



研究附件

编辑日期：2026 年 9 月 25 日

网络中断时的分布式权限模型：数字国家服务中安全本地决策的边界

Delegated Authority Under Network Partition: An Exhaustive Toy-State Study and a Research Protocol for Safe Offline Public Services

MERIDIAN FUTURES LAB | M02 Scientific Companion | Working Paper 1.0 | 编辑日期：2026 年 9 月 25 日

实际类型：概念性批判工作论文，包含已完整执行的有限状态空间穷举计算（Conceptual Working Paper with an Executed Bounded Exhaustive State-Space Exploration）。本文不作为沙特原始运行研究、完整安全证明或同行评审论文发表。

证据截止日期：2026 年 9 月 25 日。拟议研究计划期间：2026—2035 年。

中文摘要

本文研究的问题不同于中断期间服务是否“可用”：当数字系统无法实时核验共享登记信息时，它能够行使的本地权限上限在哪里，才能同时维护权利不变量与受益人安全？我们区分四类行为：查看已签名副本、临时接收申请、兑现稀缺或唯一权益，以及取得可强制执行的最终决定。本文把这一区分与一致性即逻辑单调性（Consistency as Logical Monotonicity; CALM）、避免协调（Coordination Avoidance）、无冲突复制数据类型（Conflict-Free Replicated Data Types; CRDT）的适用边界，以及“北极星项目”（Project Polaris）离线支付设计面临的难题联系起来。

本文使用三组证据：2025 年 4 月 28 日伊比利亚停电，以及西班牙银行（Banco de España）和欧洲中央银行（European Central Bank; ECB）记录的支付渠道中断、现金优势及其分配限制；英国图书馆（British Library）在 2023 年 10 月遭受攻击后，部分功能继续运行、其他功能中断的情况；以及沙特关于银行业和数字政府业务连续性管理的公开文件。这些证据都不能用于估计沙特服务中断概率或真实本地权限，却能帮助我们界定可检验的问题。

我们对一个有限合成模型进行了完整计算穷举：两个彼此隔离的地点、三个共同权利单位、每个地点五种可能的本地需求量（0 至 4），以及五项决策策略，共计 25 种需求状态和 125 次策略评估。在盲目本地批准策略下，25 种状态中有 13 种突破共同上限；把额度分割为两个单位和一个单位，则在诚实执行本地规则的前提下，于所有状态中守住上限，但把所有状态的差额相加，相较联网基线少完成了十个可安全完成的单位。这只是对假定抽象状态的穷举计数，不是统计概率，也不是对真实设施的推断。另一个示例表明：仅有有效密码学签名，并不能阻止同一凭证副本在两个地点被重复使用，除非还有相应的协调机制或物理保障。

本文提出为每项服务建立“离线权限档案”（Offline Authority Profile; OAP），并设计一套经授权的测试协议，在权利安全、实际完成量、积压、公平性和审查成本之间进行权衡。本文的贡献在于整理问题、条件和测试方法，并明确指出：在某些场景中，停止或作出临时承诺，比完成一项不可逆决定更诚实、更安全。

关键词：有界本地权限（Bounded Local Authority）；网络分区（Network Partition）；应用不变量（Application Invariants）；避免协调（Coordination Avoidance）；托管额度分配（Escrow Allocation）；双重支付（Double Spending）；签名有效性（Signature Validity）；后续对账（Reconciliation）。

English abstract

The research question is **which public-service decisions can be safely authorized locally during a network partition**, rather than simply which interfaces remain operational. A distinction is made among viewing signed and time-bounded information, receiving provisional intent, consuming preallocated scarce authorization, and making final decisions that require shared, fresh knowledge. The synthesis draws on CALM, invariant-confluent coordination avoidance, conflict-free replication, and the Bank for International Settlements' Project Polaris research on offline payment design. Documented case evidence covers the April 2025 Iberian blackout and payment disruption, the British Library's post-2023 partial-service restoration, and Saudi rules on institutional business continuity.

An **executed, fully synthetic, bounded exhaustive analysis** explores 25 demand states at two disconnected sites under five decision policies. The global scarce authorization budget equals three invented units. Blindly letting each site independently commit against the old global balance violates the shared quota in 13 of 25 cases. Honest, disjoint escrow allocation preserves the quota in all enumerated cases but yields 10 fewer safely finalized units in aggregate than an always-connected benchmark. These are **counts of constructed abstract states, not estimated risks, probabilities, Saudi results, or guarantees against adversarial compromise**. A

separate replay counterexample illustrates why a valid issuer signature alone does not ensure unique offline redemption. We propose an Offline Authority Profile and an authorized measurement protocol with explicit outcomes, safety invariants, revocation constraints, appeal handling, and distributional assessment.

Keywords: offline public services; delegated authority; safety invariants; network partition; application semantics; bounded escrow; digital identity; payment resilience; Saudi Arabia.

