[附录三](#)、[附录十三](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

图30-1 人、组织与AI智能体的授权—行动—责任链

智能体可以执行任务和生成证据，责任必须沿授权与控制关系回到人或组织



《区块链——利益相关者资本论的底层技术》V1.0 · 可编辑SVG

图30-1 人、组织与AI智能体的授权—行动—责任链

图30-1 人、组织与AI智能体的授权—行动—责任链。智能体可以执行任务和生成证据，责任必须沿授权与控制关系回到人或组织

本章注释

- [SRC-001] 美国国家标准与技术研究院（NIST）：NIST 的 AI 风险管理框架。[原文或官方页面](#)
 - 本章引证：NIST 的 AI 风险管理框架。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：NIST 的 AI 风险管理框架。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-059] 美国国家网络安全卓越中心（NCCoE / NIST）：Accelerating the Adoption of Software and AI Agent Identity and Authorization。[原文或官方页面](#)
 - 本章引证：概念文件。
 - 支持范围：用于说明公共机构对风险、身份、评估或技术能力的框架性要求，本书引用主题包括：概念文件。
 - 使用边界：框架提供分析与控制依据，不替代组织对具体事实、成本和责任的独立判断。
 - 证据等级：B（官方机构、协议项目或公共组织发布的说明与指南）；链接状态：已完成可访问性核验，核验日：2026-10-08。
- [SRC-046] OWASP Foundation：OWASP 关于智能体应用风险的资料。[原文或官方页面](#)
 - 本章引证：OWASP 关于智能体应用风险的资料。
 - 支持范围：用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：OWASP 关于智能体应用风险的资料。
 - 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
 - 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：官方来源存在访问限制，已保留人工复核标记，核验日：2026-10-08。

第三十一章 可组合制度与跨组织协作网络

一家组织可以确认自己的成员、贡献和权益，但共同创造往往发生在多家组织之间。研发方完成设计，生产方使其成为可交付产品，服务方持续改进，客户提供使用反馈；每一方都可能依自己的程序记录事实、评价贡献和承担义务。当这些记录进入下一段协作，关键问题不是把所有组织接入同一条链，而是让各方知道：对方究竟证明了什么，自己决定承认什么，承认之后承担什么。

本章所说的“可组合制度”，是指不同组织在保留各自决定权的前提下，为身份、证据、任务、结算和争议建立可对接的规则。它不是把一家组织的积分直接兑换为另一家的股权，也不是要求所有参与者接受同一个平台制定的价值尺度。技术接口可以帮助传递声明和状态，制度接口则规定信任范围、效力边界与责任承担。没有后一层，信息传得越快，误认和争议也可能扩散得越快。

第二十四章已经讨论跨组织生态治理的基本结构。本章进一步从未来制度的角度追问：如果贡献凭证、权利规则与协作流程能够组合，怎样防止“互操作”沦为单一平台对身份、评价和结算的控制？答案要从跨组织解释开始。

一、身份、贡献凭证与权利规则的跨组织解释

跨组织解释首先不是识别一个地址，而是弄清楚谁作出陈述、陈述针对谁、陈述的事项与时间范围是什么。一个自然人可以同时是甲组织的员工、乙项目的外部顾问和丙网络的客户；一家企业也可能由不同代表就不同事项签署。相同的技术标识不保证相同的代理权限，不同标识也不意味着背后必然是不同主体。接收方需要核验身份或代理的证据，并判断它是否覆盖当前任务。

贡献凭证应尽量表达可复核的有限声明，而不是总括性的“价值证明”。例如，甲组织可以声明某人在指定期间向某任务提交了成果，并由甲依其规则完成验收。乙组织可以核验声明确由甲发出、尚在有效期内，却仍须自行判断成果是否满足乙的业务需要。若甲只确认“收到交付”，乙不能把它解释为“成果已被长期使用”；若甲确认某项内部收益资格，乙也不会因此成为该收益的义务人。

第十三章界定了技术验证的证明范围，第二十四章界定了跨组织承认责任。可组合制度在此把两者压缩为三道接口门槛：凭证确由所称签发者作出，签发者有资格证明所述事项，接收组织愿意在指定用途上依赖该事项。把“可验证”直接译成“必须承认”，会让核验者失去自己的责任边界。

贡献的跨组织使用还需要保留来源与解释版本。任务名称、贡献类别、计量单位、验收方法和争议状态，应随凭证一起说明；如果一方的“已完成”只表示文件交付，另一方的“已完成”却包含商业采用，两者不能用同一个字段强行等同。可建立共同的最小词汇，例如“提交”“接收”“验收”“采用”“撤销”，同时允许每个组织为本地制度补充条件。共同词汇降低翻译成本，不应取消本地差异。

对权利规则的解释尤其要谨慎。权利不仅有名称，还包括权利主体、义务主体、标的、范围、成立与履行条件、期限、可转让性及救济。甲组织确认某人享有内部奖金请求，乙组织可以把此事作为合作履历的参考，却没有义务支付甲的奖金。若乙愿意基于甲的贡献记录提供新的待遇，应由乙依据自己的授权形成一项新安排，标明其来源及生效时间，而不是把甲的请求“搬运”过来。贡献可以成为判断材料，权利不能脱离承担义务的人自动漂移。

跨组织解释还受撤销、更正和隐私约束。原签发方发现验收错误时，接收方需要知道凭证状态已变化，以及此前依赖该凭证作出的决定是否需重审。接收方也不应因取得一次验证权限，就永久收集全部原始资料。可以对不同用途披露不同范围的证明，并约定谁保管证据、何时复核、何时删除。这样，互认才有可能同时保留核验能力与参与者对数据的控制。

二、制度接口：进入、协作、结算与退出

技术接口描述数据如何发送和读取；制度接口则描述组织在各个阶段愿意接受什么、承担什么。一个可组合的协作网络，不必拥有统一的章程和单一账户体系，但至少就要就进入、协作、结算、退出四个环节形成可公开理解的安排。每个环节都应能回答适用主体、必要证据、决策权限、状态变化及异议通道。

进入接口应明确准入条件，而不是让持有钱包或凭证自动成为共同体成员。参与者须知道所申请的角色、可见数据、可做操作、收费或保证要求、保密责任和拒绝进入的复核程序。资格可以由一个组织签发，再由其他组织分别决定是否认可；网络管理者不能仅以控制身份目录为由，任意改变各组织对合作对象的独立判断。对新进入的小组织，应尽量提供可达到的验证路径，避免把昂贵的专有认证变成隐性门槛。

协作接口要把共同任务与各自职责连起来。各方可以共享任务编号、交付标准、变更程序、提交与验收状态，并保留本地业务系统处理内部资源分配。共同账本不适合记录多方需要一致核对的关键事件；合同细节、商业秘密和个人资料可以由有责主体在受控环境中保存。若一方用智能体代表组织提交成果，还须传递代理范围和有权负责的组织，而不只是智能体标识。

结算接口不能仅约定一个转账指令。它应说明什么事件形成请求，谁确认数量与质量，采用哪一版价格或分配规则，税费与扣减由谁计算，链上记录和现实支付怎样对账，支付失败或退回如何处理。共同账本可使各方看到相同的结算状态，但不直接生成现金，也不自行解决收入确认或所有争议。一个可用的接口应允许“已提交、待核验、已确认、待支付、已支付、争议中”等不同状态，避免用一次技术确认覆盖全部履行过程。

退出接口最能检验协作网络是否真正开放。成员应能取回自己有权取得的身份、任务、贡献、结算和争议记录，撤销不再需要的访问权限，完成未结款项和交接，并明确保密、质量保证及其他持续义务。退出不应迫使参与者放弃已成立请求，也不能因节点离网就删除其历史责任。记录的格式、证明方法和转换支持应在进入时就说明；否则，所谓随时退出只是形式权利。

这四个接口可以由不同技术实现。对于稳定且相互信任的少数主体，签名日志与数据库也可能足够；当多方需要共同核验状态、没有一方被普遍接受为唯一记账者，才需要认真评估区块链的额外收益。选择依据应是协作负担、审计能力和退出可行性，而不是接口是否贴上“链上”标签。

三、不同规则体系之间的冲突、承认与仲裁

可组合并不等于规则完全一致。不同组织可能对同一交付采用不同验收期限，对同一身份设定不同资格，对保密与公开提出相反要求，对收益计算使用不同周期。若这些差异在合作前没有被识别，技术接口即使全部连通，后续执行也可能互相冲突。因此，组合的第一步是为冲突预留位置，而不是假定通用数据格式能够消灭制度差异。

冲突至少可分为三类。事实冲突，是双方对交付是否发生、质量是否达标有不同记载；解释冲突，是双方承认同一事实，却对“已验收”或“可分配”的含义不同；规范冲突，是双方都清楚事实与定义，但各自规则对权利或责任作出不兼容安排。事实冲突要补证与复核，解释冲突要回到术语、目的和约定版本，规范冲突则需要确定适用规则、优先顺序与有权裁决者。把三类问题都交给“多数节点表决”并不合适。

承认应有范围。甲可以承认乙签发的交付证明，用于免除重复核验，却保留对本组织采购资格的判断；也可以承认乙的争议处理结果仅用于内部风险评估，而不让它直接改写本组织的支付义务。承认的范围可以按事项、签发机构、时间、金额或风险级别限定，并留有暂停与撤回条件。对外部结论的依赖越深，越需要检查签发方程序是否允许受影响者参与及申诉。

合作协议应预先规定规则优先顺序。共同任务条款、本地组织规则和网络通用规则，各自适用什么事项；发生冲突时，哪些问题交由任务双方协商，哪些由多方治理机构审议，哪些进入具有约束力的裁决或适用的法定程序。若后续变更某一规则，不应追溯剥夺其他主体依旧版规则形成的请求。版本、通知与过渡安排，在跨组织情境下比单一企业内部更重要，因为没有一家企业能够单独修改所有参加者的承诺。

仲裁或其他争议解决方式，也需要与技术纠错衔接。争议期间可以标注有关记录、暂停有风险的自动结算，保全证据并保障不争议部分继续履行；最终结果可能要求追加更正、冲正、重新计算或链下赔偿。不可变记录不应被误当作不可纠错决定。裁决者的权限、选任、利益冲突、费用、可执行范围和复核机会都应事前约定，不能只写一个“争议交由社区处理”的空泛条款。

跨组织合作有时跨越不同法律和监管环境。技术系统不能自行决定何种主体有法律资格、何种财产权已变动或哪一地的强制规则可以被排除。制度设计应识别适用范围和负责机构，必要时以合同、登记、支付和现有争议程序完成链下衔接。本章提出的是治理架构与研究命题，具体法律效果仍需在相应场景中核验。

四、互操作如何避免形成新的基础设施垄断

互操作常被理解为“都接入同一个入口”，但单一入口也可能变成新的控制点。谁管理身份目录，谁能调整数据格式和接口费用，谁保管历史记录与撤销信息，谁有权暂停账户、决定升级和解释争议，谁就可能影响所有成员的协作机会。账本由多节点复制，并不意味着应用入口、标准制定、密钥托管和业务评价也已经分散。

避免基础设施垄断，首先要把握可移植性做成真实能力。成员应能按公开或充分披露的格式导出自身有权取得的凭证、任务状态和结算依据，验证者不必只依赖原平台界面才能读取历史证明。接口版本变更要有迁移期和向后兼容安排；必要的验证资料 and 状态查询在原运营者退出后仍应可获得。没有这些条件，“持有链上凭证”也可能无法在别处使用。

其次，关键治理权不宜由接口运营者单方兼任。协议升级、准入标准、收费结构、争议处理和紧急暂停可采用不同的授权与监督程序，让受影响组织和参与者有提出、审议与复核的途径。决策权配置不要求每项技术运维都全民投票，它要求改变共同承诺的重大事项不能伪装成单纯的软件更新。多方治理的有效性也须看实际参与能力，而不能仅以席位数量证明。

再次，需要防止“标准开放、实现封闭”。文档公开却必须购买唯一认证服务，数据可导出却缺少语义和历史状态，协议允许其他节点却把关键索引或身份恢复交给一家企业，都可能形成事实依赖。应定期测试替代实现能否接入、迁移所需时间和成本、退出后能否继续核验证据，以及运营者变更条件时成员是否有谈判能力。这些测试比“去中心化”自我宣称更能显示权力结构。

开放也不能无视隐私和质量。把所有组织的原始数据强制公开，会让小组织和个人付出过高代价；任何人都能签发凭证，也不意味着所有签发者都值得在全部事项上信任。较可行的方式是公开必要的接口与解释规则，允许各组织对签发者、用途和风险设定本地信任策略，同时使拒绝、撤销和更正有透明程序。互操作追求的是选择与可替换，不是取消判断。

本章的构想需要接受与集中平台、联盟数据库及双边协议的同条件比较。应观察新增组织的进入成本、跨组织重复核验次数、结算与争议耗时、退出成功率、数据迁移成本，以及关键规则实际由谁决定。若共享架构只是把原有平台依赖迁移到新的身份服务、桥接服务或标准委员会，制度效果就未达到目标。可组合制度的真正价值，是让共同创造可以跨越组织边界，同时让每一方看清自己承认的事实、承担的义务和保留的自主权。

五、最小制度接口与一致性测试

可组合制度不能只发布技术接口文档，还应发布一份“最小制度接口说明”。它不要求公开全部内部制度，而是让外部协作者在采取行动前能够知道自己正在依赖什么。至少应包含下列对象：

接口对象	最小必要字段	接收方必须自行决定的事项	失败或退出时的要求
主体与代理	主体标识、代表关系、权限范围、有效期	是否足以代表当前事项	撤销通知、代表更换、历史责任连续性
贡献凭证	任务、事件、证据范围、确认者、状态与版本	是否满足本地评价或资格要求	更正传播、依赖影响清单、复核入口
权利规则	权利主体、义务主体、标的、条件、期限、可转让性	是否愿意承担新的本地义务	过渡、结算、既有请求保存
结算状态	请求来源、币种或资源、核算版本、支付状态	税费、合规与本地账务处理	失败重试、退回、冲正和对账
争议状态	争议对象、影响范围、处理机构、临时措施	是否暂停本地采用及暂停范围	证据保全、决定承认、补偿执行
撤销与更正	原记录、变更原因、授权者、生效时间	既有决定是否重新审查	通知可达、追加证明、历史可追溯
退出包	可导出记录、未结事项、持续义务、验证方法	是否接受迁移后的证明	开放格式、合理期限、独立验证路径

接口能传递字段，只证明语法层互通。真正的制度互操作至少要经过五级检查：传输是否到达，格式是否可读，语义是否一致，采用是否获得有效授权，错误是否存在救济。前三级可以由技术测试较多覆盖，后两级必须进入组织治理和责任安排。某项接口只有“成功响应”而没有说明接收方据此承担何种后果，不应被称为完成制度互认。

一致性测试应当包含正常路径，也应包含拒绝、撤销、冲突和退出。可以使用一组共同测试情景：代理权限在结算前到期；签发方撤回贡献确认；两个组织对“已验收”含义不同；网络规则升级而本地制度尚未批准；基础设施运营者停止服务。通过测试的标准，不是所有组织得到相同结论，而是每一方能够准确识别差异、阻止无授权后果，并沿预定程序继续协商、仲裁或退出。

还需要做替代实现测试。至少由一个不受原运营者控制的工具读取凭证、核验状态和导出退出包，测量迁移所需时间、费用和信息损失。如果所谓开放标准只能通过原平台的索引、密钥恢复或解释服务使用，就仍然存在事实锁定。对共同基础设施的评价，应把这种可替换性作为持续指标，而不是上线前一次性的合规声明。

最小试验可以从两家组织之间的一类有限凭证开始，只互认一项明确事实，不交换总括性评分，也不让外部凭证直接生成本地财产权。试验要故意触发一次更正、一次拒绝和一次退出，观察通知能否到达、已有处理能否定位、主体能否带走必要记录。只有在异常路径也可运行时，才有理由扩展到结算、权益或多方网络。

六、未来命题卡：保留自主权的制度组合

项目	本章命题
可检验命题	有限声明、明确承认范围、版本化制度接口和可验证退出为基础的跨组织网络，可以减少重复核验与结算摩擦，同时不要求各组织交出本地权利判断和治理自主权。

项目	本章命题
适用对象	供应链、联合研发、专业服务网络、跨平台人才与贡献凭证，以及需要多方结算的协作生态。
成立条件	最小语义能够共同解释；签发和采用责任明确；争议与更正可传播；至少存在一条非原平台控制的验证和退出路径。
主要风险	通用词汇掩盖制度差异；身份或桥接服务集中；开放格式仍依赖专有索引；强势平台把互认变成准入控制。
反证情形	重复核验未减少，争议因误认增加，退出记录无法在外部验证，或关键规则仍由单一运营者无约束决定。
最小试验	两家组织、单一凭证类型、一个结算周期，必须包含签发、采用、拒绝、更正、争议和退出六条路径。
观察指标	接入时间、重复核验次数、语义误读率、更正传播时间、争议处理成本、退出成功率、迁移信息损失和关键规则控制集中度。
人的最终责任	签发组织对声明负责；采用组织对依赖决定负责；网络治理者对共同接口与通知负责；争议机构对其裁决范围负责。

如果互操作只能通过统一身份、统一评分和统一结算实现，它可能降低表面摩擦，却同时把制度选择权集中到基础设施层。可组合制度的研究目标应是降低协作成本并保存可退出的多元秩序，而不是把多元组织改造成一个无法离开的超级平台。

当制度能够互相解释，下一步的问题是制度自身能否被检查和改进。最后一章将讨论如何从文本走向可检查的规则模型，在有限试验中识别后果，并以审议和授权推动修订，而不牺牲既有承诺与人的最终责任。

定稿补强：语义互操作与版本化接口

跨组织互操作不仅是消息能够送达，还包括同一对象在不同制度中是否具有相同含义。身份、贡献、证据和权益对象应采用明确命名空间、模式版本、主体标识与来源，必要时提供语义映射和测试向量。字段同名而定义不同，应被视为不兼容，而不是静默合并。

接口变更应有兼容期、弃用通知、迁移工具和失败回退。合作方需要知道哪个版本可以进入、如何结算、争议时保存哪些证据、退出后如何导出数据。技术映射无法解决准据法、管辖、破产和权利优先问题，这些仍由跨组织协议单独规定。

本章工具与图表

本章的制度关系可结合[附录十三](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。



第三十二章 可验证、可修订与可演化的制度

制度一旦进入技术系统，就不再只以文字存在。谁可以提交贡献、何种证据使其进入确认程序、什么条件下形成收益请求、谁能修改参数、何时可以暂停执行，都可能成为实际运行的权限与状态转换。技术使规则更易被持续执行，也使规则中的缺口、偏差和权力分配更直接地影响参与者。因而，制度技术不能只追求“按既定代码自动运行”，还要能说明其规则、检查其后果、纠正其错误，并在有效授权下演进。

本书的基本判断在这里达到一个新的层次。区块链可以使多方对某些记录和操作保持一致，却不负责决定共同创造的全部价值，更不会让制度自动正当。可验证，是检查事实、规则和执行之间能否对上；可修订，是承认既有设计可能不完善并设立更正途径；可演化，是在长期合作中积累经验、调整安排，同时保护参与者有理由信赖的承诺。三者必须同时成立，才有可能让制度技术支持共同成长。

前章讨论不同组织如何解释和组合各自的规则。本章作为正文最后一章，把视角转向制度自身的检查、试验与修订，并强调一个不能交给系统自动完成的判断：什么改变是改进，什么改变只是把成本转嫁给更弱的一方。

一、从制度文本到可检查的规则模型

制度文本通常用概念、原则和例外来表达共同意图。它允许解释，也依赖人们对具体情境作出判断。要把其中一部分放进数字系统，首先需要找出哪些内容已经足够明确，哪些仍留有裁量。若“重大贡献”“合理分配”尚未确定证据和程序，就不能假装通过一段代码把它们变成精确事实。规则模型应当暴露未决问题，而不是掩盖它们。

一个可检查的模型至少要说明主体、角色、权限、对象、状态、触发事件和义务。以贡献确认为例，应区分提交者、被归属者、验证者和异议者；区分“已提交”“待补证”“已确认”“被驳回”“争议中”“已更正”；规定每种状态由谁、凭什么证据改变，以及改变后是否产生新的请求。规则模型还要指出哪些后果由程序直接执行，哪些只能在具有权限的人作出决定后生效。

从文字到模型，不能省掉权利的相对面。有人取得收益请求，就应能找到负责核算和履行的主体；有人获得治理权限，就应能说明其授权来源和作用范围；有人能够撤销贡献确认，就应能看到通知、理由与复核程序。若模型只包含账户余额和操作按钮，缺少义务主体与救济路径，它可能是可运行的软件，却不是充分表达资本治理关系的制度模型。

可检查性有不同层次。结构检查问是否存在无主体、无依据或无期限的权利状态；一致性检查问相同条件是否在不同模块得到冲突结果；过程检查问未经授权者是否可能改变已确认记录、争议期间是否可能继续错误支付；效果检查则问规则运行后是否真的改善了协作。前三者可以在一定范围内借助形式化描述、测试和审计；最后一项不能只由代码推导，必须观察真实参与者与组织行为。

规则模型还应把关键的“不应发生”写清楚。例如，一项贡献不经确认不能直接生成已到期收益；退出不能自动消灭此前已归属请求；同一任务不能被重复结算；处理自身争议的审查者不能同时充当唯一裁决者。这类约束可以转为系统不变量并在有限模型中检查。TLA+ 的模型检查资料〔1〕说明，形式工具能检查所建模型的行为是否满足所写性质；它不能证明模型遗漏的现实事实不存在，也不能代替对性质本身是否公正的判断。因此，形式检查的成果应与制度审议并列，而非取而代之。

规则版本、证据类型及术语解释也应纳入模型。一项“已验收”究竟意味着收到文件、质量合格还是开始实际使用；相同字段在不同组织中是否指同一事实；证据被撤销后依赖它的请求如何处理，都需要明确。可检查的制度，不是把所有复杂性消除，而是使各方能定位复杂性所在，并知道谁有权解释和处理。

二、在仿真与有限试验中检验制度后果

规则在纸面上自洽，不代表其激励和分配后果可接受。贡献计量可能鼓励拆分任务以多领分数，审核门槛可能使小组织难以进入，自动结算可能在错误证据被纠正前完成不可逆支付。仿真与有限试验的价值，是在影响扩大之前寻找这些后果，并检验制度是否具备纠错能力。

仿真应从问题出发，而不是把一组理想参与者放入系统后展示漂亮曲线。至少要纳入不同资源与议价能力的主体、正常与恶意行为、证据延迟、系统故障、规则版本变化和退出。可以设置若干边界情境：贡献被多人共同完成，验收者与受益者存在利益关系，外部智能体批量提交近似成果，支付后发现凭证错误，某个大型参与者威胁退出。观察的不是“平台运行了多少笔交易”，而是风险由谁承担、谁能及时提出异议、错误能否被纠正。

仿真结果依赖所设假设。参与者是否会为长期声誉克制短期套利、审核者是否有足够时间复核、客户是否愿意提供真实反馈，都不能从模型自身得到保证。应公开关键假设，做敏感性分析，并记录哪些结论会随参数变化而反转。仿真没有发现问题，只表明在给定场景、参数和模型边界内尚未发现；不能宣布制度已经通过现实检验。

有限试验则应把范围、时间和损失边界事前确定。先选择可追溯的业务流程、有限数量的参与者及明确的退出方式，运行完整的“承诺—投入—交付—确认—回报—评价—修订”闭环。试验要包括真实的申诉和更正，而非只验证正常路径。涉及权益的承诺应说明其效力、资金或资源来源及争议处理方式；不能把尚未获授权的实验积分呈现为已成立的财产权。

评价需设置对照。没有区块链时，用数据库、签名日志或现有合同程序能否达到类似效果？若多方对账更快，是账本机制的作用，还是参与者因试点而集中投入了更多管理资源？若争议减少，是规则变清楚，还是弱势者放弃申诉？应将技术效果、制度效果与经营效果分别记录，并观察成本是否从组织转移给个人或合作伙伴。试验的成功标准应在启动前确定，避免结果出现后调整叙事。

有限试验还要设计停止条件。若虚假贡献无法有效识别、错误支付不能及时纠正、隐私泄露风险超出控制能力、关键参与者缺少可行的申诉渠道，就应暂停扩大范围，并先修订相应制度。试验不以“必须上线成功”为使命；诚实地发现不适用条件，也是制度研究的重要产出。

三、反馈、审议、授权与版本演进

制度演进不等于参数自动优化。参与者的反馈可能指出事实错误，也可能指出规则本身不公平；运营数据可能显示执行缓慢，却无法解释等待是否来自必要的审查。要使反馈可用，需要区分服务故障、证据缺陷、规则解释分歧、权力配置失衡和外部环境变化，再分别进入技术修复、个案救济或制度修订程序。

反馈通道应允许受影响者表达具体后果。提交意见后，制度应说明谁受理、何时答复、是否可以请求复核，以及重复出现的问题如何上升为规则议题。只让高频用户或大额持有人参与反馈，容易使不经常使用系统、但承受较高风险的人被忽略。投诉数量低也不能直接表明制度良好，可能是渠道难用或参与者担心提出异议后的合作机会。

规则修订需要可审议的提案。提案应列明要改变的条款、拟解决的问题、受影响主体、预期收益、可能损失、实施成本和替代方案；若涉及收益、治理或退出条件，还应分别分析已有请求和未来关系。支持者可以提出效率理由，反对者也应有机会提供反例。审议不是机械计算赞成票，而是让影响和理由能够被看见、回应并记录。

授权应与改变的性质相称。修正明显错误的显示文字、调整不影响实质权益的技术参数，与改变贡献评价权重、收益资格或申诉期限，并非同一等级。前者可由受托运营者按限定权限处理；后者可能需要更广泛的代表、通知、表决、个别同意或其他有效程序。即使协议层多签已经通过，也仍须核查签署者是否有权改变相应承诺。技术授权是制度授权的一部分，不是其全部。

每次修订都应形成版本关系：旧规则适用于哪些事件，新规则何时生效，进行中的任务如何过渡，已确认贡献与已归属请求如何保留，软件升级与数据迁移怎样实施，以及如果新规则失败如何恢复。版本记录应允许参与者回答“当时适用哪份规则、由谁批准、我为何受到影响”。版本可追溯，才有可能在争议中还原共同承诺；只有最新版本而没有过渡依据，反而会让制度演进成为追溯改写。

反馈可以持续，正式修订却需要节制。过于频繁的参数变化会使参与者无法预期投资和合作回报；长期拒绝修订又会把早期设计错误固化。可设置定期评估与有限的紧急修订通道，前者用于系统性调整，后者仅处理明确、迫切、范围可控的风险。紧急决定要有期限、理由、事后复核及补偿安排，不能把“安全”当作永久绕过共同决策的通行证。

四、演化边界：基本权利、稳定承诺与人的最终责任

制度能够演化，不意味着一切都可由多数、平台或算法重新分配。首先应保护参与者作为人的基本地位：有机会知悉与自身有关的重要决定，能够质疑错误事实，拥有合理的隐私与退出路径，不因技术能力不足而被任意排除。不同组织和地区对这些要求有不同具体规定，本书不以技术模型替代适用法律；但在制度设计上，若没有最低限度的知情、申诉和责任通道，“共同治理”就缺少实际基础。

稳定承诺是第二条边界。参与者依据公开规则投入时间、资源与声誉后，制度不能在结果已出现时单方改写归属。应区分尚未形成的未来资格、附条件的期待、已经归属的请求和已经到期的履行义务。未来规则可以经过授权调整，既有请求则需要按原约定和适用法律处理；确有必要修改时，应说明依据、受影响范围、个别同意或过渡措施及救济。对不确定性的诚实披露，比含糊地许诺“永久权益”更能建立长期信任。

人的最终责任是第三条边界。模型可以推荐贡献分配，智能合约可以执行明确条件，共同账本可以保存决定过程，但谁制定评价目标、谁批准高影响变更、谁面对错误承担解释和补救义务，仍须落到可识别的人或组织。不能因为算法复杂，就把歧视性结果说成“数据自己的选择”；也不能因为多数节点同意，就取消受影响者的合理救济。技术越能自动行动，责任主体越需要在事前明确。

这些边界并非阻碍创新，而是区分“演化”与“漂移”。演化是观察后果、提出理由、征求意见、按权限修订并检验新结果；漂移则是在无人负责的参数更新、平台规则和默认设置中，使参与者的地位悄悄改变。判断一项修订是否改进，应同时看协作效率、真实成果、权利兑现、风险分配和受影响者的可参与程度，而不是只看交易吞吐量或短期总收益。

五、制度编译、回归检验与发布门槛

制度从文本进入运行，可以被理解为一个受治理的“编译链”：原则和条款先转化为主体、权限、状态、事件与约束，再转化为流程、配置或合约，最后在具体数据和行动中产生结果。这个比喻不意味着制度只是程序，而是要求每次转化都能回到上一级依据。若代码中存在一个改变收益的参数，却找不到相应批准文本；若文本承诺了申诉，系统中却没有可到达的入口，都说明编译链已经断裂。

制度层	主要产物	发布前检查	运行后证据
原则与规范	目标、权利义务、禁止事项、救济	权限来源、受影响者、基本权利和稳定承诺	解释、申诉与修订记录
决定与版本	提案、审议、批准、生效和过渡	决定者资格、程序完整性、版本适用范围	通知、接受、过渡和争议状态
规则模型	主体、状态、触发、约束、不变量	完备性、一致性、例外、不可达或危险状态	模型与真实案例的差异
实现与配置	程序、参数、权限、接口和迁移方案	代码审查、权限审查、边界测试、升级与回退	部署版本、实际配置和管理操作
运行与效果	交易、审核、支付、纠错和退出	监测、数据质量、职责分离、异常阈值	技术、制度和经营效果指标

回归检验用于防止一次修订破坏先前保护。每个版本至少应保留一组制度不变量和反例：未确认贡献不能直接产生到期收益；争议中的局部记录不能冻结无关请求；退出不能抹去已归属权利；任何高影响自动操作都能追溯到有效授权；紧急权限不能无限期持续。新版本即使提高效率，只要使这些保护失效，就不能以普通软件升级名义发布。

制度回归还要包含分布后果。相同规则可能对资源充足者和小型参与者产生不同负担；平均处理时间缩短，不能掩盖少数申诉被长期搁置。测试情景应覆盖不同角色、能力、信息和依赖程度，检查谁得到便利、谁承担新增证明成本、谁失去议价或退出能力。模型无法替代受影响者表达，但可以迫使设计者在发布前呈现这些差异。

发布门槛应与变更影响相匹配。低风险文字或界面修正，可以由受托运营者处理并留档；改变计算逻辑、权限或证据要求，需要独立复核和限定试验；改变收益资格、治理权、退出或救济条件，则应进入正式制度修订，并对既有请求作专门评估。软件部署完成不是制度生效的充分条件，制度批准完成也不表示技术已经正确部署。系统应分别显示批准、部署、核验和正式适用状态。

对于高影响版本，可以采用影子运行：新规则在不改变正式权利的条件下处理同一批输入，把结果与现行规则比较，发现差异后由有权主体审议。影子运行不能长期秘密评价参与者，也不能把实验结果用于事后追溯处分。其用途是暴露后果、验证迁移和准备救济，而不是绕过正式生效程序。

制度演化的最小闭环因此是：提出问题，形成可比较方案，检查规则模型，运行有限试验，公开影响，取得有效授权，分阶段发布，监测后果，提供救济，再决定维持、修订或回退。区块链可以保存版本和决定的关联，也可以约束部分发布条件；“哪一种后果值得追求”仍然必须由负责任的人和组织在可审议的制度中决定。

六、未来命题卡：受宪制约束的制度演化

项目	本章命题
可检验命题	将制度文本、决定版本、规则模型、技术实现和运行效果建立双向追溯，并对每次高影响修订执行不变量检查、有限试验和分阶段发布，可以减少规则意图与实际执行之间的偏离，同时保留有效修订能力。
适用对象	贡献确认、动态权益、跨组织结算、多方治理及其他规则会持续更新的数字制度。
成立条件	文本和模型能够对应；核心权利与稳定承诺被列为不变量；修订权限有效；试验不会把未经授权的状态伪装成正式权益；存在真实回退和救济能力。
主要风险	模型遗漏被误当作制度安全；仿真制造虚假确定性；频繁更新破坏预期；平台借技术发布绕过治理；回退只恢复软件而不补偿现实损失。
反证情形	双向追溯无法帮助发现偏离；高影响缺陷仍在正式运行后才暴露；参与者理解度下降；普通制度审查与数据库发布流程表现更优。
最小试验	选择一项影响范围有限的规则，完成文本—模型—实现—影子运行—正式决定—监测—救济全链条，并人为注入至少一种事实错误和一种权限错误。
观察指标	规则偏离发现率、发布前缺陷拦截率、版本误用率、修订周期、申诉可达率、回退与补偿完成时间、参与者理解度及不同群体承担的证明成本。
人的最终责任	制度制定者对目标和权利边界负责；技术团队对忠实实现负责；治理机构对发布与修订负责；义务主体对现实履行和损害补救负责。

这里的“可验证”始终是有范围的：可以检查明确写入的结构、约束和行为，不能证明未被表达的价值判断已经正确。这里的“可演化”也始终是受约束的：它允许在证据和审议基础上改善制度，不允许算法、平台或一时多数自行取得追溯改写基本权利和稳定承诺的权力。

本书从区块链的制度技术属性起步，经由数字资产转移、共同账本、共识机制、贡献证据、资本形成与多方治理，走到可演化制度的门口。未来的可能性不在于把所有关系写进一份不可更改的代码，而在于让共同创造的事实更容易被核验，让承诺更可靠地得到执行，让错误更有程序地得到纠正，让制度改进仍受参与者控制。这些都还是需要持续检验的命题。只有当技术始终服务于清楚的权利义务和真实的共同成长，它才配得上“利益相关者资本治理的底层技术”这一称谓。

定稿补强：把未参与者和退出者纳入制度反馈

制度反馈不能只来自活跃参与者。没有进入系统的人、曾经退出的人、少数群体以及受到间接影响的主体，往往最能揭示准入、成本、权力和救济的问题。只从成功完成流程的人取样，会系统性低估沉默、放弃和被排斥的成本。

制度试验应预先定义受影响群体，设置退出访谈、未完成路径、申诉与沉默数据，并允许独立研究或代表机制补充难以直接发声的群体。评价结果按群体拆分，检查平均改善是否掩盖少数人的显著损失。制度演化的证据，既包括系统内部的效率，也包括谁无法进入、谁承担代价以及谁选择离开。