1. 分析单元：改变权利的行为

业务连续性（Business Continuity）讨论常常迅速落入基础设施词汇：第二台服务器、备用区域、备用连接、降级模式。这些手段都很重要，却没有直接回答一个问题：如果完成某项行为所需的共享信息缺失，该行为产生的后果是否仍然有效。本地设备可以继续接收申请，但接收申请不等于最终处分一项法律或财产权利。因此，本文选择不同的分析单元：经授权的状态变更行为（Authorized State-Changing Action）；对于不改变状态的读取行为，则必须说明其证据的新鲜度。

核心问题是：当与共同权威的中断持续时间未知时，分支机构、地点、设备或服务代表在什么法律、信息、密码学与运行条件下，可以完成一项具体行为，同时既不超出所获授权，也不产生无法修复的冲突？

本文提出五个子问题：

1. 哪些决定在以后收到新增信息时仍然有效？哪些决定依赖于知道远方并不存在另一项权利或限制？
2. 密码学签名有效，与资源或授权只能使用一次，有什么区别？
3. 如何在彼此独立的地点之间分割稀缺权利，而不突破全局登记的不变量？未使用额度的代价是什么？
4. 什么时候，临时登记意向能够带来社会价值，又不会把回执变成不实的最终承诺？
5. 如何同时依据服务法律、人的真实可达条件，以及设备、电力和时间分配不均，检验本地能力？

本文的目标是概念与设计研究，辅以一个已经完成的说明性计算模块。本版不检验全国层面的因果关系，不推断故障或暴露发生率，也不验证真实支付系统的安全性。本文把功能、法律、安全和社会评估分开：一台示例状态机即使守住了数字上限，也不会因此自动获得机构采用资格。

假设与反证指标

H1——有条件的预先授权：某些行为的不变量可以通过有权主体授予、彼此隔离的有限授权在本地维护，前提是具备证据、签名、审计，并向用户如实说明申请状态。

H2——中断时无知的边界：另一些行为需要最新登记信息或资源唯一性。如果允许每个地点使用同一份旧副本，就可能产生多余或相互冲突的权利。

H3——边界的代价：预先分配可以保证排他性并减少损害，却会把额度冻结在危机中并不需要它的地点，使其他地点无法完成联网时本来合法可做的事务。

H4——临时承诺的价值：有记录的临时接收可以保留提交时间和申请人的复核权，但它不能代替最终执行，也不适用于所有权利类型。

H5——可行的反方：对多数敏感功能而言，最佳设计可能是安全停止、提供受保护的有限连接，或加强向线下人工服务的转换，而不是复杂的本地授权。这些替代方案必须留在比较范围内。

如果经授权测试显示，计入攻击、纠错后的权利与成本后，一项具体本地授权并未比临时停止增加有效完成量，或造成公共政策不能接受的可达性不公，那么其实用价值主张就应被否定。

2. 知识基础：从通信转向行为语义

2.1 为什么复制数据还不够？

分布式系统（Distributed Systems）研究描述的是独立设备共同运行、彼此消息可能延迟或中断的环境。在这种环境里，“正确”并非只有一种含义。它可以指副本重新连接后显示相同数值，也可以指中断期间每个用户或机构所作决定始终符合一项任何时刻都不应突破的规则。第一个目标可能在第二个目标已被违反后才实现。

马克·夏皮罗（Marc Shapiro）等人在无冲突复制数据类型（Conflict-Free Replicated Data Types；CRDT）研究中表明，在特定条件下可以设计出更新后仍会收敛的分布式数据类型。然而，这类工具保证的是特定合并属性，本身不足以定义稀缺权利的法律，也不足以确保一项权利不会被使用两次。[S10](#)

2.2 哪些事可以不经协调完成？

一致性即逻辑单调性（Consistency as Logical Monotonicity；CALM）研究某些逻辑操作模式，与在保持一致语义的同时免于持续协调的可能性之间的关系。约瑟夫·赫勒斯坦（Joseph M. Hellerstein）与彼得·阿尔瓦罗（Peter Alvaro）阐述了这一区分及其对分布式软件设计的影响。[S08](#)

这里的单调性是一个技术概念：在适当的逻辑表达中，向一组输入加入新输入后，程序不应以违反原有条件的方式撤回已经证明的结果。因此，记录独立事件或增加一份符合条件的文件，通常比作出一个依赖“系统其他部分没有发生某事”的决定更简单。不过，并非所有“增加”操作都安全；删除后果、撤销许可和资源余额变化，都可能改变判断。

彼得·贝利斯（Peter Bailis）等人在《数据库系统中的避免协调》（Coordination Avoidance in Database Systems）中提出了与应用不变量相关的标准：不变量汇合性（Invariant Confluence；I-Confluence）。对本文最重要的实际含义是：不能只看副本是否收敛，还要判断两个各自在本地有效的状态合并后，是否会违反全局正确条件。该研究明确区分了可用性与收敛属性，以及应用不变量安全保证。[S09](#)

在数字国家服务中，不变量可能是：许可撤销后不得继续使用，某项权益额度不得发放两次，或一个唯一登记对象不得分配给多方。这些不变量必须先有法律定义，才能表示为软件条件。研究者不能虚构一套发放规则，再假定所有机构都有义务遵守。

2.3 离线支付不是一个现成的开关

国际清算银行（Bank for International Settlements；BIS）在“北极星项目”（Project Polaris）下于 2023 年发布央行数字货币离线支付手册。报告把隐私、包容性、设备安全、持有与支出上限、运行政策和重复使用风险都列为设计选择，不存在适合所有场景的单一方案。2023 年 10 月发布的后续文件进一步指出，当时许多方案仍处于实验或开发阶段，能够普遍投入运行的成熟方案数量有限。[S06S07](#)