本章工具与图表

本章的制度关系可结合[附录八](#)、[附录十三](#)使用。附录用于形成可填写、可核对的工作成果，不能把模板中的默认项视为已经生效的组织规则。

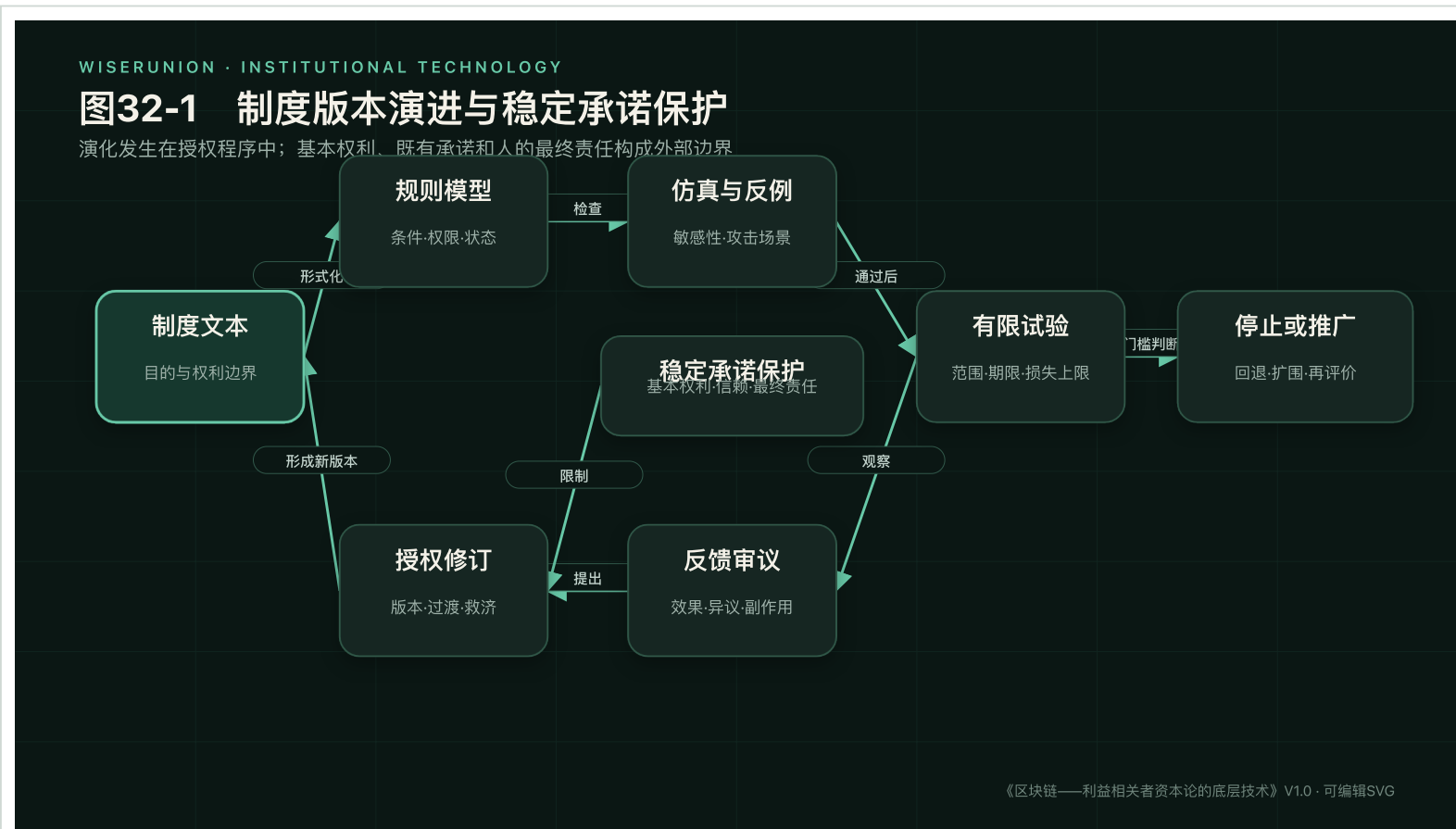


图32-1 制度版本演进与稳定承诺保护

图32-1 制度版本演进与稳定承诺保护。演化发生在授权程序中；基本权利、既有承诺和人的最终责任构成外部边界

本章注释

1. [SRC-056] Leslie Lamport: TLA+ 的模型检查资料。[原文或官方页面](#)

◦ 本章引证：TLA+ 的模型检查资料。

◦ 支持范围用于展示具体实现方式、工具接口或实践中的可行安排，本书引用主题包括：TLA+ 的模型检查资料。

- 使用边界：实现资料用于说明可行技术路径，不等同于独立安全审计、法律效力或经营效果证明。
- 证据等级：C（实现层或第三方技术资料，用于说明具体工具与实践）；链接状态：已完成可访问性核验，核验日：2026-10-08。

结语 让共同创造，成为共同成长的资本

本书从一个看似简单的区别开始：发送一份文件，接收者获得副本；转移一项资产，原有控制状态必须按规则失效，新的控制状态才可能成立。信息可以不断复制，而同一项资产不能仅因记录被复制就同时归属于多个有效控制者。区块链在一定条件下提供了多方共同验证状态转换的办法，也因此使数字技术更深入地进入授权、归属与权利变动的制度问题。

但走到这里，问题才刚刚开始。资产的控制能够转移，并不意味着现实中的物权已自动转移；交易能够得到协议确认，并不意味着其依据的交付事实真实；多个节点对账本状态达成一致，也不意味着参与者已经就收益和责任形成正当安排。技术可以可靠地执行一条规则，却无法仅凭执行的可靠性回答规则应当由谁制定、谁有权修改、受影响的人如何提出异议。

这正是把区块链称为“制度技术”所要承担的解释责任。它的意义不在于给传统合作换一套账本名称，而在于使某些制度关系具有可核验的记录、可约束的权限、可重复执行的程序与可追溯的变更。相应地，它的限度也应当清楚：链上的有效签名不自动证明现实中的合法授权，共享记录不自动证明输入事实的真实性，智能合约不自动创造履约资源，通证不自动成为资本或企业的全部权益。

共同创造比一次转账复杂得多。有人提出需求，有人投入资金和劳动，有人提供知识、组织协调或长期维护，也有人承担失败风险。贡献可能散落在不同岗位、企业和时间之中，其价值不总能在发生的当下被准确计量。一项交付被记录，不等于它已经被采用；被采用，不等于形成能够跨期发挥作用的能力；形成长期能力，也不自动确定谁拥有所有权、谁可以请求收益、谁有权参与治理。这些转化都需要相应的事实、组织吸收、制度依据和可履行的承诺。

因此，让共同创造成为资本，不是给每一项行为标价，也不是把所有参与者放进同一张积分榜。资本在这里指向能够持续支持共同事业的资源、能力和合作关系。若贡献确认只奖励容易记录的动作，而忽略信任、维护、照护和承担责任，技术就会改变人们的行为，却未必增加共同事业的力量。若权益凭证可以流转，却找不到负责兑现的主体，参与者得到的也只是形式上的占有。真正重要的是，从贡献事实到资本形成，再到具体权益及治理安排，能否建立可理解、可核验、可履行的联系。

这样的联系离不开组织。组织要对共同目标作出选择，提出判断贡献的标准，吸收成果并承担持续使用的成本；它也要决定风险由谁承担、收益依据什么分配、错误由谁纠正。区块链可以支持多方对这些过程中的关键状态形成共同记录，却不能替组织作出所有价值判断。将判断过程藏在算法参数中，反而可能使本应公开讨论的分配决定失去可见性。

共识机制同样如此。工作量证明、权益证明或许可型网络中的确认程序，各自规定谁能参与、怎样验证、如何处理冲突以及为安全承担什么成本。它们让“按规则形成共同账本”成为技术上可执行的过程，却不能代替社会中的目标协商、治理授权与争议解决。协议共识的力量，应当用于维护已经有正当依据的合作规则，而不是被误用为一切制度问题的最终答案。

在实际运行中，制度的质量往往由例外时刻决定。有人丢失密钥，证据被证明有误，自动分配遇到资金不足，贡献确认遭到申诉，组织需要退出协作网络，规则升级影响既有请求——这些情形不能简单归入“系统故障”。它们揭示一项制度是否说明了权利与义务的相对方，是否为人保留更正、解释和救济的路径。不可轻易改写的历史记录，应当服务于追溯责任；它不能成为拒绝承认错误的理由。

面向未来，权利义务关系可以比今天的静态账户得到更细致的表达。收益、治理、使用与退出条件可以分别编排；不同组织可以在有限范围内相互承认贡献凭证；人与智能体的协作可以留下更清楚的授权、行动与审核证据；规则可以在仿真、试运行和审议中逐步改进。这些可能性值得研究，也同样需要警惕。可编程不等于可以随意变更承诺，可组合不等于所有组织必须接受同一套价值尺度，可演化不等于由平台或模型持续改写人的位置。

衡量区块链是否真正发挥作用，需要回到合作本身。它是否使资产控制转移更可靠、重复确认和对账更少？是否让贡献依据更清楚、分配争议更容易处理？是否让参与者能够知道自己承担什么、可以请求什么、规则将如何改变？这些效果应与数据库、签名日志和其他组织安排在相近条件下比较，并同时计算技术维护、隐私保护、治理参与和退出迁移的成本。若更简单的办法足以支持同样的承诺，就应采用更简单的办法。制度技术的价值由它改善了什么来证明，而不是由它使用了哪一种名称来保证。

本书因此提出的，是一条持续研究和建设的路径，而不是一份已经完成的制度蓝图。路径的起点，是承认共同创造中的多种投入及其差异；中间，是为贡献确认、资本形成、权益配置与多方治理分别建立依据；落点，是让承诺能够履行、错误能够纠正、规则能够在参与者的授权下改进。每一步都可能失败，也都应允许检验、比较和修订。只有不把愿景冒充成果，未来的制度创新才可能获得可信的基础。

共同成长并不要求所有参与者得到相同的回报，而要求各方有机会理解共同事业如何形成、自己的贡献怎样被对待，以及未来的收益、责任与决定权为什么如此安排。它要求能够长期合作的人，不必只依赖某位管理者的记忆或某个平台的善意；也要求掌握技术和组织权力的人，对自己制定和执行的规则负责。

当可核验的事实与有依据的判断相接，当有效的权利与可承担的义务相接，当技术执行与人的审议、纠错和责任相接，共同创造才可能积累为跨越当期的能力，成为参与者愿意继续投入、也能够共同维护的资本。

让共同创造，成为共同成长的资本。

附录一 — 利益相关者资本概念与技术对象对照表

本附录把全书容易混用的概念转化为可检查的判断表。使用者应从业务事实和制度关系开始填写，不能先选定通证、链或账户，再反向把全部对象解释成资产或资本。

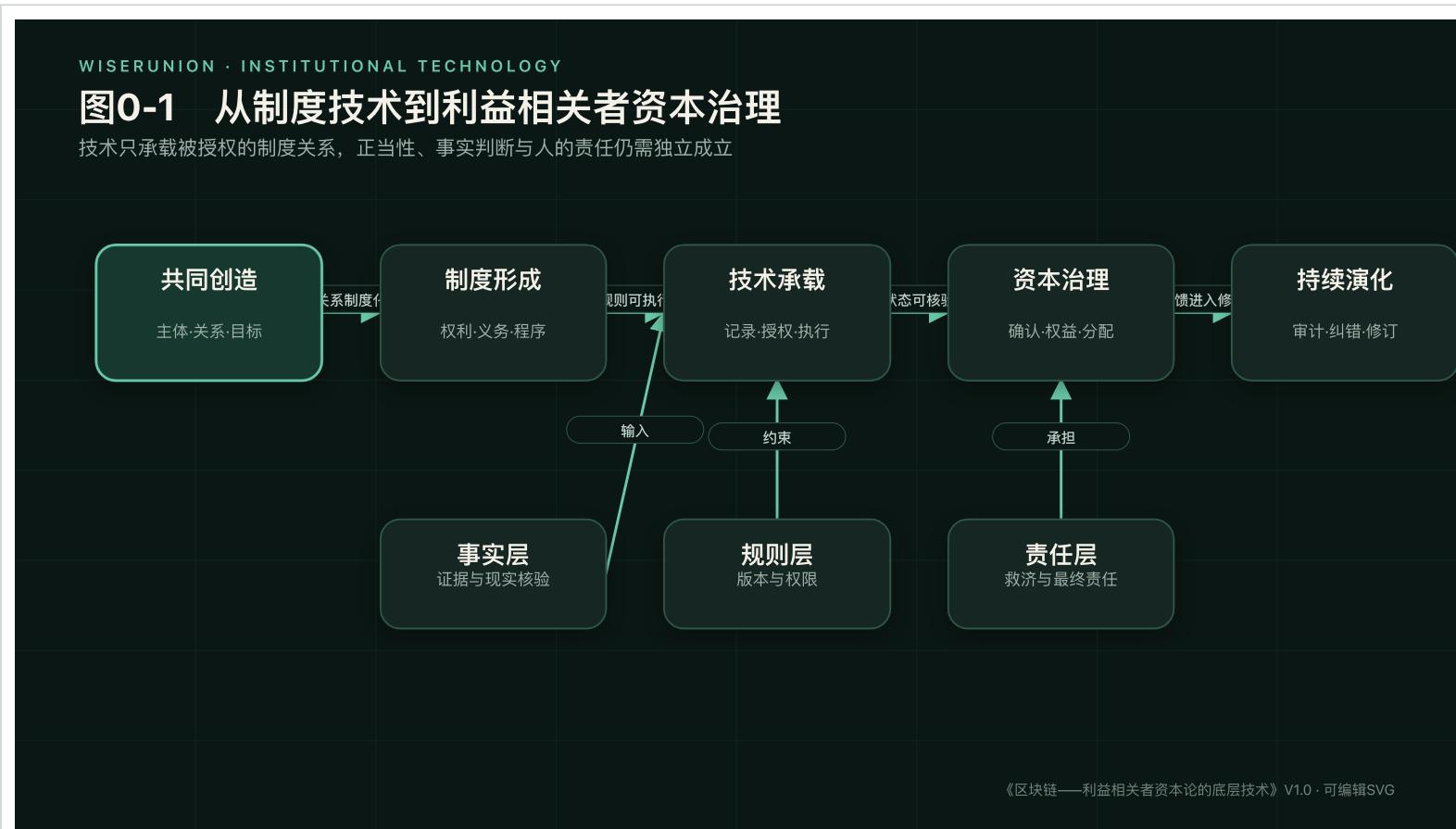


图0-1 从制度技术到利益相关者资本治理

图0-1 从制度技术到利益相关者资本治理。技术承载的是经过授权的部分规则；事实判断、制度正当性和人的最终责任保持独立。

一、概念对照

表A1-1 核心概念、判断问题与禁止推导

概念	本书工作定义	判断问题	不能自动推导	主要记录对象
数据	对事实、行为、状态或声明的符号表达	数据来自哪里，按什么格式形成	数据存在即事实真实	字段、文件、消息
记录	被特定主体按一定程序保存的数据	谁记录、何时记录、能否更正	记录一致即评价合理	事件、版本、时间、来源
资源	参与共同创造所需的资金、时间、知识、关系或设施	谁能支配，投入条件是什么	资源投入即形成贡献	资源标识、投入范围、限制
承诺	主体对未来行动、交付或责任作出的可识别表示	内容、期限、角色和违约后果是否明确	承诺即已经履行	承诺版本、签署、适用条件
贡献	已经发生并经相应程序确认的行动、投入、交付或结果	发生了什么，谁确认，证据范围多大	贡献即资本或所有权	贡献事件、证据、确认状态
价值	某对象对特定主体和目的的重要性或效用判断	谁评价、为何评价、时间范围是什么	分数即市场价格或经济价值	评价模型、范围、不确定性
资产	能够在既定制度中被识别、控制并带来相应利益或能力的对象	控制边界、权利依据和负担是什么	链上记录即法律资产	标识、控制状态、权利依据
数字资产	主要以数字状态存在或通过数字系统控制的资产	状态如何排他成立，谁能改变	私钥控制即所有权	状态、授权条件、转移记录
资本	被组织持续吸收、承担风险并跨期支持共同事业的资源、能力或关系	是否持续使用，是否进入风险与组织安排	可计量即可以资本化	形成决定、维持条件、终止状态
权益	依据制度、合同、登记或其他正当基础形成的具体请求或参与资格	谁对谁享有什么，在何种条件下兑现	收益权包含治理权或所有权	主体、义务人、内容、条件
账户	按既定口径归集状态与变动的记录结构	账户记录什么，不记录什么	账户余额就是法律权利	余额、期间、变动依据
凭证	对身份、资格、事实、状态或权利主张的可出示表达	谁签发、证明什么、是否可撤销	持有凭证即主张真实有效	签发者、持有人、声明、状态
通证	WISERUNION · V1.0 在特定协议中可识别并按规则流转或绑定的数字凭证或状态单位	为什么需要可转让、可替代或协议原生表达	通证即股权、货币或企业价值	202 / 240 发行、归属、锁定、转移、销毁

二、四层判断卡

表A1-2 记录、事实、评价与权利的分层检查

层次	需要回答的问题	主要证据	有权决定者	常见误读
记录可信	内容是否完整，版本和来源能否核验	哈希、签名、日志、共同账本	系统与记录责任人	不可篡改等于内容真实
事实可信	所声明行为或结果是否实际发生	业务材料、实物核验、独立证明	业务确认者、审计或争议机构	上链等于事实成立
评价合理	权重、分值和经济判断是否适合目的	评价模型、比较依据、敏感性分析	获授权的评价与治理主体	算法输出等于客观价值
权利有效	主体是否依法依约取得可执行请求	合同、章程、登记、有效决定	有权组织、登记或司法机构	持钥或持证即合法权利人

三、概念转化检查

表A1-3 从共同创造到权益的七个关口

关口	最低问题	合格输出	失败时处理
资源进入	投入者、范围和限制是否明确	资源投入记录	补充授权或不受理
贡献发生	行动、交付、使用与结果是否分别记录	贡献事件	退回补证或标记未完成
事实确认	证据是否覆盖所声称事实	确认结果及证明范围	异议、复核、部分确认
价值判断	评价目的、模型和不确定性是否公开	分项评价而非单一真值	人工裁量或暂停评价
资本形成	组织是否持续吸收并承担相应风险	资本形成决定	留在贡献账户
权益配置	权利主体、义务主体、内容和条件是否明确	权益登记	不生成或限制执行
兑现运行	资源是否可用，支付、治理和退出是否可执行	结算或参与结果	延期、冲正、救济、退出

四、工作记录模板

使用者应为每一个拟进入系统的对象填写下列字段：对象名称、概念类别、现实载体、技术标识、控制主体、制度依据、法律依据、记录责任人、更新条件、终止条件、可公开范围、争议处理路径。若同一对象同时被称为“贡献”“资本”“权益”和“通证”，必须分别说明其在四个层次的状态，不得用一个名称遮蔽多次判断。

五、使用边界

本表用于概念澄清，不代替会计确认、资产评估或法律定性。正文中的完整论证分别见第四章、第十六至十九章及第二十三章。技术控制、制度认可和法律权利的对应该检查见附录十二。

审读补强：治理资本与会计概念对照

制度对象	本书中的用途	不得自动推定	另行责任
贡献事实/分数	描述行为、证据和评价	会计金额、公允价值、交易价格	评价者与规则批准人
利益相关者资本	判断跨期能力和关系是否值得制度维护	财务报表资产、所有者权益、注册资本	治理机关与资本形成决定人
权益记录	表达具体请求、权限和限制	股权、负债或其他法定分类	法律与会计分类责任人
可分配资源	在义务、限制和储备后可用于分配的资源	收入、利润或现金余额可直接全额分配	财务、法律与治理批准人

每项数值必须记录计量目的、单位、基准日、方法、假设、不确定性、批准人和禁止用途。

使用与控制栏

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

附录二 – 区块链方案适用性判断表

本附录用于在技术选型之前判断问题是否真的需要共享账本。任何评分都必须在“硬边界”检查之后使用；若隐私、退出、治理或性能条件无法满足，较高的需求分数也不能把方案变成可接受方案。

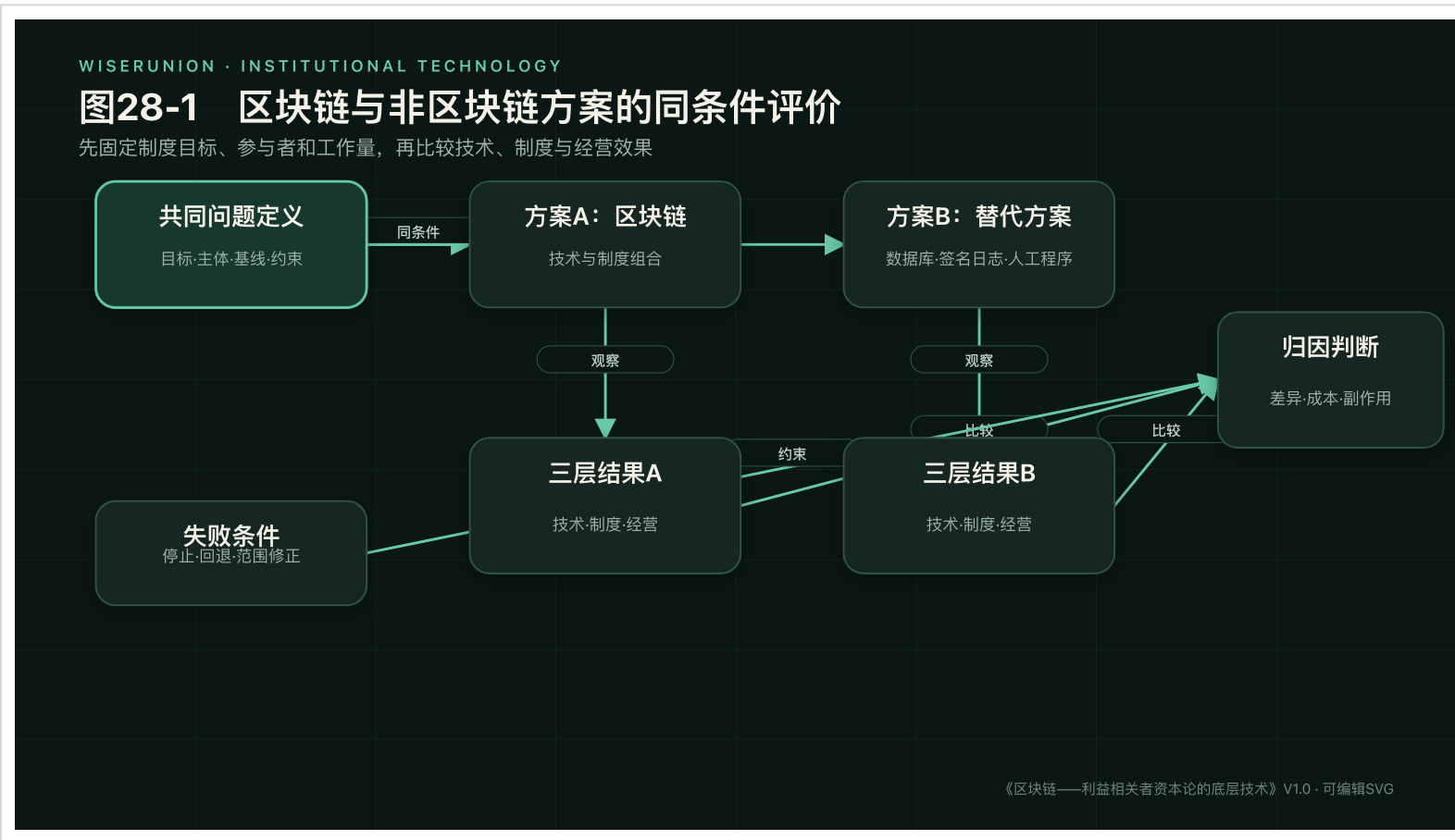


图28-1 区块链与非区块链方案的同条件评价

一、先行否决问题

表A2-1 硬边界检查

检查问题	是时的编辑判断	所需行动
单一可信主体可以合法、低成本地维护全部状态	区块链必要性较弱	优先比较数据库和签名日志
参与方并不需要独立验证共同状态	共享账本价值不足	明确普通数据共享方案
原始敏感数据必须永久删除且无法只记录最小摘要	公开或多副本账本可能不适合	改用链下存储或不采用
业务需要的吞吐、延迟或可用性无法由候选网络达到	技术条件不成立	更换架构或停止方案
没有明确的规则制定、升级、应急和退出主体	制度基础不成立	先建立治理制度
参与者不能承受节点、密钥、审计和长期维护成本	持续运行不可行	重新测算总成本或不采用
链上状态无法与关键链下事实建立可负责的输入路径	自动执行依据不足	补充核验制度或缩小范围

二、需求评分

每项按0—2分记录：0表示不存在或可忽略，1表示部分存在，2表示明显且持续存在。评分只用于比较需求强度，不是自动审批器。

表A2-2 共享账本需求评分卡

维度	0分	1分	2分	得分
多方独立参与	单一主体	少量受控协作者	多个利益不同的独立主体	

维度	0分	1分	2分	得分
共同状态需求	各自数据即可	定期对账	需持续共享同一有效状态	
相互核验价值	完全信任运营者	抽样核验	各方需独立验证	
单方改写风险	可接受	需审批控制	单方控制会损害关键利益	
资产重复成立风险	无	可人工处理	必须系统性拒绝冲突状态	
跨组织审计	单方审计足够	有联合审计	需跨机构连续追溯	
规则共同执行	人工程序即可	部分自动化	多方需要共同确认执行结果	
基础设施制衡	无要求	需合同约定	不能由单一平台掌握全部入口	
退出与迁移	可忽略	偶发需要	必须证明可独立带走状态与证据	
网络效应	无	局部互认	多方接入显著增加协作价值	

参考解释：0—6分通常优先非区块链方案；7—13分进入局部采用比较；14—20分可进入完整方案论证。任何结论都必须同时通过表A2-1，并完成表A2-3的同条件比较。

三、三方案同条件比较

表A2-3 候选架构比较记录

比较项	共享数据库	签名日志或透明日志	区块链或分布式账本
状态维护者			
独立验证者			
冲突与重复处理			
身份与准入			
最终性和回滚			
隐私与数据最小化			
性能与可用性			
建设及五年总成本			
升级、暂停和迁移			
供应商或平台依赖			
争议和法律执行			

四、结论规则

- 采用：存在持续的多方共同状态与独立核验需求，硬边界可满足，区块链方案相对替代方案具有可说明的净价值。
- 局部采用：仅把共同确认、关键状态或审计锚点放入分布式账本，原始材料、复杂计算和私人数据留在链下。
- 不采用：替代方案在相同制度目标下更简单、更便宜、更可控，或关键硬边界不能满足。

五、决策记录

最终记录至少包括：问题定义、参与主体、当前基线、候选方案、硬边界结果、需求评分、五年成本、重大风险、可逆性、退出路径、批准者、复审日期。决定采用区块链时，还要记录“不采用的最佳替代方案”，防止项目后续只与不存在的理想状态比较。

使用与控制栏

字段	填写要求
对象与适用范围WISERUNION . V1.0	说明组织、业务、群体、资产或系统边界

字段	填写要求
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

附录三 – 利益相关者身份、角色与权限模型

本附录把“是谁”“以什么角色参与”“能做什么”和“由谁承担后果”分开建模。自然人、组织和AI智能体都可能出现在系统中，但代理工具不能因可以签名或调用接口就被视为独立的最终责任主体。

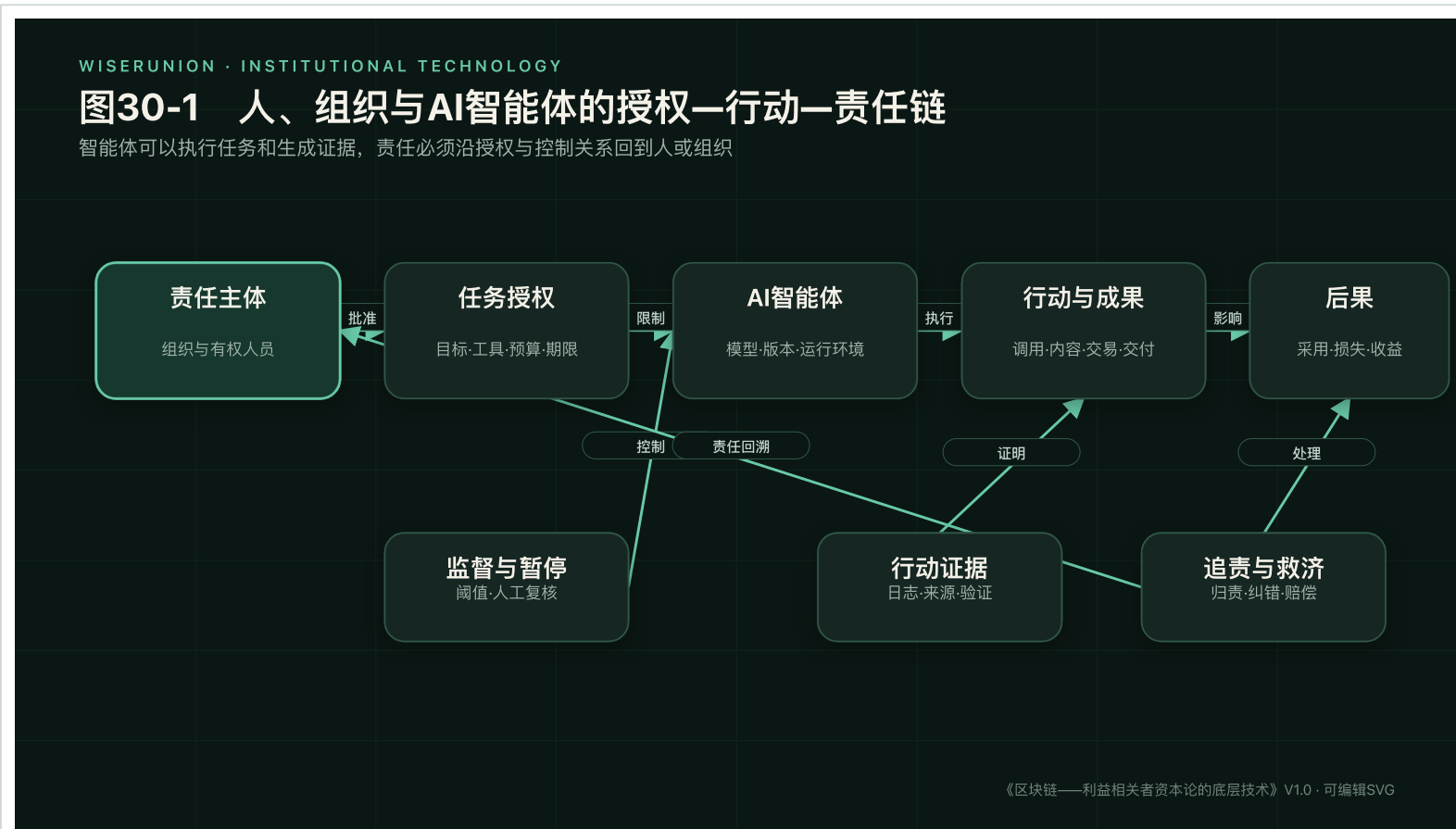


图30-1 人、组织与AI智能体的授权—行动—责任链

一、五层模型

表A3-1 身份与权限的五层分离

层次	核心问题	记录内容
主体	谁在现实中承担权利义务	自然人、法人、非法人组织、责任主体
身份	系统如何把表示与主体联系	标识符、凭证、核验方法、有效期
关系	主体与组织处于何种关系	员工、客户、供应商、成员、受托人
角色	在特定事项中承担什么职责	申报者、核验者、审批者、支付者、监督者
权限	可以对哪个对象实施什么行动	读取、提交、确认、修改、暂停、恢复、委托

二、角色—权限基准矩阵

表A3-2 最小职责分离示例

角色	提交贡献	核验证据	批准资本形成	配置权益	执行支付	修改规则	审计复核
贡献申报者	是	否	否	否	否	提案	查看自身
业务确认者	查看	是	建议	否	否	提案	提供材料
资本委员会	查看	复核	是	建议	否	提案	接受审计
权益管理员	查看决定	否	否	按决定登记	否	否	提供记录

角色	提交贡献	核验证据	批准资本形成	配置权益	执行支付	修改规则	审计复核
财务执行者	查看资格	否	否	否	是	否	对账
治理机构	查看	指定	授权	授权	监督	是	接收报告
独立审计者	只读	复核	只读	只读	只读	建议	是

矩阵是基准，不是固定组织架构。小型组织可以合并角色，但必须记录冲突、替代控制和复核方式。任何人不得仅因掌握系统管理员权限而自动取得业务批准权。

三、授权记录字段

表A3-3 授权最小记录

字段	要求
授权编号	全局唯一，能够被撤销和追溯
授权主体与代理	分别标识作出授权者、执行者及最终责任主体
角色与事项	说明本次授权适用的业务角色和对象范围
允许行动	采用明确动作列表，不使用“全部权限”等模糊表达
金额、频率和风险限额	对资产、数据和自动化操作设置上限
生效与终止	包括开始时间、到期、撤销、关系终止和密钥更换
转委托条件	是否允许、允许给谁、是否需再次批准
人工复核阈值	哪些情形必须暂停自动执行并交人处理
证据与日志	保存批准依据、调用记录、版本和异常信息

四、角色生命周期

角色应经历申请、核验、批准、激活、使用、定期复核、变更、暂停和终止。关系终止不一定自动删除历史记录，但必须停止未来权限；密钥仍然有效也不能继续代表已经终止的组织授权。恢复权限时应重新核对主体、角色和事项，不能只恢复设备访问。

五、多重身份与反操纵

系统应分别处理自然人的多个业务角色、组织的多个代理入口以及同一控制者制造大量虚假身份三类问题。反女巫措施可以使用实名核验、组织担保、押金、关系证明、行为分析或限额，但每种方法都可能带来排斥、隐私和权力集中。采用前要说明防范的具体攻击，不以“唯一身份”作为无限收集个人信息的理由。

六、AI智能体责任卡

每个进入生产环境的智能体都应记录：责任组织、业务所有者、模型与工具版本、可访问数据、允许调用、资金限额、禁止事项、人工复核阈值、暂停入口、输出标识、日志期限和损害处理人。智能体可以作为技术代理和事件参与者记录，但其行动不得切断对授权者、部署者和采用结果者的追责路径。

审读补强：代表、身份等级与密钥独立性

对象	必填控制
代表关系	所代表群体、事项、任期、利益披露、协商、报告、罢免、补位
委托关系	可否再委托、撤回方式、受托权重、集中度、关联方合并计算
身份等级	证明目的、最少字段、签发/验证者、期限、撤销、升级触发
多签/门限	密钥保管域、设备与人员独立性、阈值变更、恢复等待、恢复后撤销

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业/审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

本附录提供贡献记录的最小数据模型。模型刻意区分承诺、投入、交付、使用和结果，避免把“做过一件事”“交付了产出”“组织采用了产出”和“产生了结果”合并为一个无法复核的积分事件。



图14-1 从承诺、贡献到权益与回报

一、事件主表

表A4-1 贡献事件核心字段

字段	含义	来源	必填	隐私级别
event_id	事件唯一标识	系统生成	是	内部
event_type	承诺、投入、交付、使用、结果、修订、撤销	业务规则	是	公开或内部
subject_id	对应任务、项目、资产或关系	业务系统	是	内部
actor_id	实际实施行动的主体或代理	身份系统	是	受限
responsible_party	对行动承担最终责任的人或组织	授权记录	是	受限
role_id	行动发生时的角色	权限系统	是	内部
commitment_id	对应的事前承诺	合同或任务系统	条件必填	内部
occurred_at	现实行动发生时间	业务来源	是	内部
recorded_at	记录进入系统的时间	记录系统	是	内部
quantity_unit	数量及计量单位	业务材料	条件必填	内部
deliverable_ref	交付物标识与版本	档案系统	条件必填	受限
use_context	谁在何种业务中使用	使用方	条件必填	受限
result_claim	所声称的直接结果	申报者	可选	受限
evidence_refs	支撑材料清单	证据模块	是	分级

字段	含义	来源	必填	隐私级别
dedup_key	用于识别重复记录的业务键	规则模块	是	内部
rule_version	受理和确认采用的规则版本	规则登记	是	公开或内部
status	当前生命周期状态	确认程序	是	内部
supersedes	被本事件修订或替代的旧事件	审计链	可选	内部
privacy_class	公开、内部、受限、严格受限	数据治理	是	内部
retention_rule	保存期限与删除或归档条件	数据治理	是	内部