欧洲中央银行（European Central Bank；ECB）于 2026 年 8 月就安全元件和嵌入式芯片标准展开咨询，这是其规划数字欧元离线支付能力的一部分。截至本论文证据截止日期，数字欧元本身尚未成为公众可用货币；未来年份可能推出，但仍取决于立法、决定和测试。[S16S17](#)

这些来源把问题收窄得更准确：转移到设备上的权限，需要真正管理稀缺性、防止复制，并核验获授权者身份。中心失联后，仍有一些性质无法在本地证明，包括某些撤销状态和多个独立设备上的同步转移。

3. 现实世界证据：三种不同的观察单元

3.1 2025 年 4 月 28 日的西班牙与葡萄牙

西班牙银行（Banco de España）在 2026 年 4 月 27 日发布的回顾中记录，大范围停电约于 2025 年 4 月 28 日中午 12:33 开始，电子支付和取款机受到影响，人们手中的现金则仍是无须电力或即时连接便可直接交换的媒介。报告还指出，一些取款机虽然装有现金却无法工作，银行及运钞机构于 4 月 29 日和 30 日为取款机补钞。[S01](#)

欧洲中央银行（European Central Bank；ECB）2025 年的研究指出，按文中比较，受影响地区的线下银行卡支付下降约 41%—42%，线上购买下降约 54%。凯克萨银行研究部（CaixaBank Research）基于其交易样本与比较研究估计，停电当天其指标覆盖的消费支出下降约 34%，随后几天弥补了部分差额。这些比例不是随机实验结果，也不代表全部经济活动；地区差异、延期购买和机构数据范围都会改变其含义。[S02S04](#)

欧洲输电系统运营商联盟（European Network of Transmission System Operators for Electricity；ENTSO-E）于 2026 年 3 月 20 日发布伊比利亚停电调查摘要，重点讨论电力系统中多个相互作用的因素。本文不以数字权限理论重新解释停电原因，只将该事件视为一场有文献记录的外部中断：它暴露出某些支付场景必须向当时无法响应的网络申请许可。[S03](#)

3.2 2023—2025 年的英国图书馆

英国图书馆（British Library）于 2023 年 10 月遭受网络攻击后，阅览设施和馆舍仍然开放，检索、编目和在线服务能力却陷入中断。该机构于 2024 年 3 月发布自身复盘，并在 2025 年持续报告服务逐步恢复情况。现有资料没有证明曾使用任何特定的“本地权限”模型，只说明了：机构使命的一部分可以继续履行，同时另一部分仍处于严重且公开的失能状态。[S14S15](#)

3.3 沙特是问题发生地，而非预设的失败案例

沙特中央银行（Saudi Central Bank；SAMA）的监管网站收录了自 2017 年发布的业务连续性管理框架，以及 2021 年关于银行备用供电、发电机检查、容量与维护的指引。数字政府管理局（Digital Government Authority；DGA）也发布数字政府风险与连续性管理的监管资料和参考指南，其中包括 2.0 版控制要求及后续指南。[S11](#)（[相关的 2025 年指南](#)）[S12S13](#)

本研究计划无权访问内部故障记录或权限资料，也不推断任何敏感沙特应用缺少本地授权，或已经采用本文描述的某种形式。连续性监管说明机构重视这个问题，却不能证明断网时哪些行为能够合法、可运行地最终完成，也不能证明响应演练结果。

推断边界表

证据组	来源能够证明的观察	在本研究中的作用	不允许据此作出的主张
伊比利亚 2025	大范围停电；部分支付渠道中断；持有人已有的现金仍可交换	说明某些结算方式不依赖即时授权网络	现金足以覆盖所有用户，或所有数字支付同等失败
英国图书馆 2023—2025	阅览空间继续开放，检索与编目服务长期受扰	显示不同层级的权限和操作可以呈现不同持续程度	部分运行消除了攻击后果，或当时实施了某份本地授权文件
沙特文件	指定行业存在正式管理、测试与替代方案框架	确定可以围绕哪些制度基础寻求研究合作	已对离线执行单元开展并公布实验，或其成效已获证明

4. 概念模型：决定由信息、权力与证据构成

以 a 表示服务行为， i 表示希望完成该行为的主体， t 表示时刻。本地决定至少需要核验四类条件：

1. 行为合法性（Authorization）：机构、设备或工作人员有权在有效管辖范围内实施具体行为。
2. 证据完整性（Evidence Integrity）：来源、签名、文件或申请副本完整，并且核验密钥在相关政策下有效。
3. 条件新鲜度（Freshness）：数据签发时间、断网期间改变或撤销的风险，以及可以容忍这种无知的时长。

4. 不变量安全 (Invariant Safety)：与其他地点的结果合并后，该行为不会产生双重权利、债务或被禁止的变更。

在拟议设计框架中，可以用下面的逻辑条件表示是否允许本地行为：

$$\text{ALLOW}(a, i, t) = A(a, i, t) \wedge E(a, i, t) \wedge F(a, t) \wedge I(a, i, t).$$