二、证据记录

表A4-2 证据对象字段

字段	说明
evidence_id	唯一标识，支持同一证据被多个事件引用
evidence_type	文件、签名、传感数据、交易记录、验收、证人说明、外部凭证
issuer_or_source	谁生成或保管该材料
claim_scope	材料能够证明什么，明确不证明什么
integrity_method	哈希、签名、可信时间、原件核验或其他完整性方法
storage_location	链下地址、档案编号或受控访问入口
availability_owner	谁负责在保存期内使材料可取得
verification_result	通过、部分通过、不通过、无法判断
verified_by	核验主体及其角色
verified_at	核验时间
challenge_status	无异议、异议中、已复核、已撤销

三、确认状态机

表A4-3 状态及允许转换

状态	含义	可转入	可转出	禁止效果
草稿	尚未正式提交	无	已提交、已取消	不得参与评价
已提交	申报完成，等待形式检查	草稿	待核验、退回补正、拒绝受理	不得生成权益
待核验	材料进入事实核验	已提交	部分确认、已确认、未确认、异议中	不得视为最终结果
部分确认	仅部分事实或范围成立	待核验、异议中	已确认、未确认、已修订	仅按明确范围使用
已确认	按指定规则和范围确认	待核验、异议中	异议中、已修订、已撤销	不自动形成资本
未确认	证据不足或不符合条件	待核验、异议中	异议中、已修订	不得计入确认贡献
异议中	结论受到有效挑战	任一确认状态	已复核、已修订	暂停不可逆兑现
已修订	新结论替代旧结论	已确认、部分确认、未确认	异议中	不删除旧历史
已撤销	原结论不再作为执行依据	已确认、已修订	原则上终止	不得继续用于新权益

四、重复记录与共同贡献

重复识别至少同时使用业务对象、行动类型、时间窗口、交付版本和责任主体。相同文件哈希可能表示多人共同交付同一成果，也可能是重复申报；不同哈希也可能只是格式变化。系统不得仅凭技术相似度自动删除。多人贡献应建立父事件和参与事件关系，分别保存共同成果、个人行为、归因方法和未能区分的部分。

五、最小示例

一个“客户培训手册”贡献至少形成：任务承诺、作者投入、版本化交付、业务验收、实际使用及使用后的结果观察六类记录。若手册交付但未采用，交付贡献可以成立，使用和经营结果不能据此成立。若后来修订，新增修订事件并关联旧版本，保留当时确认所依据的材料。

审读补强：语义版本与评价问责字段

贡献事件增加 namespace 、 schema_version 、 source_system 、 canonical_subject_id 、 prior_event_id 、 capital_decision_id 、 entitlement_record_id 与 distribution_batch_id 。评价记录增加理由代码、不确定性、评价者利益关系、复核者、偏差抽样和申诉结果。跨组织导入必须通过语义映射和测试向量，不以字段同名作为相同含义的充分条件。

使用与控制栏

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

本附录用于处理全书最关键的转换边界：贡献记录可以成立，但只有在组织持续吸收、承担风险并作出有效决定后，才可能进入资本记录；权益又需要独立的权利配置依据。

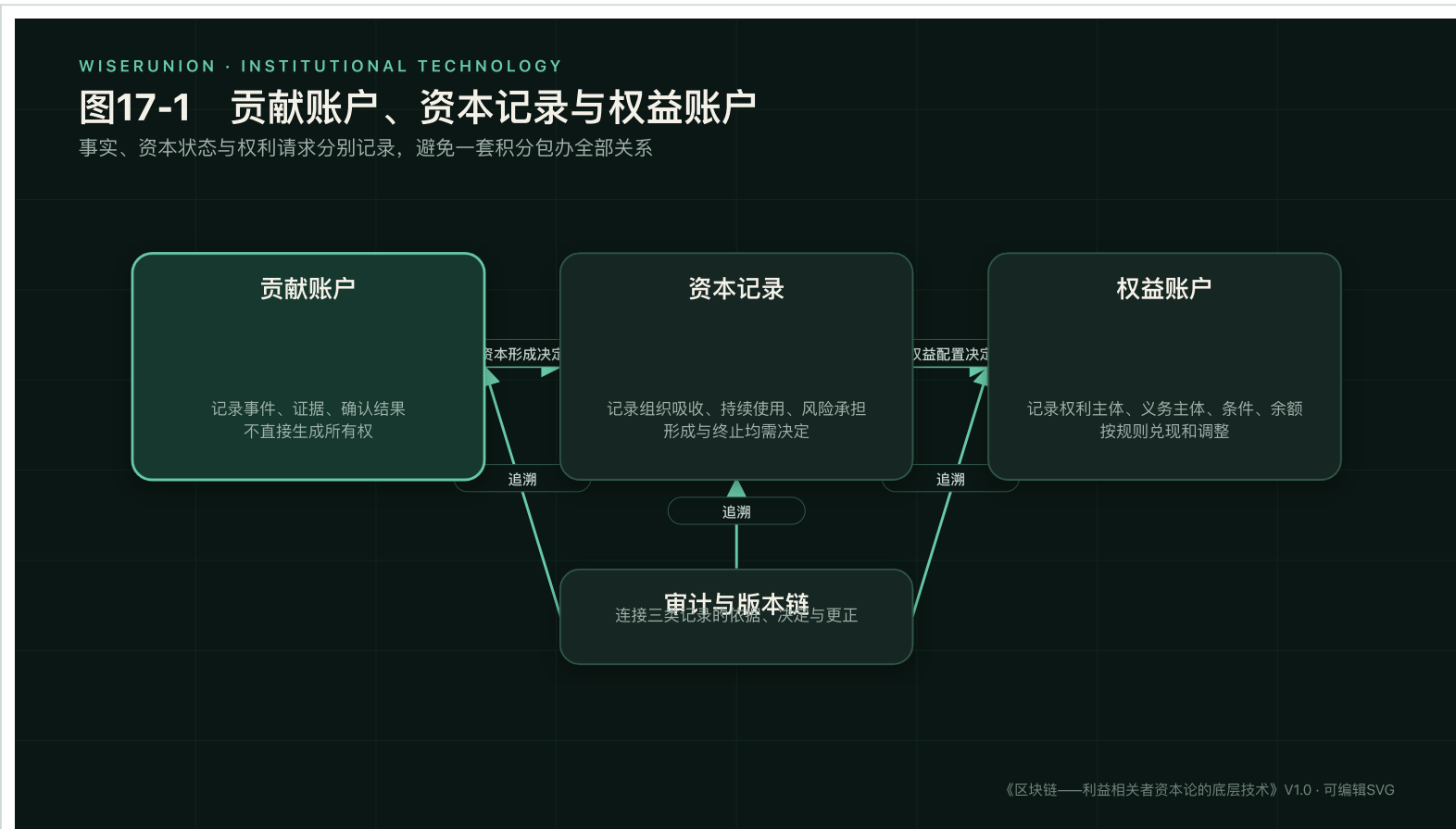


图17-1 贡献账户、资本记录与权益账户

一、资本形成门槛

表A5-1 六项必要判断

门槛	判断问题	合格证据	未满足时的状态
贡献事实	相应行动、交付或结果是否已经确认	贡献事件及确认记录	留在待核验或未确认
组织吸收	组织是否实际采用并纳入能力、流程或关系	采用决定、使用记录	保留为已确认贡献
持续性	价值是否跨越一次性交付并在一定期间存在	持续使用、维护或关系证据	一次性费用或奖励处理
风险承担	谁承担失败、维护、机会成本或损失风险	风险分配和责任记录	不进入资本或降低范围
可识别性	能否说明形成对象、范围与与其他贡献的关系	对象边界、归因与去重记录	合并记录或停止资本化
有效决定	有权主体是否按适用规则批准形成资本	议案、回避、批准、版本	不得自动生成资本状态

六项均通过并不必然形成会计意义上的资产或所有者权益。本书的“资本记录”服务于利益相关者资本治理；对外财务报告仍须按照适用会计准则处理。

二、资本形成决定书

表A5-2 决定书字段

字段	填写要求
WISERUNION · V1.0 capital_record_id	资本记录唯一编号

字段	填写要求
contribution_refs	进入本次判断的贡献事件清单
capital_object	形成的能力、关系、资源或其他资本对象
absorption_evidence	组织采用和持续使用的证据
risk_allocation	形成、维护和失败风险由谁承担
effective_period	开始、复核和可能终止的时间
valuation_scope	是否评价及评价目的；金额不得自动决定权益比例
approving_body	有权决定者、回避情况和表决结果
rule_version	适用的资本形成制度版本
maintenance_duties	谁维护，资源从何而来
termination_triggers	停用、失效、退出、替代或违法等条件
equity_follow_up	是否另行进入权益配置程序

三、权益登记模板

表A5-3 权益登记最小字段

字段	含义
entitlement_id	权益唯一标识
right_holder	权利主体；与密钥或账户控制者分别记录
obligor	承担给付、允许、结算或治理义务的主体
right_type	所有权、收益权、治理权、使用权或其他明确类型
right_content	可以请求、参与、使用或处分的具体事项
source_decision	合同、章程、治理决定、登记或法律依据
vesting_condition	归属、期限、绩效、继续关系或其他条件
transferability	可转让、限制转让、批准后转让或不可转让
exercise_method	账户操作、凭证出示、申请、表决或其他方式
suspension_and_revocation	可以暂停或撤销的条件及程序
priority_and_burden	优先顺序、税费、损失分担和其他负担
dispute_and_remedy	异议、复核、补偿、仲裁或诉讼路径

四、三账变动规则

- 贡献账户更正不自动反向删除已经依法依规形成的全部权益，必须判断更正影响和信赖保护。
- 资本记录终止时，应检查未兑现权益、维护义务和退出补偿，不能只把状态改为零。
- 权益账户的支付或转让不改写原贡献事实；必要时建立引用关系而非覆盖历史。
- 同一贡献可以支持多种权益，也可能不产生长期权益；必须分别批准并防止重复配置。
- 任何自动转换规则都要设上限、复核期、版本和人工停止入口。

五、登记前核对

- ☐ 权利主体和账户控制者已经分别核验；
- ☐ 义务主体有资源和权限履行；
- ☐ 权利内容不使用“共享价值”等无法执行的空泛表述；
- ☐ 条件、期限、转让和退出清楚；

- ☐ 与公司法、劳动、合同、税务、证券及数据规则的关系已经专项审查；
- ☐ 不利情形、损失分担和救济已经说明；
- ☐ 采用的是经授权且仍有效的规则版本。

审读补强：资本决定的专业边界

资本形成决定增加：关系类型与既有报酬、知识产权归属/许可、不得替代的法定义务、会计主体与适用准则、会计确认/费用化结论、发行人和持有人分类、税务审查状态。每项资本决定必须通过唯一标识关联贡献事件、权益登记和后续分配，禁止同一贡献在多条路径重复资本化。

使用与控制栏

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

附录六 – 制度条款与智能合约功能映射表

本附录把制度文本拆成机器可处理的条件、权限与状态，同时明确保留人工判断和不得自动化的事项。目标是让代码执行制度决定，而不是让代码开发过程替代制度决定。

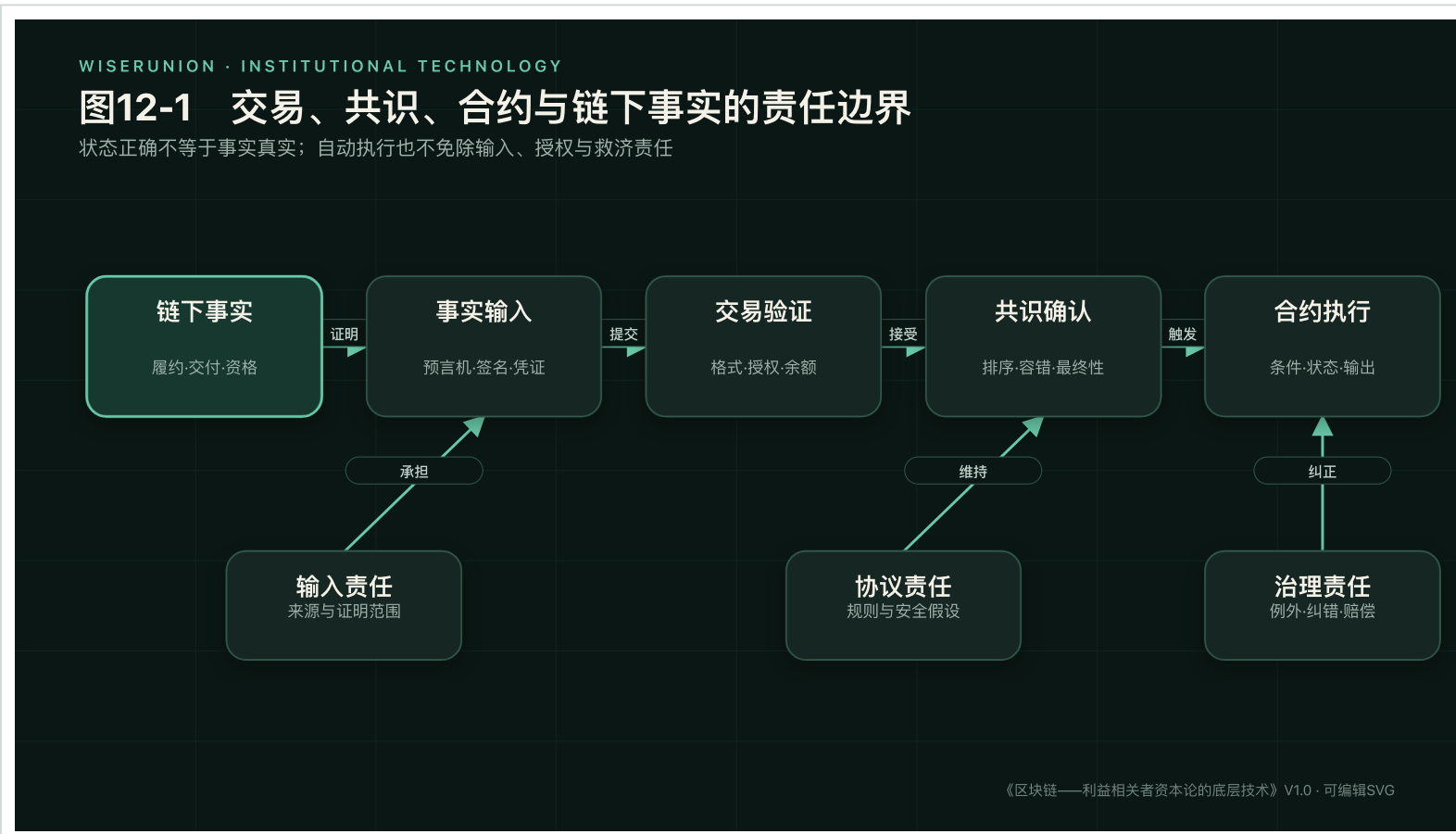


图12-1 交易、共识、合约与链下事实的责任边界

一、自动化分级

表A6-1 条款自动化等级

等级	适用条件	处理方式	示例
L1 可自动执行	输入可核验、规则确定、后果可逆或风险有限	合约直接转换状态并留下记录	到期解锁、限额内按比例分配
L2 自动计算后审批	计算规则明确，但事实、例外或重大后果需人判断	系统生成建议，有权人员批准后执行	贡献分值、较大支付、资格变更
L3 人工决定后自动落实	决定需要裁量、听取意见或利益冲突处理	治理决定形成后由合约实施	争议结论、权益撤销、规则升级
L4 不得自动决定	涉及基本权利、开放性事实或法律最终判断	只提供证据和流程支持	人格判断、违法认定、最终责任分配

二、映射主表

表A6-2 制度条款—功能映射字段

字段	填写说明
clause_id	制度条款和版本的唯一标识
policy_purpose	条款保护的利益和所要解决的问题
subjects	适用主体、角色及排除范围
inputs	所需数据、凭证、时间和外部事实
input_owner	谁对输入来源、完整性和更新负责

字段	填写说明
conditions	可以形式化检查的条件表达
authorized_action	条件成立时允许的最小行动
state_transition	旧状态、新状态及禁止状态
automation_level	L1至L4
approval_role	需要人工批准时的有权角色
exception_path	输入缺失、争议、不可抗力 and 特殊情况
pause_and_recovery	暂停者、恢复条件和超时处理
audit_events	必须保留的请求、判断、执行和错误记录
upgrade_rule	参数调整、重大修订和迁移程序
legal_and_rights_review	法律、基本权利和不利影响审查结论

三、示例：收益分配条款

表A6-3 示例映射

制度内容	技术表达	自动化级别	人工责任
只分配已经确认的可分配资源	收益批次状态必须为已确认	L1	财务确认收益来源
参与者按有效权益比例参与	读取指定快照和规则版本	L1	权益管理员保证快照依据
存在争议的账户暂缓	争议标记触发冻结队列	L2	争议机构决定释放或调整
重大亏损时可延期	触发阈值后停止自动支付	L3	治理机构审议延期、披露和救济
不得剥夺法定请求	合约不得自行覆盖外部权利	L4	法律和治理主体承担最终判断

四、合约发布门槛

发布前至少完成：条款文本批准、数据源测试、角色和密钥核验、边界值测试、重复执行测试、权限升级测试、暂停恢复演练、迁移方案、独立代码审查和最终业务验收。测试通过只能证明在测试范围内按模型运行，不能证明制度公平或外部事实真实。

五、版本与例外

合约地址、代码版本、参数版本和制度文本版本应分别记录。参数管理员只能调整被明确授权的参数；改变权利主体、分配原则、救济或退出条件属于制度修订，不得伪装成技术维护。紧急暂停用于限制损失，暂停者没有因此获得永久改变权益的权力。