任一条件为零，按照这项规则，最终完成就应停止；临时接收、解释或通过其他路径转交申请仍可能继续。这是概念表达式，不是完整法律决策机。每个函数都需要定义，并在必要范围内与监管依据、测试和已发布数据关联。

本文不把签名等同于全部证据有效。若密码学模型成立，签名可以证明一条消息未被修改且来自特定密钥，却不能单独证明持有人仍享有该项权利、断网期间密钥没有被撤销，或消息没有在别处使用。这个问题并非每种设计都必然存在：更短期的授权、分割额度、受保护硬件、金额与使用限制、审计记录，都可能缓解风险；但每种处理都会增加成本与新的信任条件。

4.1 决定安全与对话持续之间的必要区别

本文区分四类结果：

- **Completed Valid**：在公开且可审计的授权范围内，最终有效地完成行为。
- **Accepted Provisional**：申请已接收，回执明确说明仍待复核或结算。
- **Deferred or Escalated**：申请暂缓处理，并提供清楚理由、状态、复核时间或援助通道。
- **Rejected or Unsafe**：因缺少授权或证据而正确拒绝；或阻止了一次若被允许便会违反条件的尝试。

不能把这四类结果合并成“已完成交易”数量。同样，临时接收也不应一概视为失败：若政策赋予回执真实而非最终的效力，它可以保留权利人的顺序和申请时间。具体判断仍取决于法律环境以及延迟会造成何种损害。

5. 维护稀缺权利：从无法协调到有条件分割

先建立一个故意简化、便于审计的模型。某项权利的总量为 B 。中断前，有权的中央主体向各独立地点分配互不重叠的额度 q_i 。每个地点只能在自身额度内完成使用量 c_i 。如果满足：

$$q_i \geq 0, \quad c_i \leq q_i, \quad \sum_i q_i \leq B,$$

那么：

$$\sum_i c_i \leq \sum_i q_i \leq B.$$

这一论证只在模型内部成立，并以额度未被伪造或复制、本地状态得到诚实保存、所有参与者同意使用规则为前提。它不是现实系统的安全证明：没有研究设备丢失、硬件复制、密钥共享、重放攻击、既有授权撤销，也没有研究人员违反政策的决定。这些条件并非枝节，因为其中任何一项被破坏，都可能摧毁上述上限保证。

这项机制类似预先预留或托管额度分配（Escrow Allocation）：无须每次行动都重新请求许可，因为行动权的一部分已经被限定范围，并排他地留在一个地点。代价在于：额度分配发生在知道中断期间实际需求之前。A 地点不能仅凭需要，就拿走 B 地点未使用的额度；否则必须恢复连接，或引入能够保证转移没有重复发生的新协议。

5.1 为什么两个地点各持一份旧余额仍然不够？

如果中断前两个地点都保留一份写着“还剩三个单位”的共同副本，又分别允许自己使用三个单位，总使用量就会变成六。双方都诚实地依据本地副本行动，却违反了总量条件。这是未分割稀缺资源副本在缺乏协调时产生的典型反例（Counterexample）。必须把它与真实资金体系区分开：金融系统可能具备其他规则、结算机制、硬件与保障，而本文模型没有模拟这些内容。

5.2 为什么签名有效不等于只能兑换一次？

我们另行执行了一个示例：一个可复制的数字令牌 `t1` 带有有效发行方签名，两个隔离地点都认识它。如果每个地点都无法看到另一地点的使用记录，令牌也没有绑定到不可克隆硬件或独占使用地点，那么两个地点都可能各接受它一次。签名两次都有效，但令牌在全球只能使用一次的条件失败。

`data/duplicate_token_counterexample.json` 明确记录了这一状态。

这并不是说每种签名或安全数字钱包都存在同一攻击。模型说明，任何“签名足以防止离线双重支付”的主张，都必须交代硬件设计、余额绑定方式、额度或复制限制。“北极星项目”（Project Polaris）文件区分了结构不同的方案与风险，并把安全元件和运行限制置于核心位置。[S06S07](#)

6. 已完成的计算实验：25 种状态 × 五项策略

6.1 穷举范围与主张边界

程序完整枚举了一组预先界定的状态，并非蒙特卡洛模拟（Monte Carlo Simulation），也不是机构样本。每种状态中，A、B 两地各自的请求数都取自集合 $\{0, 1, 2, 3, 4\}$ ，因此共有 $5 \times 5 = 25$ 个组合。总权利 $B=3$ 个合成单位。每个组合都在五项策略下比较。模型没有为这些组合赋予发生概率，没有人口权重、断网时长、运行密码学过程或人的行为模型。

6.2 五项策略

P0——Central Stop: 所有最终批准都等待与中央恢复连接；隔离期间不执行任何最终操作。其他机构仍可提供信息或援助，但不在本次数值计算范围内。

P1——Provisional Intake: 系统记录全部意向，并标记为临时接收；它们不计入最终完成，等待恢复连接后的复核。

P2——Escrow (1,2): 为 A 预留一个单位，为 B 预留两个单位。没有连接时，每个地点都不能超出自身上限，超额请求进入复核队列。

P3——Escrow (2,1): 与上一项完全相反，用以检验在需求分布未知时，预先让一个地区获得另一地区两倍额度会产生什么影响。

P4——Blind Local Commit: 每个地点最多完成三个单位，仿佛自己独占全部资源。这项策略只用于暴露违规行为，不作为专业上可接受的选项。

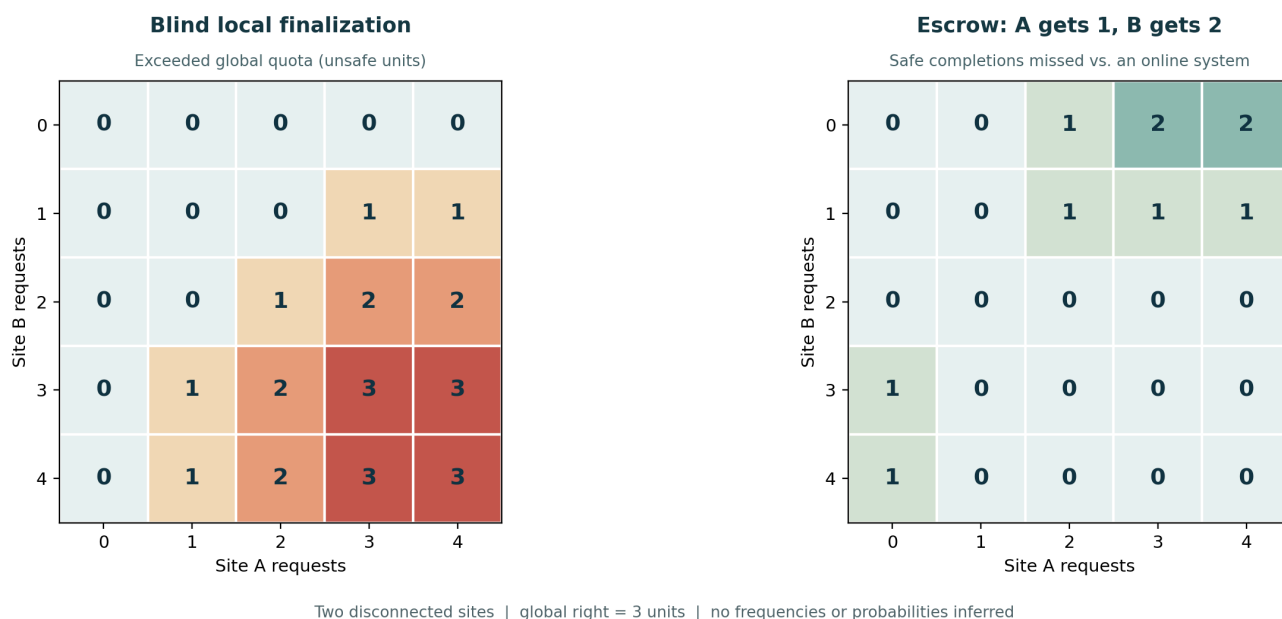
联网参考基线能够在知道两地需求后，于每种状态完成 $\min(3, d_A + d_B)$ 个单位。模型不计算等待时间、运行成本或核验耗时，因此不能用于财务比较，也不能描述真实中断时长。

6.3 可复现结果

策略	测试状态	超出上限的状态	最大超出单位数	25 种状态的最终完成总数	临时意向总数	相较联网基线少完成的安全单位数
中央停止 P0	25	0	0	0	0	65
临时接收 P1	25	0	0	0	100	65
托管额度 (1, 2) P2	25	0	0	55	45	10
托管额度 (2, 1) P3	25	0	0	55	45	10
盲目批准 P4	25	13	3	90	0	0*

P4 的缺口栏为零，并不表示运行安全；该策略在 13 种状态中突破总权利，其中一部分批准无效。所有总数都是对彼此排斥的替代状态求和，并非同一时间发生的交易或涉及的人数。不得把 13/25 解释为 52% 的失败概率。

Twenty-five EXHAUSTIVE, SYNTHETIC request states



分割授权下的上限违规与错失机会热图

图 2——每条轴代表一个地点的请求数，共有 25 个单元格。第一幅图显示超出权利上限的程度，第二幅图显示固定按 1+2 分配时，相较完整联网信息错失的安全完成机会。数字直接由代码生成，不含沙特数据。

6.4 一个反例，以及不应忘记的一个优点

若 A 请求三个单位而 B 没有请求，（1，2）授权只能让 A 完成一个单位；也就是说，A 少完成两个本可由中心在不突破上限的情况下安全完成的单位。这是在看到需求前规划的代价。可以在危机前仍有连接时重新分配额度，也可以划分得更细，或在法律与技术保障允许时建立有限的权限转移通道，以减少这一代价。不能靠复制余额就声称稀缺问题已经解决。

反过来，当两个地点各请求两个单位时，盲目策略会批准四个单位，尽管总权利只有三个。分割额度守住上限，却可能拒绝一个请求，或让其等待。正确选择取决于不公平与延迟的代价、公开的优先规则和权利性质，不能只追求监控面板上“已完成”一栏的最大值。