审读补强：升级不变量清单

不变量	验收问题
权利语义	既有权利义务是否仅按获批内容改变
接口兼容	旧调用、事件和外部系统如何继续解释
状态完整	存储布局、余额、状态机和迁移前后是否勾稽
权限最小	升级、暂停和迁移权限是否扩大，何时撤销
证据连续	版本、提案、代码、部署、测试和快照能否追溯
失败处置	停止条件、回滚边界、外部后果和补偿如何处理

使用与控制栏

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

附录七 – 收益核算、分配与对账流程图

本附录把收益从业务来源到参与者实际收款的过程拆成可核对步骤。链上分配记录、银行或支付机构付款、会计入账和参与者可用余额是不同状态，必须通过批次编号和凭证建立联系。



图14-1 从承诺、贡献到权益与回报

一、流程

表A7-1 收益核算与对账九步流程

步骤	责任主体	输入	输出	异常处理
1 确认收益来源	财务与业务	合同、收入、成本、限制条件	收益来源清单	不明来源隔离
2 确认可分配资源	有权财务机构	现金、准备金、债务、法定限制	可分配批次	资源不足则暂停
3 冻结规则版本	治理与规则管理员	有效制度、参数、快照时间	batch_rule_version	规则冲突交治理审议
4 确认分配资格	权益管理员	权益账户、锁定、争议状态	合格主体清单	争议账户暂缓
5 计算分配结果	计算系统	批次、资格、比例、上限	计算明细	总额不平衡则拒绝发布
6 审批与发布	批准者	计算明细和例外清单	已批准分配批次	利益冲突者回避
7 执行支付	合约或财务	收款信息、币种、费用	链上交易或支付指令	失败进入重试队列
8 三方对账	财务、账本、支付方	分配记录、交易回执、银行流水	对账结果	差异分类和冲正
9 结案与申诉	审计和争议机构	对账、通知、异议	结案报告或调整批次	保留原批次历史

二、分配批次主记录

表A7-2 批次字段

字段	说明
batch_id	贯穿计算、链上交易、银行支付和会计凭证的唯一编号
source_period	收益对应业务和期间
distributable_amount	经批准的可分配总额及币种
reserve_and_losses	准备金、亏损和不可分配项目
rule_version	分配规则与参数版本
eligibility_snapshot	权益资格快照时间和摘要
calculation_hash	计算输入、程序和结果的完整性标识
approved_by	批准主体、回避和签名
payment_channels	链上、银行、第三方支付或混合路径
reconciliation_status	未执行、部分支付、已对账、有差异、已结案

三、三方对账

表A7-3 分配记录、实际支付与会计记录的核对

核对关系	必须相等或可解释的项目	常见差异
分配批次对链上交易	主体、金额、资产、批次标识、状态	Gas费、失败交易、错误地址
分配批次对银行支付	收款人、币种、金额、支付日、状态	手续费、退票、汇率、账户冻结
实际支付对会计凭证	总额、期间、科目、税费和冲正	跨期、扣税、支付在途
参与者通知对可用余额	应得、已付、暂缓、扣减及原因	显示延迟、争议冻结、提现限制

四、例外规则

亏损、资源不足、法律冻结、主体身份变化、错误地址和争议都不得通过静默修改结果处理。应建立原批次、异常事件、临时处置、批准依据、通知、最终决定和调整批次之间的引用。冲正使用反向记录或新的调整记录，不删除原交易。退出者的已归属权益、未归属部分、未决争议和后续责任分别处理。

五、结案条件

只有在总额守恒、每个参与者状态明确、差异已经解释、应付与实付可以对应、税费与会计处理完成、申诉期限已经说明后，批次才能结案。结案不妨碍后来发现重大错误，但后续更正必须进入新版本和审计链。

审读补强：分配瀑布与批次字段

分配顺序统一为：来源确认→成本费用与税费→法定/合同限制→储备与持续经营→可用现金或资产→治理批准→个体毛额→代扣、汇率与费用→净额支付→子账/总账对账。批次记录增加税费类型、代扣主体、汇率来源和时点、失败支付、重新支付、准备金、负余额、追回依据、截止性、总账凭证和唯一贡献链标识。

使用与控制栏

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态

字段	填写要求
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

附录八 – 治理提案、表决与规则升级流程图

本附录为制度规则从议题进入到实施、复核和退出提供统一流程。节点验证者、通证持有人、董事、员工代表或其他利益相关者是否拥有治理权，取决于明示制度，不由技术身份自动决定。

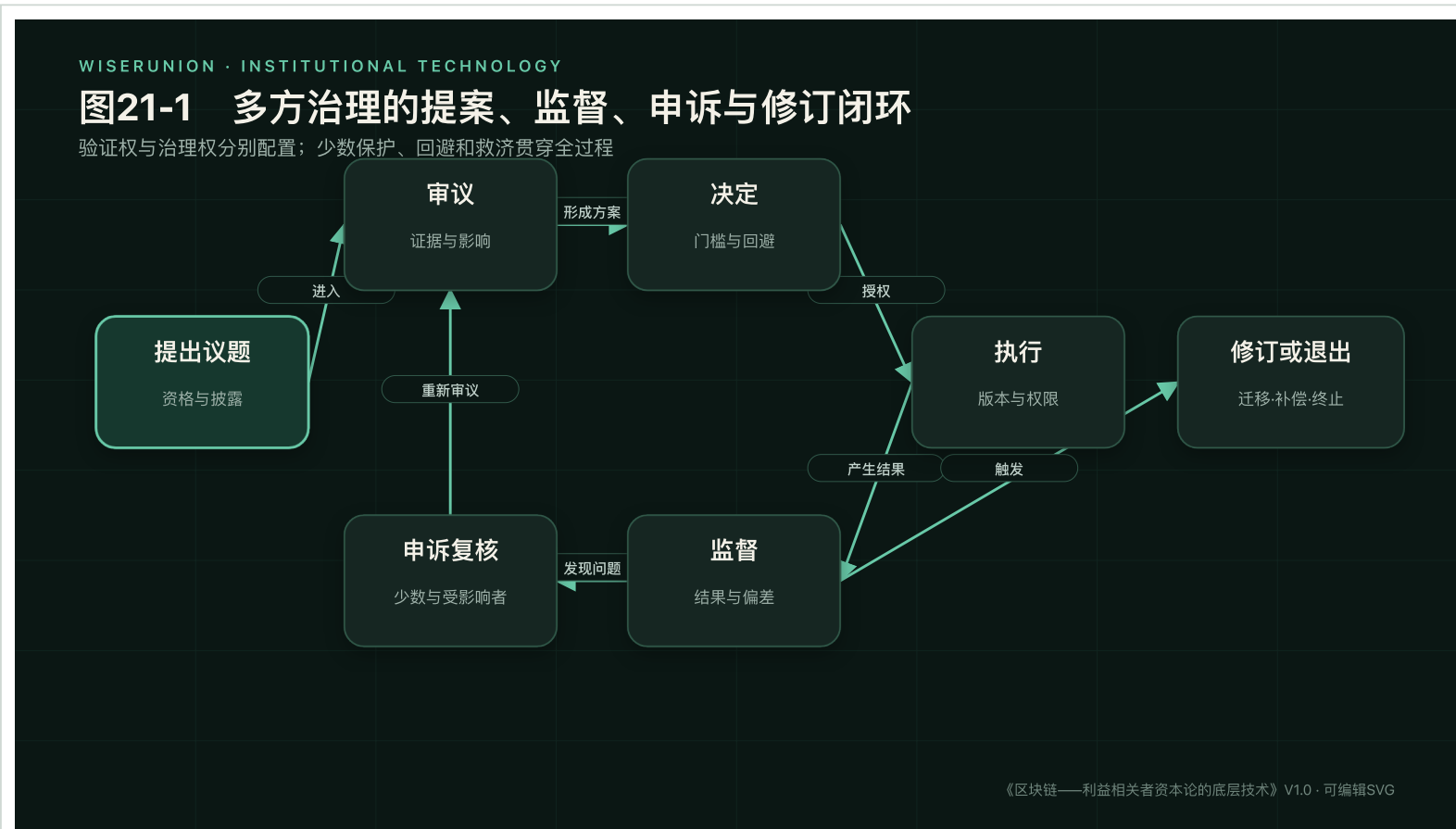


图21-1 多方治理的提案、监督、申诉与修订闭环

一、变更分类

表A8-1 变更等级与程序

等级	典型事项	最低程序	生效保护
G1 日常运行	不改变权利结构的业务配置	授权岗位审批、日志、定期报告	可即时生效，可回退
G2 参数调整	在既定边界内改变阈值、周期或限额	影响说明、回避、授权委员会批准	延迟生效、监控窗口
G3 重大制度修订	改变资格、分配、治理、救济或退出	正式提案、利益相关者审议、特别门槛	过渡期、异议和退出安排
G4 基本性变更	改变基本权利、组织目的或控制结构	最高治理程序及适用法律要求	强化同意、信赖保护、补偿或分离
E 紧急处置	正在发生的重大安全或合法性风险	有限暂停、理由记录、立即通知	自动到期、事后复核，不得永久改权

二、治理流程

表A8-2 从提案到复核

阶段	必要输出	否决或退回条件
议题登记	问题、提案人、受影响者、变更等级	无具体问题或权限不足
资格和冲突检查	提案资格、利益冲突和回避安排	重大未披露冲突
影响说明	权利、成本、安全、法律、数据和退出影响	无法说明受影响范围
公开审议	支持、反对、替代方案和证据	信息不足或参与程序失真

阶段	必要输出	否决或退回条件
形成方案	最终文本、代码、参数、迁移和测试	文本与实现不一致
表决或批准	选民资格、权重、门槛、委托和结果	法定人数或特别门槛未达成
延迟与异议	生效日期、挑战窗口和紧急停止入口	有效异议未处理
部署与迁移	版本、权限、数据、未决事项处理	验收失败或迁移不可逆风险超限
运行复核	指标、异常、少数影响和继续条件	失败条件触发

三、提案登记表

提案至少包含：编号、提出者、问题描述、现行规则、拟议文本、变更等级、授权依据、受影响群体、预期收益、直接和间接成本、替代方案、数据与隐私影响、安全分析、法律和财务审查、代码或参数变更、迁移、退出、测试、观察指标、失败条件和复核日期。

四、表决完整性

表决前冻结资格快照和规则版本；分别记录本人投票、委托投票、弃权、回避和无效票。权重来自什么必须可解释，不能把资产余额、节点数量或贡献积分未经授权直接当作治理权。多数决定仍受基本权利、法定权限、少数保护和利益冲突规则约束。

五、升级与分叉

升级应同时管理制度文本、合约代码、接口、数据结构和客户端。不同意升级的主体能否继续使用旧系统，是技术问题也是组织连续性问题。若形成分叉，必须说明资产和证据如何识别、义务由谁承担、名称与基础设施如何使用、个人如何退出，以及跨分支重复执行怎样防止。

六、紧急治理

紧急权限只允许实施预先界定的限制性行动，如暂停特定功能、限制额度或隔离输入。每次使用要记录触发事实、权限来源、作用范围、预计期限和恢复条件，并在限定时间内交常规治理程序确认、修改或终止。

审读补强：规则层级、委托、申诉与紧急治理

控制	必填内容
规则层级	基本规则、政策、参数、操作指令及各自权限和门槛
委托集中	自有/受托权重、关联方、再委托、撤回、异常复核
独立申诉	回避、材料访问、举证、时限、暂缓、再审
紧急权力	触发证据、最小范围、自动失效、追认、补偿、撤权
稳定承诺	是否追溯、既得结果、过渡、补偿、退出、基本权利
人类批准	高影响事项、双人复核、意见分歧和最终责任人

使用与控制栏

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

WISERUNION

· V1.0

224 / 240

附录九 – 安全、隐私、异常与恢复检查表

本附录覆盖的不只是共识攻击。利益相关者资本治理系统的关键资产包括密钥、身份关系、业务证据、规则版本、权益状态、支付能力、治理权限和恢复资料；任何一项失真都可能造成权利或责任错误。

一、威胁与控制检查

表A9-1 七域检查表

域	预防	监控	响应与恢复
密钥与账户	分级密钥、多签或门限、最小权限、离线恢复材料	异常签名、权限变化、失败尝试	轮换、撤销、迁移、历史行为调查
智能合约	独立审查、边界测试、升级限制、限额	异常调用、状态偏差、费用突变	暂停、修复、迁移、补偿决定
预言机与输入	多来源、责任人、证明范围、时间有效性	来源中断、偏差、重复和异常值	隔离输入、人工核验、重算和冲正
身份与权限	身份角色分离、到期、回避、反女巫	孤儿账户、权限累积、异常委托	暂停角色、重新核验、责任追溯
数据与隐私	数据最小化、分级、加密、保存期限	越权访问、关联风险、导出异常	限制访问、通知、修复、删除或不可用化
治理	分级变更、延迟执行、少数保护、紧急权到期	突袭提案、集中委托、投票操纵	延迟、复核、接管、撤销或补偿
基础设施与供应链	多区域、可替换接口、依赖清单、备份	节点故障、依赖漏洞、服务商中断	切换、降级、恢复、迁移与退出

二、上线前逐项核对

- ☐ 已识别会造成资产损失、错误权利、隐私伤害和治理接管的主要路径；
- ☐ 关键权限没有集中在未经说明的单一管理员或恢复入口；
- ☐ 合约、接口和数据结构有明确版本，旧版本停止方式已定义；
- ☐ 预言机停止、错误和串谋情景已经演练；
- ☐ 敏感原始数据不上链或仅在明确必要时采用受控方案；
- ☐ 备份能够实际恢复，恢复密钥与生产密钥分离；
- ☐ 系统停止时仍能查明权利、未决义务和争议；
- ☐ 服务商退出、链停止或成本骤升时有迁移路径；
- ☐ 紧急暂停不会由同一人永久改变权益；
- ☐ 事故通知、取证、补偿和对外责任主体已经指定。

三、数据生命周期

表A9-2 隐私生命周期控制

阶段	核心问题	最低控制
收集	本次判断真正需要什么	目的限定、最小字段、告知或其他合法基础
使用	谁为哪个目的使用	角色权限、用途绑定、选择性披露
共享	是否跨组织或公开	接收者、字段、期限、再使用限制
保存	需要保存多久及为何	保存表、可用性责任、定期检查
更正	错误怎样标记和修订	新旧记录关联、当前状态查询
删除或不可用化	哪些副本能够实际处理	链上最小化、链下删除、密钥与访问处置
退出与迁移	数据如何带走或封存	标准格式、完整性清单、责任交接

四、事件分级

表A9-3 事件级别

级别	情形	首要动作	治理要求
S1 观察	未造成影响的异常或弱信号	记录、分析、加强监控	定期报告
S2 局部	有限账户、数据或功能受影响	隔离、暂停局部、通知责任人	复核与修复验收
S3 重大	关键权益、支付、隐私或治理受到实质影响	启动应急、保全证据、限制损失	独立调查、补偿和治理审议
S4 危机	系统性错误、控制权丧失或组织连续性受威胁	全面接管或安全停机	最高治理与法律处置、迁移或终止

五、恢复目标与演练

每项关键能力分别记录最大可接受中断时间、最大可接受数据损失、最低降级服务、恢复顺序和依赖。至少每年进行密钥丢失、预言机错误、合约漏洞、治理账户被接管、链停止和服务商退出六类演练。演练必须产生实际恢复证据，不能以“已有备份”代替恢复成功。

六、异常结案

事件结案需同时说明技术根因、制度缺口、受影响主体、权利更正、经济补偿、责任归属、控制改进和复验结果。若无法恢复到原状态，应由有权治理程序决定替代履行、补偿、迁移或终止，而不能由技术管理员单方宣告“系统已恢复”。

审读补强：迁移、可用性、输入和数据责任

检查表增加密码资产清单与后量子迁移、历史验证环境、密钥独立性与恢复撤权；分别记录协议数据可用性、证据可取回性和业务连续性的所有者及恢复目标；记录预言机来源独立性、新鲜度、分歧、停机与降级；记录处理目的、必要字段、更正/删除替代、跨境和泄露；恢复结案区分技术状态、支付、现实履行和法律救济。

使用与控制栏

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

附录十 – 系统验收与技术效果评价指标表

本附录把“系统上线”与“治理改善”分开评价。指标分为技术、制度和经营三层，每项都要记录基线、分母、观察期和失败条件；没有对照或合理替代解释时，只能报告变化，不能宣称因果。