6.5 实际验证了什么，又没有验证什么

代码已运行并生成 125 行的 `model_check_states.csv`、包含五项策略的 `model_check_summary.csv`、假设文件、复制凭证违规记录，以及两幅原创图。程序内部还执行了计算断言：在既定状态中，诚实的托管额度设计都不突破上限；总行数为 125；盲目策略确实出现违规。这只是一个小型程序模型的测试，不测试设备、支付协议或密钥保管，也不形成全面的机构保证。

我们没有加入人口分层或虚构概率分布来做敏感性分析。应用研究必须在获得授权后，使用真实需求份额、优先级差异成本，以及存储、电池、断网、密钥撤销、钱包被盗和审计完整性等约束重新运行。

7. 授予权限不等于赋能设备

7.1 撤销与时间边界

一份文件签发时可能拥有有效签名，断网期间其指向的权利却被撤销。设系统存在两种可能历史： H_0 中没有撤销， H_1 中撤销发生在本地设备听不到的中心。如果设备在两种历史中看到的全部输入完全相同，任何纯本地算法都无法判断哪一种历史真实发生。此时需要公开政策规定可接受的证据时效，或选择状态改变后仍然有效的行为，或建立连接路径、期限更短的授权，也可能必须停止最终执行。

摆脱这种无知的唯一办法，不是让机器学习猜测撤销概率。概率猜测不会把未获授权的决定变成获授权决定。人工智能（Artificial Intelligence；AI）模型可以帮助安排复核案件，或在恢复连接后发现矛盾，却不能创造法律授权来源，也不能证明自身不可见的信息。

7.2 危机中，持有人未必能行使所持权利

用户可能持有一份可以离线展示的数字文件，却仍需机构按法律和实践予以接受。支付卡也许能在本地核验部分数据，商户设备却可能因断电而无法运行。因此，测试对象必须是完整系统：签发方、设备、工作人员、受益人的证据、投诉通道、本地电力和回执最终去向。

7.3 隐私与歧视

离线能力可能帮助连接较差地区的用户，也可能排除没有新式设备、有效文件或预存余额的人。过度强调可同步审计记录，还可能收集并转移并非必要的个人数据。系统需要数据最小化和并行人工路径，并在隐私保护与获授权参与规则下，衡量适当地区与群体之间的表现差异。不能用总体平均速度掩盖资源较少的用户根本没有可行路径。

7.4 并非所有后果都可修复

队列顺序可以纠正，两条登记笔记可以合并。但把一件唯一物品交给无权接收者、作出不安全医疗决定，或执行一项操作者没有最终权限的法律转移，其后果可能无法挽回。“以后可以同步”描述的是信息能力，并不必然意味着社会与权利状态能够恢复原状。

8. 经授权的沙特田野研究设计

8.1 样本与记录单元

本文建议与拥有适合隔离演练、或可在独立测试环境运行的服务功能的机构开展自愿且获授权的合作，不中断真实公共服务。观察单元是经授权测试窗口中的行为类别，而不是服务器名称或敏感设施地址。按法律后果对行为分类：读取、接收、预留资源、可逆的最终完成，以及只能由中心完成的高影响最终行为。

8.2 需要收集的变量

变量	必要的操作性定义	可能的授权来源	保护或解释限制
行为类型	查询、接收、签发、发放，还是撤销？	服务政策与规格	研究者不得改变真实权限类别
本地授权	授权文件类型及其时间、事项和数量边界	经批准、去身份化的机构文件	不公开密钥秘密或存储位置
证据新鲜度	数据与权限上次核验的时间	汇总后的本地测试日志	不公开个人记录路径
正确完成	按实验前选定政策有效完成的最终决定	对输出进行法律与运行复核	不得与临时接收混为一谈
临时回执	申请已保存，并包含时间证明、防篡改与后续跟踪信息	测试或合成记录	结算前不得宣称权利已获接受
冲突	本地决定彼此不同，或与后来登记信息冲突	受保护环境中的合成事件	真实损害分类需要专业批准
复核与补救	解决争议所需时间，以及如何通知受益人	机构程序测试	不得假定所有错误都能自动修复
公平性	适当群体提交或完成申请的能力差异	受隐私保护的汇总指标	没有需要和依据，不得推断敏感属性
运行成本	培训、硬件、复核、延迟与人工援助费用	汇总后的内部财务数据	只能比较同类成本

8.3 比较设计

对每个同类行为，在测试环境中比较预先规定的策略：停止最终完成、临时接收、在合法可行时分配本地授权额度，以及可能的备用连接路径。获得批准后，可在测试中对合成情景随机分配，同时保持请求类型、额度和假定断网时长相同。本文不建议为了实验，故意让真实用户或真实法律权利承受超限风险。

主要结果：在法律边界内正确完成的行为数量；被发现并阻止的不变量违规尝试数量；待处理回执的结算时间；没有人工介入便无法解决的状态数量；汇总后的可达性差异；总成本。可接受边界必须在看到比较结果之前确定，任何偏离分析计划之处都应记录。

可以接受的竞争性结论：研究可能表明，有限备用连接、强化人工沟通通道，或停止执行某些行为，比分布式授权更有用、更安全。届时应按证据推荐这些方案，不能强迫研究证明发起者偏好的模型有价值。

8.4 对抗与安全测试

在获授权的防御环境中测试以下情况：证据已超过时效；文件在中断期间被撤销；令牌再次提交；设备丢失；时钟不可信；更新到达顺序不同；一张临时接收的回执后来无法兑现；连接只恢复一部分、未覆盖全部记录；以及对账期间反复断网。公开研究报告无须披露密钥信息、关键拓扑或可用于攻击具体设施与服务操作步骤。

9. 离线权限档案（OAP）：一项设计提案

本文建议为每项敏感行为建立结构化机构记录，而非仅把它附在应急运行计划之后。记录应同时回答七个问题：权利是什么、谁有权、证据是什么、时间范围多长、使用边界在哪里、何时停止，以及如何对账和申诉。可以按下表表示：

拟议字段	最低内容要求	值得警惕的失败标准
authority_source	授权依据，以及允许该行为的制度	权力没有定义，或机构超出管辖范围
action_class	查询、接收、预留、最终完成、转交	把最终行为称作“临时申请”，或反过来
evidence_policy	来源、签名、数据有效性与更新时间	核验已经到期的签名或已撤销的证据
scarcity_guard	防止超用不可重复资源或权利的排他上限	令牌或额度可被复制
stop_rule	证据不足、发生冲突或无法保证公平时的条件	明知违反强制不变量仍继续最终完成
reconnect_policy	事件记录、对账、审计、通知与申诉	静默合并，掩盖损害及其对用户的影响
inclusion_path	人工或实物援助，以及延期权利的公平期限	服务连续性只面向某类设备或某类用户

这份档案只是供研究与审查的初步提案，不是政府标准，也不是与真实机构举行研讨后的成果。它需要法律、身份和安全专家共同制定，也应利用现有标准和沙特框架，但不能声称得到任何机构归属或认可。

10. 至 2035 年的经济与战略影响

经济影响不能只用“服务可用小时数”衡量。机构可能离线完成五十项行为，却为解决五项不可逆错误付出高昂代价；也可能只推迟少数行为，但这些行为极其重要，等待的社会成本因而急剧上升。本文因此提出一个多目标决策前沿（Multi-Objective Decision Frontier），同时纳入正确完成量、排他性、延迟时间、潜在损害、成本和可达性差异。在权重和比较合法性达成共识前，不构造全国综合数字。

面向沙特，可以提出四项有条件的研究与政策选择：

1. 最终行为保持完全中心化，同时提供临时接收入口。当排他性无法保证，或法律不允许下放时，这可能是最佳方案。它需要清楚的回执标准、保存申请与时间，以及申诉机制。
2. 对高度特定的事务预先分配额度。当边界可管理、审计实验令人信服时，此方案可能有用，但要承担断网期间额度冻结的成本。
3. 依据短期有效的签名证据授权。它可能适合信息展示或影响有限的程序，却面临最新撤销与不安全密钥携带风险。数学能够核验签名，并不会自动让设计获得法律授权。
4. 开发管理权限档案与对账流程的本国产品。行为与权益测试、建模软件可能形成领域，但只有产品能销售、反复通过客户的测试、安全与运行检验，市场才算成立；在国家地图上画箭头不构成市场证据。

这些不是带概率的预测，也不是正式结果。研究机构若要建立未来预测登记，应明确可测事件、判定日期、结果来源和概率规则，同时不得把发布时间倒签到过去。

11. 科学限制：这项研究的发言权到哪里为止？

1. 测量：本文不含沙特服务的运行数据、可用率、本地权限份额、事故记录或法律适用结果。模型中的三个合成单位不能外推到任何真实金额或登记簿。
2. 计算：本文完整探索的是 25 种需求状态，而非真实系统的全部状态空间。真实系统可能包含数千种角色、密钥、设备、撤销、胁迫与人为错误。
3. 安全：模型没有证明硬件、密钥、消息或支付方式能够抵御攻击；可复制令牌示例专门用于说明签名有效性的局限。
4. 社会代表性：示例中的每种状态只是两个数字。人的能力差异、行为重要性、申诉权和补救权只作为拟议研究要求提出，没有进入计算。
5. 历史：伊比利亚事件或英国图书馆事件都不能转化为某项具体本地设计质量的证据。来源记录的是服务中断或部分持续运行，不测量拟议“离线权限档案”的效果。
6. 偏差：停止和临时接收被纳入真实替代策略；盲目策略则被故意设计为产生违规反例。因此，这项比较不声称在已经部署的商业解决方案之间保持中立。
7. 合法性：个人与机构权限属于法律和行政问题。实验模型无权代替获授权机构签发许可。先要定义哪些行为被允许，才能研究其技术边界。

12. 下一项关键研究

最有价值的下一步不是建设一座号称“离线运行”的庞大平台，而是选择一项依法可以临时接收的公共行为、一项在政策允许时可以凭有效额度完成的行为，以及一项必须停止的行为。在具有明确法律输出的获授权环境中测试，并测量申请、证据、权利和申请人在断网期间及恢复连接后分别发生了什么。

我们需要的关键论文应能够这样表述：在特定断网类型和明确条件下，架构 X 相比策略 Y，在不突破已批准不变量的前提下增加了正确完成量，其成本与社会边界为何。结果也可能是拟议设计失败，或更简单的替代方案更好。接受这种结果属于研究方法，而不是需要掩盖的编辑尴尬。