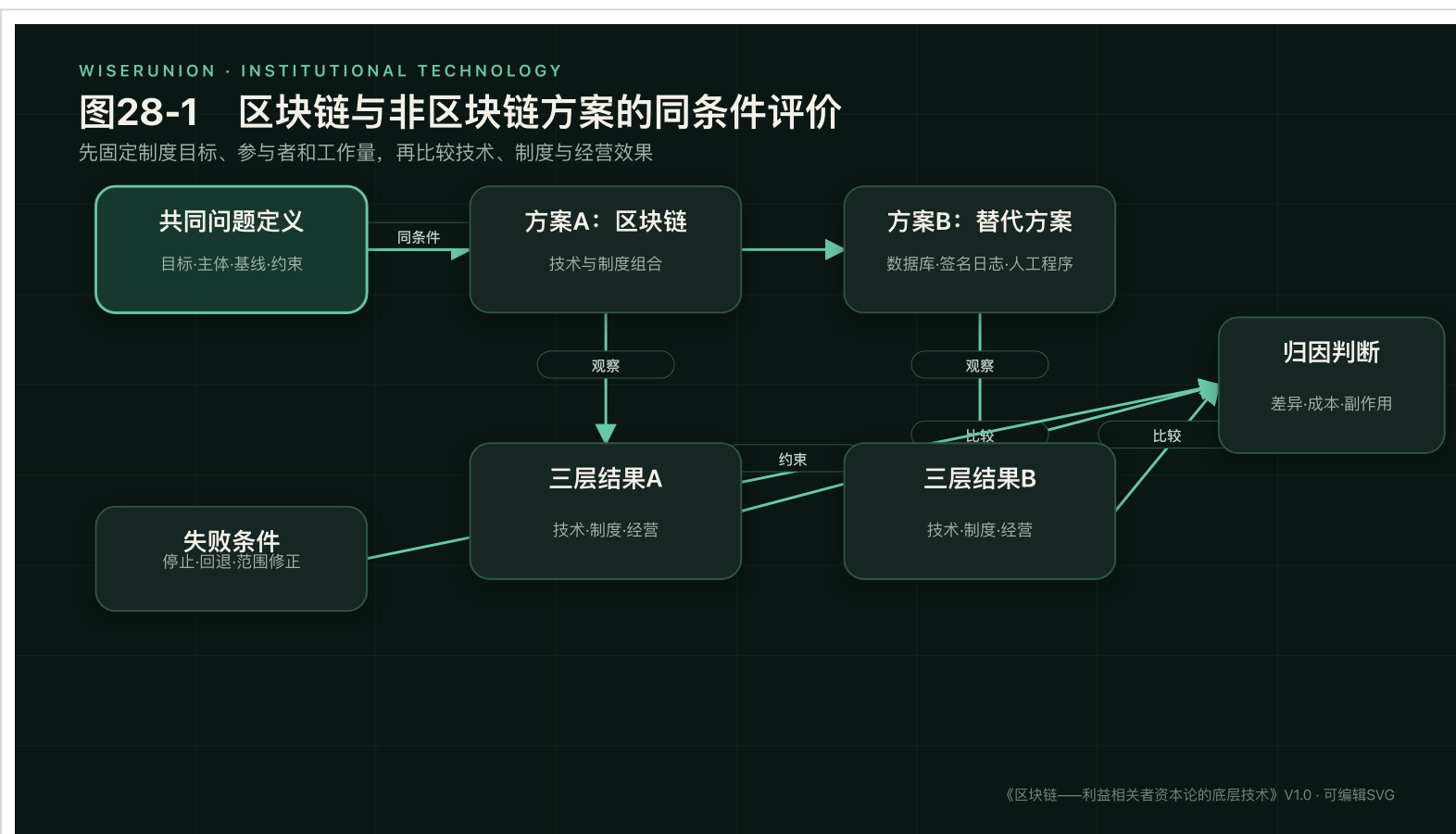


图28-1 区块链与非区块链方案的同条件评价

一、指标卡格式

表A10-1 每项指标必填字段

字段	说明
metric_id	唯一编号和所属层次
decision_use	指标影响哪项验收、继续或停止决定
numerator_denominator	明确定义分子、分母和排除项
baseline	改造前同口径数值及期间
target	目标、容忍区间和失败阈值
source_owner	数据来源、责任人和核验方法
frequency	采集和报告周期
comparison	对照组、替代方案或趋势比较方法
caveat	不能由该指标推出的结论

二、技术层指标

表A10-2 技术效果

指标	计算口径	必看边界
有效交易成功率	有效且最终确认交易数除以有效提交数	排除无效测试和重复请求
状态确认时间	从有效提交到满足业务最终性的时间分布	报告中位数和尾部，不只平均值
冲突拒绝正确率	正确拒绝冲突请求数除以已知冲突数	需有独立真值集
节点可用性	节点可验证时间除以应服务时间	不等同于端到端业务可用性
恢复达标率	演练中达到RTO与RPO的关键能力比例	以实际恢复为准
单笔总成本	基础设施、运行、审计和人工成本除以有效业务量	包含链下和治理成本
数据暴露量	每类参与者可见的非必要字段数或比例	同时检查关联推断风险

三、制度层指标

表A10-3 制度效果

指标	计算口径	失败信号
证据完整率	满足规定证据集的确认事件比例	关键字段长期缺失
确认一致性	复核者按同规则得到相同结论的比例	高分歧且无解释机制
异议处理时长	从有效异议到形成可执行结果的时间	争议长期冻结权益
更正闭环率	完成标注、冲正、通知和补偿的错误比例	只改状态不处理后果
规则可追溯率	结果能够定位规则版本、输入和批准的比例	无法重现关键决定
权限集中度	关键行动由最少多少独立主体可完成	单一入口可绕过治理
退出可行率	在演练期限内完成数据、状态和义务迁移的比例	退出依赖原运营者善意
少数保护有效性	不利决定中获得说明、复核和救济的比例	多数票直接终结全部权利

四、经营层指标

表A10-4 经营效果

指标	计算口径	归因限制
对账成本变化	同业务量下人员、时间和外部费用变化	同时记录业务规模和流程重构
争议损失变化	已确认争议造成的直接损失与机会成本	规则变化可能改变报案率
协作周期	从承诺到确认、结算和复核的周期	区分技术等待与人工等待
参与者净收益	收益与非经济价值减去时间、费用、风险和隐私成本	不用总收益替代分配公平
组织吸收率	被持续采用的确认贡献除以可采用贡献	需区分质量、资源和战略选择
长期协作留存	在可比较群体中的持续参与与退出原因	留存不必然代表自愿和满意

五、验收门槛

最小可行系统只有在关键状态正确、权限边界有效、异常可恢复、历史可追溯和退出可执行五项同时通过时，才能进入下一阶段。安全、法律或基本权利相关的关键失败不得用其他指标平均抵消。

六、评价报告结论

结论采用四类：技术达标且制度有效；技术达标但制度效果不足；制度流程改善但区块链无增量价值；关键条件失败应停止或回退。报告必须列出最佳非区块链替代方案、未能排除的外部因素和下一观察期，禁止只展示交易量、节点数或上链记录数。

审读补强：同条件基准与总拥有成本

技术指标增加工作负载、数据规模、并发、节点分布、P50/P95/P99、故障注入、网络分区、冷启动、恢复时间和重复次数。财务指标增加开发、基础设施、身份密钥、预言机、合规、审计、治理、升级、故障、迁移、培训和机会成本。比较统一功能单位、期间、币种、汇率/通胀、折现、数据质量、情景与敏感性。

使用与控制栏

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

附录十一 共识机制的制度维度比较表

本附录不把共识机制只理解为算法名称。比较对象包括进入资格、提议权、验证责任、最终性、成本、奖励、惩罚、集中风险和退出条件。实际网络可能组合多种机制，表中类型是分析框架。

一、统一维度比较

表A11-1 工作量证明、权益证明与许可型BFT

制度维度	工作量证明	权益证明	许可型拜占庭容错
参与准入	原则上以计算和网络资源进入	以质押资产及协议资格进入	由成员、运营者或治理机构许可
抗女巫基础	获得算力具有外部成本	获得并锁定有效质押具有成本	依赖身份核验和成员治理
提议权	通常按算力竞争获得	按质押和随机或轮次规则选择	按轮次、领导者或协议选择
验证职责	节点验证交易和累计工作链	验证者证明、投票和遵守罚没规则	已许可节点发送协议消息并达成门槛
冲突选择	累计工作最多等规则	最终性投票与分叉选择组合	达到法定节点门槛后确定
最终性	通常为概率性，确认随区块增加	可结合经济或协议最终性	常见为门槛达成后的确定性最终性
主要成本	能源、硬件、运维和机会成本	资本锁定、运维、惩罚和流动性成本	成员治理、身份、运维和通信成本
激励安排	区块奖励与交易费	奖励、费用、罚没和机会成本	可无原生奖励，由组织合同承担
违规约束	攻击需要持续资源，部分成本沉没	罚没、奖励损失和退出延迟	除协议排除外还可有合同与组织责任
集中风险	矿池、硬件、能源和网络集中	质押、托管、流动性质押和财富集中	成员选择者、节点少量化和运营者控制
弱主观或信任入口	软件、检查点和社会协调仍存在	新加入者可能依赖检查点与社会信息	直接依赖成员身份、配置和治理
退出	节点停止投入，资产转移视协议而定	提款期、退出队列和惩罚处理	成员变更、证书撤销和业务迁移

二、选择问题

表A11-2 机制选择提问

问题	需要的证据
谁需要防范谁	威胁主体、串谋规模和外部控制能力
谁有资格确认共同状态	准入理由、代表性和排除救济
安全成本由谁承担	资源、资本、合同责任和间接成本
谁从奖励和费用中获益	收入分布、集中趋势和行为激励
失败时何时可认为最终	业务容忍度、回滚和补偿能力
新参与者怎样知道正确历史	启动信息、检查点和可信来源
谁能改变验证者集合	正式权限、门槛、时间和争议程序
退出网络后如何保留权利与证据	数据导出、状态证明和未决义务

三、组合机制

应用层可以使用许可身份管理，同时把摘要锚定到开放网络；权益证明网络也可能采用确定性最终性协议；工作量证明系统仍依赖客户端规则和社会协调处理极端分歧。比较时应把“参与与抗女巫”“排序和最终性”“执行和数据可用性”“治理与升级”分别描述，避免用一个标签包办整个制度。

四、治理权边界

账本验证权是按协议确认交易和区块的能力。企业治理权是依组织制度决定目的、资源、分配和责任的权力。验证者可以拒绝协议无效交易，却不因此当然有权决定员工报酬、客户救济或股东权利。若组织确实授予验证者治理角色，授权来源、范围和冲突处理必须另行记录。

审读补强：分层比较矩阵

维度	工作量证明	权益证明	许可型BFT	必须披露
身份/抗女巫	计算与工作成本	质押与协议资格	组织身份和准入	虚假身份和准入风险
提议与验证	矿工提议、节点验证	验证者/委员会提议与证明	指定节点提议与投票	角色、轮换、失效
排序与执行	分叉选择后执行	分叉选择/最终性后执行	排序服务/共识后执行	排序权与有效性检查
最终性	概率稳定为主	检查点与经济/协议最终性	模型内确定性	逆转条件、等待与业务规则
安全/活性	算力、传播和验证假设	权益、验证者、同步与弱主观性	故障阈值和同步假设	分区时保护什么
激励与治理	奖励、费用、外部升级	奖励、惩罚、退出、检查点	合同责任与成员治理	集中、处罚、损失承担

任何具体网络都可能组合多种机制。本表比较的是制度维度，不把三类名称理解为功能完全对称的产品选项。

使用与控制栏

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

附录十二 链上控制、制度权益与法律权利对应检查表

本附录用于阻止“上链即确权”“持钥即所有”“凭证即权利”等跨层推导。每项重要资产或权益都应建立技术控制、制度认可和法律权利三栏记录，并说明三层不一致时的处理。

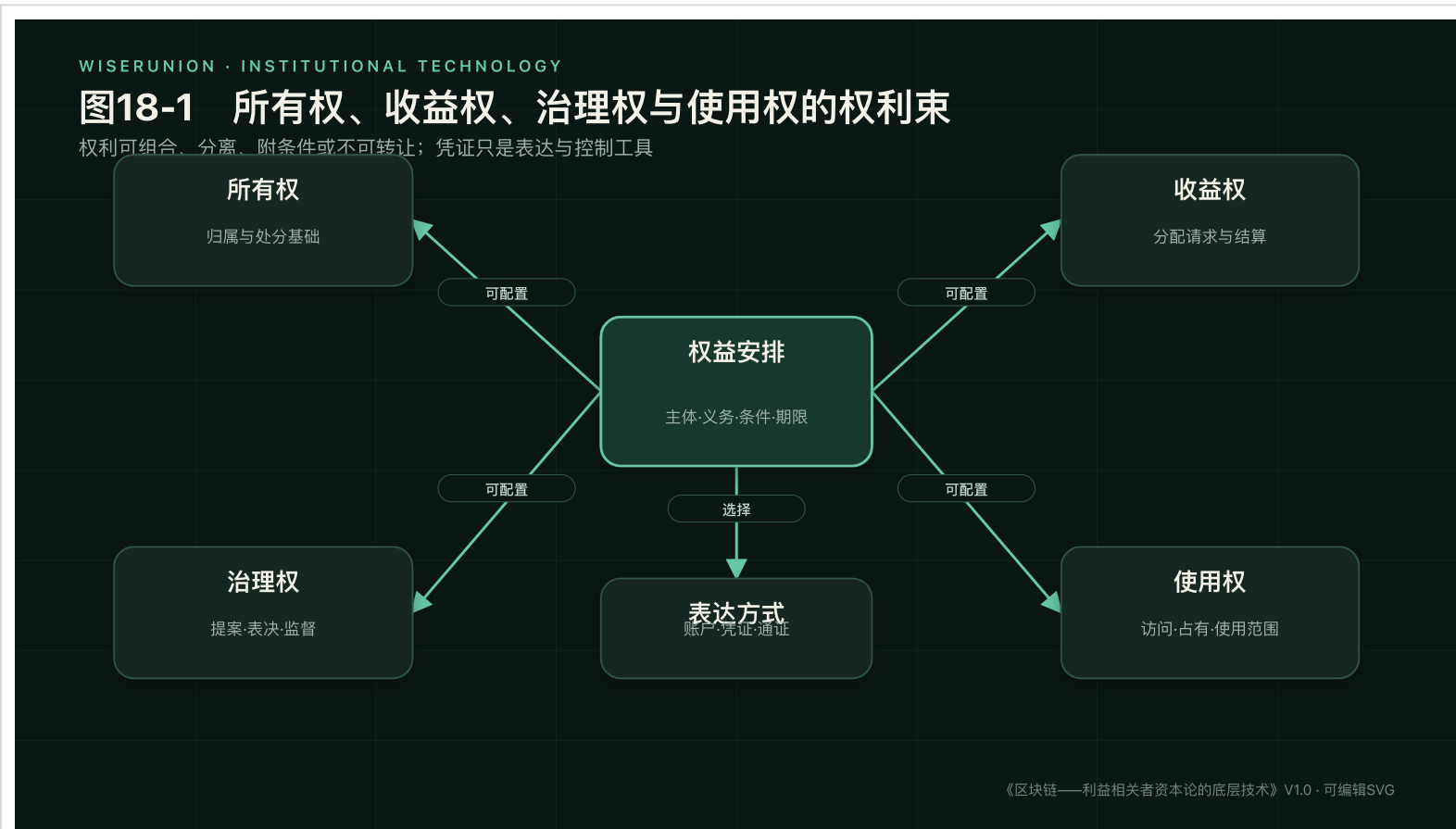


图18-1 所有权、收益权、治理权与使用权的权利束

一、三层对应主表

表A12-1 逐项核对模板

项目	技术控制	制度权益	法律权利
主体	哪个地址、账户或密钥满足控制条件	组织认可谁为权益人	法律、合同或登记确认谁为权利人
对象	哪个链上状态或凭证	哪项收益、治理、使用或退出请求	哪项物权、债权、成员权或其他权利
依据	协议规则、合约和签名条件	章程、计划、治理决定或账户规则	法律、合同、登记或有权机构决定
变动	交易、授权、更换密钥或合约调用	批准、归属、撤销、转让和冲正	交付、登记、通知、同意或法定程序
限制	锁定、多签、黑名单、暂停或额度	条件、期限、回避、不可转让	强制性规定、第三人权利、监管和司法限制
证据	交易回执、状态证明、签名和日志	权益账户、决议、版本和通知	合同、登记簿、证书、裁判或其他法定材料
救济	恢复、迁移、暂停和技术更正	申诉、复核、补偿和治理接管	仲裁、诉讼、执行及行政救济

二、常见不一致情景

表A12-2 三层分离及处理

情景	风险	处置原则
私钥被盗，链上资产已经转出	技术状态改变但原权利人未授权	保全证据、停止后续执行、依法依规判断返还与补偿
托管人控制账户WISERUNION · V1.0	控制者与权益人不同	明确受托范围、隔离资产、对账和退出交接

情景	风险	处置原则
员工代组织签名	操作者可能无业务决定权	核对组织授权、事项范围和权限有效期
通证可转让但合同权益不可转让	技术转移无法产生完整制度或法律效果	在协议中限制或要求外部批准与登记
权益已经终止但凭证仍可展示	旧签名有效，当前状态失效	提供撤销和状态查询，接收者检查时点
合约自动分配违反强制规则	技术执行完成但权利结果受挑战	启动暂停、冲正、补偿和法律处置
现实资产毁损而链上映射仍存在	映射与关联资产脱节	更新关联状态、披露风险、处理保险和责任

三、现实资产映射检查

- ☐ 关联资产可以被唯一识别，状态更新责任明确；
- ☐ 映射主体有权作出声明并持续维护；
- ☐ 实物保管、保险、负担、查封和毁损能够进入更新流程；
- ☐ 链上转移触发何种合同、交付或登记后果已经说明；
- ☐ 第三人和公共登记的优先关系已经审查；
- ☐ 凭证持有人能够取得必要信息并行使救济；
- ☐ 映射终止、资产替换、托管人退出和系统迁移已有方案。

四、权利束登记

所有权、收益权、治理权和使用权分别记录，不使用一个“所有者”字段隐含全部能力。每类权利必须包含权利主体、义务主体、内容、条件、期限、转让、优先、负担、行使方法和救济。若采用同一通证表达多项权利，仍要能够单独查询每项权利的依据和状态。

五、专项审查触发

涉及现实资产、融资、公开转让、消费者、劳动报酬、跨境数据、证券或集体投资安排时，必须进入适用法域的法律和监管审查。本表只能暴露问题，不能自行给出法律效力结论。

审读补强：法律分类与救济字段

每项对应检查增加：适用法域、对象类型（原生资产/合同请求/登记型权利/现实映射）、权利和义务主体、生效与第三人条件、代表权与签署形式、通证或发行分类、准据法与争议地、破产/优先顺位、技术纠错、现实履行和法律救济。未完成专业审查时，状态必须标为“制度模型，法律效力待确认”。