13. 复现、参考文献与数据

重新运行：保存本目录文件，安装 `analysis/requirements.txt` 中列出的依赖，然后运行：

```
python3 analysis/reproduce.py
```

程序会重新生成 `data/model_check_states.csv`、`data/model_check_summary.csv`、`data/model_assumptions.json`、`data/duplicate_token_counterexample.json`，以及 SVG 和 PNG 两种格式的两幅图。代码与合成数据完整包含在本资料包内，不依赖私有运行数据集或访问密钥。

现实世界来源的可得性：已发表文章与报告链接到其机构或作者页面；本文不重新分发受保护文件，也不声称拥有原始银行数据的许可。来源登记记录的是原始资料包编制期间的访问状态；那是一条历史审计记录，并不表示文档当前限制文本提取。模型的全部计算数值都来自代码中公开说明的合成变量。

按引用顺序核验的参考文献

1. S01 Banco de España. *How do we pay when the power goes out? Spain's blackout experience*. 27 April 2026. Original institutional blog. <https://www.bde.es/wbe/en/noticias-eventos/blog/como-pagamos-cuando-todo-se-apaga-la-experiencia-del-apagon-en-espana.html>
2. S02 European Central Bank. *Keep calm and carry cash: lessons on the unique role of physical currency across four crises*. ECB Economic Bulletin, 2025. https://www.ecb.europa.eu/press/economic-bulletin/articles/2025/html/ecb.ebart202506_02~1a773e2ca3.en.html
3. S03 ENTSO-E. *Final report of the expert panel on the blackout in Spain and Portugal*. Published 20 March 2026. <https://www.entsoe.eu/news/2026/03/20/entso-e-publishes-expert-panel-final-report-on-28-april-2025-blackout-in-spain-and-portugal/>
4. S04 CaixaBank Research, Josep Mestres Domènech and Zoel Martín Vilató. *The economic impact of the blackout in detail*. 18 June 2025. <https://www.caixabankresearch.com/en/sectoral-analysis/consumption/economic-impact-blackout-detail>

5. S05 Banco de España. *Situation of payment infrastructures and the banking sector in Spain after the blackout*. 29 April 2025. <https://www.bde.es/wbe/en/inicio/noticias/monitorizacion-del-impacto-del-apagon-el-sistema-financiero.html>
6. S06 BIS Innovation Hub. *Project Polaris: handbook for offline payments with CBDC*. 11 May 2023. <https://www.bis.org/publications/project-polaris-handbook-offline-payments-cbdc>
7. S07 BIS Innovation Hub. *Project Polaris: high-level design guide for offline payments*. 26 October 2023. <https://www.bis.org/publications/project-polaris-high-level-design-guide-offline-payments>
8. S08 Joseph M. Hellerstein and Peter Alvaro. *Keeping CALM: When Distributed Consistency is Easy*. Author-hosted 2019 preprint; subsequent publication context noted separately in source ledger. <https://arxiv.org/html/1901.01930v2>
9. S09 Peter Bailis and collaborators. *Coordination Avoidance in Database Systems*. Proceedings of the VLDB Endowment, volume 8, 2014. <https://www.vldb.org/pvldb/vol8/p185-bailis.pdf>
10. S10 Marc Shapiro, Nuno Preguiça, Carlos Baquero and Marek Zawirski. *Conflict-Free Replicated Data Types*. SSS 2011, LNCS 6976. DOI: 10.1007/978-3-642-24550-3_29. <https://inria.hal.science/inria-00609399v2/document>
11. S11 Digital Government Authority. *Controls of Risk and Business Continuity Management for Digital Government, V2.0, Guideline of Risk and Business Continuity Management for Digital Government, V1.0* (2025). <https://dga.gov.sa/sites/default/files/2024-02/Controls%20Of%20Risk%20and%20Business%20Continuity%20Management%20For%20Digital%20Government%20V2.0.pdf>
12. S12 Saudi Central Bank. *Business Continuity Management Framework*, introduction, 27 February 2017, in force. <https://rulebook.sama.gov.sa/en/11-introduction-bcm-framework>
13. S13 Saudi Central Bank. *Providing Backup Generators in Branches and Remittance Centers*, circular of 18 May 2021. <https://rulebook.sama.gov.sa/en/providing-backup-generators-branches-and-remittance-centers>
14. S14 British Library. *British Library Cyber Incident Review*. 8 March 2024, primary post-incident account. <https://www.bl.uk/files/v5dwkion/production/99206a2d1e9f07b35712b78f7d75fbb09560c08d.pdf/british-library-cyber-incident-review-8-march-2024.pdf?dl=>
15. S15 British Library. *Restoring our services – November 2025 update*. 21 November 2025. <https://www.bl.uk/stories/news/restoring-our-services-november-2025-update>
16. S16 European Central Bank. *Call for expression of interest to provide feedback on the list of standards relevant for the offline digital euro*. 18 August 2026. <https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews260818.en.html>
17. S17 European Central Bank. *FAQs on the digital euro*. Updated 17 August 2026; conditions for development, legislation and potential 2029 issuance. https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html