使用与控制栏

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

本附录把第二十九至三十二章的未来构想转化为可被限制、试验和反驳的研究命题。所有命题均属于本书提出的制度设计方向，不表示相关能力已经普遍实现。

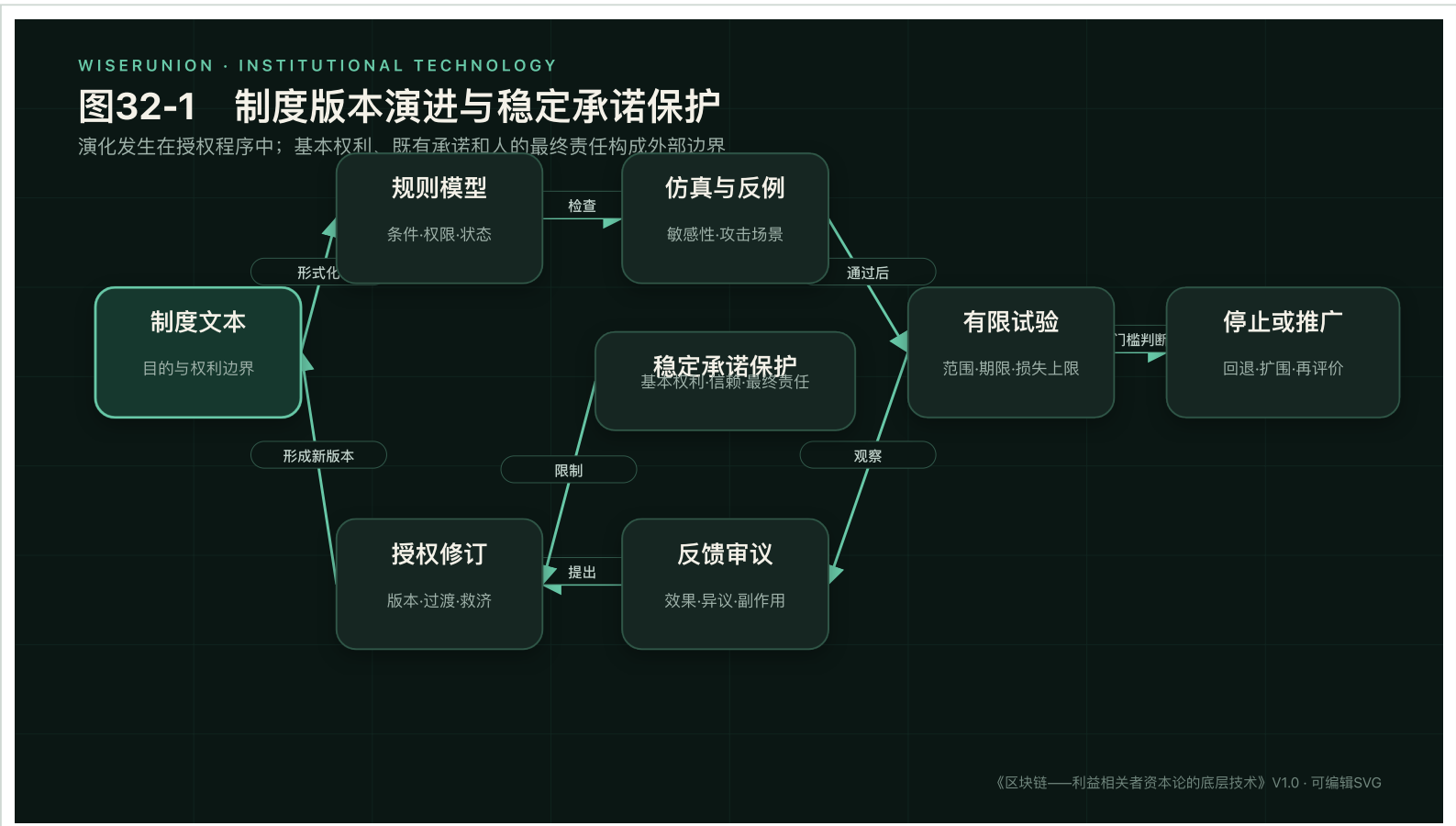


图32-1 制度版本演进与稳定承诺保护

一、统一命题卡

表A13-1 未来命题登记字段

字段	要求
proposition_id	唯一编号和对应章节
proposition	能够被事实否定或被条件限制的陈述
target_context	组织、协作网络、资产、任务和参与者范围
institutional_conditions	权限、责任、救济和稳定承诺条件
technical_conditions	身份、数据、协议、安全和可迁移条件
legal_conditions	适用法域、主体资格和不可排除权利
minimum_trial	主体、期限、资金、损失上限和退出安排
indicators	技术、制度、经营和不利影响指标
counterexample	足以挑战命题的情景或观察结果
stop_condition	必须暂停、回退或缩小范围的阈值
human_accountability	授权、监督、例外和救济的最终责任人

二、四组核心命题

表A13-2 命题、条件与反证路径

编号	命题	关键成立条件	主要反例或失败信号
P29-1	权益可以按贡献、责任、风险和时间依已授权规则动态变化，同时维持可预期性	规则公开、版本固定、追溯限制、申诉和退出	参与者无法预见变化，既有承诺被追溯改写
P29-2	可转让权益与不可转让关系可以在同一架构中协同	权利束分离、身份绑定、转让批准和义务继受	转让后义务无人承担，身份关系被商品化
P29-3	动态权益能够降低一次性分配的僵化	持续评价成本可控、数据可靠、变更有上限	频繁波动导致参与者无法规划和长期投入
P30-1	AI智能体产生的行动可以进入贡献证据链	任务授权、模型版本、行动日志和成果采用记录完整	大量自动活动被计作贡献但没有可识别价值
P30-2	人机协作能提高确认和分配效率而不制造责任空缺	人工复核阈值、责任主体、暂停和赔偿路径明确	人与系统互相推责，受影响者找不到救济对象
P30-3	可以识别并限制规模化虚假贡献和代理串谋	成本、身份、行为和业务结果交叉验证	攻击者以低成本制造大量互证并影响权益
P31-1	身份、贡献凭证和权利规则可以通过制度接口跨组织解释	共同语义、信任注册、验证规则和冲突处理明确	相同字段在两组织产生相反权利效果
P31-2	进入、协作、结算、争议和退出接口可以降低跨组织摩擦	接口开放、基础设施可替换、数据可迁移	互操作层成为新的单一控制者和收费入口
P31-3	组织可以互认有限事实而保留制度自主权	承认范围和非承认事项清楚	技术互联被误解为全面接受对方制度
P32-1	制度文本可以部分转化为可检查规则模型	条款结构化、歧义显式化、模型与文本可追溯	形式模型省略关键裁量和受影响者利益
P32-2	仿真和有限试验能在全面实施前发现部分制度缺陷	情景与反例充分、试验范围有限、观察指标可信	模型只验证设计者预设的顺利情景
P32-3	制度能够依据反馈演进，同时保护基本权利和稳定承诺	分级授权、过渡、信赖保护、人的最终责任	算法或多数借“优化”持续削弱少数和退出权

三、人一组织—智能体授权与责任矩阵

表A13-3 智能体协作矩阵

行为	人或组织必须决定	智能体可执行	必须保留的证据	责任不得空缺的位置
接受任务	目的、范围、禁区、预算和期限	解析任务和形成计划	授权文本、版本、接受时间	授权者对边界负责
调用工具	允许的系统、数据和额度	按策略调用	调用者、参数、返回值和时间	部署者对权限配置负责
生成内容	使用场景和质量标准	生成、修改和组合	模型、提示、来源和审校	采用者对实际使用负责
执行交易	资产、限额、对手方和复核阈值	构造并在限额内提交	授权、签名、交易和回执	账户责任主体承担后果
评价贡献	评价目的、权重和申诉规则	计算特征和建议分数	输入、模型、输出和人工决定	评价机构对结果负责
处理异常	暂停条件和升级路径	识别、隔离和通知	异常、处置和人工接管	应急负责人作最终决定

四、最小试验协议

每项试验必须限定主体数量、任务类型、最长时间、最高资金和数据暴露、可逆范围、对照方案及停止条件。试验状态不得与正式权益混淆；参与者应知道哪些结果只是模拟、哪些会产生现实后果。至少保留一条无需使用新系统即可提出异议和退出的路径。

五、反证与停止

命题不是通过展示一次成功案例获得永久确认。连续出现下列情况之一，应暂停或缩小范围：无法解释的权益变化；责任主体不可识别；少数申诉长期无结果；攻击成本显著低于收益；互操作依赖单一平台；试验损失超过上限；模型与制度文本出现实质偏离；基本权利或稳定承诺受到不可逆损害。

六、研究登记

每次试验公开或内部登记：命题、预注册指标、数据口径、对照、预计结果、反例、参与者保护、利益冲突、分析方法、负面结果和后续决定。模型和规则改变后不得继续沿用旧试验结论，必须说明哪些证据仍适用。

审读补强：智能体控制、稳定承诺与反馈代表性

智能体矩阵增加部署者、授权人、受益人、供应者、模型/工具版本、数据与许可、提示注入/工具滥用/投毒/漂移风险、沙箱、限额、熔断、证据和最终责任人。高影响事项标记人类批准与双人复核。制度试验同时采集未参与者、退出者、少数群体和间接受影响者的证据；任何动态权益试验都要检查追溯、既得结果、过渡、补偿、退出与基本权利。

字段	填写要求
对象与适用范围	说明组织、业务、群体、资产或系统边界
负责人/批准人	分别记录编制、维护、批准与独立复核责任
版本与日期	版本、生效日、复核日、失效或替换版本
证据与保留	证据位置、访问权限、保留期和删除/归档规则
法域与专业/审查	适用法域、法律/技术/治理/财务审查人及状态
状态与关闭证据	草案、试验、有效、暂停、终止；附批准、测试或复核证据

控制栏未填写完整时，本附录只能作为建模或审议工具，不能被表述为已经生效的合同、决议、登记、会计确认或系统控制。

本表收录 V1.0 正文实际引证的全部文献，核验日期为 2026-10-08。同一文献的页面、PDF和章节锚点已经归并；SRC 编号与来源数据库、章末注释一致。

链接可访问性仅表示核验时可以取得相应资源。文献的适用范围、版本变化、法律效力和事实证明能力，以章末注释和来源数据库所列边界为准。

法律、示范法与私法原则

- [SRC-004] 中华人民共和国最高人民法院网站：《中华人民共和国民法典》第114—127条、第209条、第224条，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-071] 联合国国际贸易法委员会（UNCITRAL）：电子签名示范法，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-072] 联合国国际贸易法委员会（UNCITRAL）：UNCITRAL《电子可转让记录示范法》概览，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-079] 国际统一私法协会（UNIDROIT）：Principles on Digital Assets and Private Law，A 级来源，2026-10-08核验，[原文或官方页面](#)。

标准与技术规范

- [SRC-006] 美国国家标准与技术研究院（NIST）：NIST FIPS 180-4: 安全哈希标准，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-007] 美国国家标准与技术研究院（NIST）：NIST FIPS 186-5: 数字签名标准，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-008] 美国国家标准与技术研究院（NIST）：NIST FIPS 204: 基于模块格的数字签名标准，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-023] Ethereum Improvement Proposals：EIP-1: 提案目的与流程，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-024] Ethereum Improvement Proposals：ERC-20 通证标准，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-025] Ethereum Improvement Proposals：ERC-5192 最小账户绑定通证接口，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-026] Ethereum Improvement Proposals：EIP-712: 结构化数据签名与重放保护边界，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-027] Ethereum Improvement Proposals：ERC-721 非同质化通证标准，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-069] RFC Editor：Certificate Transparency Version 2.0 (RFC 9162)，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-073] 万维网联盟（W3C）：去中心化标识符规范，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-074] 万维网联盟（W3C）：Decentralized Identifiers (DIDs) v1.0，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-075] 万维网联盟（W3C）：PROV Data Model，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-076] 万维网联盟（W3C）：Verifiable Credentials Data Model v2.0，A 级来源，2026-10-08核验，[原文或官方页面](#)。

学术与基础研究

- [SRC-002] Ethan Buchman、Jae Kwon、Zarko Milosevic：The latest gossip on BFT consensus，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-003] Satoshi Nakamoto：Bitcoin: A Peer-to-Peer Electronic Cash System，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-022] 测量指南联合委员会（JCGM）：Guide to the Expression of Uncertainty in Measurement, Part 1，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-048] Michael J. Fischer、Nancy A. Lynch、Michael S. Paterson：Impossibility of Distributed Consensus with One Faulty Process，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-055] Wesley M. Cohen、Daniel A. Levinthal：Absorptive Capacity: A New Perspective on Learning and Innovation，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-058] John R. Douceur / Microsoft Research：John R. Douceur：The Sybil Attack，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-061] 诺贝尔奖官方网站：Douglass C. North，诺贝尔奖演讲，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-062] 诺贝尔奖官方网站：Ostrom，2009，诺贝尔奖演讲，A 级来源，2026-10-08核验，[原文或官方页面](#)。

财务、审计与治理规范

- [SRC-045] 美国政府问责局（GAO）：内部控制《绿皮书》，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-051] 国际财务报告准则基金会（IFRS Foundation）：《财务报告概念框架》，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-052] 国际财务报告准则基金会（IFRS Foundation）：IFRS 基金会：IAS 38《无形资产》，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-053] 国际财务报告准则基金会（IFRS Foundation）：IAS 7 现金流量表，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-054] 国际财务报告准则基金会（IFRS Foundation）：IFRS 15 客户合同收入，A 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-067] 美国公众公司会计监督委员会（PCAOB）：AS 1105《审计证据》，A 级来源，2026-10-08核验，[原文或官方页面](#)。

官方指南与治理框架

- [SRC-001] 美国国家标准与技术研究院（NIST）：[NIST 的 AI 风险管理框架](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-005] 美国国家标准与技术研究院（NIST）：[多方门限密码学](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-009] 美国国家标准与技术研究院（NIST）：[基于属性的访问控制指南](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-010] 美国国家标准与技术研究院（NIST）：[NIST SP 800-57 Part 1 Rev. 5：密钥管理建议](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-059] 美国国家网络安全卓越中心（NCCoE / NIST）：[Accelerating the Adoption of Software and AI Agent Identity and Authorization](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-060] 美国国家标准与技术研究院（NIST）：[网络安全框架 2.0](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-063] 美国国家标准与技术研究院（NIST）：[《AI 风险管理框架 1.0》附录 C](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-064] 经济合作与发展组织（OECD）：[OECD／欧盟联合研究中心：综合指标的敏感性与稳健性](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-065] 经济合作与发展组织（OECD）：[董事会职责与利益冲突管理](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-066] 美国国家标准与技术研究院（NIST）：[数字身份指南 SP 800-63-4](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-077] 世界银行：[Impact Evaluation in Practice](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-078] 美国国家标准与技术研究院（NIST）：[Blockchain Technology Overview（NIST IR 8202）](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。

协议与项目文档

- [SRC-011] Bitcoin Project：[Bitcoin开发文档：工作量证明与分叉选择](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-012] Bitcoin Project：[Bitcoin开发文档：挖矿与矿池](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-013] Bitcoin Project：[比特币开发文档：运行模式](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-014] Bitcoin Project：[Bitcoin开发文档：交易](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-015] IPFS Documentation：[持久化、固定保存与垃圾回收](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-028] Ethereum.org：[以太坊开发文档：账户](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-029] Ethereum.org：[交易回执与区块状态查询](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-030] Ethereum.org：[Ethereum开发文档：共识机制](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-031] Ethereum.org：[Ethereum开发文档：权益证明](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-032] Ethereum.org：[Ethereum开发文档：Gasper](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-033] Ethereum.org：[Ethereum开发文档：权益证明奖励与处罚](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-034] Ethereum.org：[Ethereum开发文档：弱主观性](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-035] Ethereum.org：[数据可用性](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-036] Ethereum.org：[Ethereum开发文档：Gas与执行费用](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-037] Ethereum.org：[Ethereum开发文档：预言机](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-038] Ethereum.org：[Ethereum开发文档：智能合约简介](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-039] Ethereum.org：[Ethereum开发文档：智能合约的形式化验证](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-040] Ethereum.org：[Ethereum开发文档：智能合约升级](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-041] Ethereum.org：[Ethereum开发文档：交易](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-042] Ethereum.org：[质押提款](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-043] Ethereum.org：[零知识证明](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-044] Ethereum.org：[协议治理与参与主体](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-049] Hyperledger Fabric：[Hyperledger Fabric文档：排序服务及容错类型](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-050] Hyperledger Fabric：[Hyperledger Fabric文档：交易流程](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-068] PostgreSQL Global Development Group：[PostgreSQL：事务](#)，B 级来源，2026-10-08核验，[原文或官方页面](#)。

实现与工程参考

- [SRC-016] OpenZeppelin：[OpenZeppelin文档：延迟操作与时间锁](#)，C 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-017] OpenZeppelin：[OpenZeppelin 的 VestingWallet 文档](#)，C 级来源，2026-10-08核验，[原文或官方页面](#)。
- [SRC-018] OpenZeppelin：[延迟执行控制](#)，C 级来源，2026-10-08核验，[原文或官方页面](#)。

- [SRC-019] OpenZeppelin: OpenZeppelin文档: Pausable, C 级来源, 2026-10-08核验, [原文或官方页面](#)。
- [SRC-020] OpenZeppelin: 链上治理的权限、计票与执行配置, C 级来源, 2026-10-08核验, [原文或官方页面](#)。
- [SRC-021] Solidity Documentation: Solidity文档: 异常与状态回退, C 级来源, 2026-10-08核验, [原文或官方页面](#)。
- [SRC-046] OWASP Foundation: OWASP 关于智能体应用风险的资料, C 级来源, 2026-10-08核验, [原文或官方页面](#)。
- [SRC-047] Cloud Native Computing Foundation / CloudEvents: CloudEvents: 事件标识与来源规则, C 级来源, 2026-10-08核验, [原文或官方页面](#)。
- [SRC-056] Leslie Lamport: TLA+ 的模型检查资料, C 级来源, 2026-10-08核验, [原文或官方页面](#)。
- [SRC-057] Microsoft: Microsoft: 事件溯源模式, C 级来源, 2026-10-08核验, [原文或官方页面](#)。
- [SRC-070] Uniswap Labs: Uniswap: 价格冲击与流动性, C 级来源, 2026-10-08核验, [原文或官方页面](#)。