



战略文章

编辑日期：2026 年 9 月 25 日

当中心沉默，谁有权说“可以”？

一个无需全程联网也能继续运转的国家：无需即时许可的现金，以及可在断网前预先分配的权力

The State That Can Authorize Without Calling Home: Bounded Authority, Offline Transactions, and Saudi Digital Government

MERIDIAN | 第二篇战略文章 M02 | 编辑日期：2026 年 9 月 25 日 | 研究范围：2026—2035 年

导语：西班牙和葡萄牙大片地区停电的那一天，一个人可能带着银行卡、智能手机和足够的余额，却无法完成一笔简单的购买。消失的不是钱，而是让远方机构说“可以”的通道。本文向沙特数字国家提出一个新问题：哪些决定的作出权可以预先交给用户、设备或工作人员，哪些决定必须等到与中心建立可靠连接？

编辑说明：西班牙、英国图书馆和欧洲相关进展均依据注明日期的已发布来源。所谓“断网前分配权限”及其操作卡片属于研究提案，并非对沙特现有系统的描述。随文实验只探索 25 个有限的合成计算状态，既不测量沙特的实际表现，也不估计攻击发生风险。

1. 纸张比光更快的那一小时

2025 年 4 月 28 日星期一中午 12:33，伊比利亚半岛（Iberian Peninsula）发生大范围停电。许多通信中断，电子支付无法完成，一批自动取款机停止工作，人们手里的纸币却仍可用于交易。我们无须虚构收银台前的场景。西班牙银行（Banco de España）在 2026 年发布的回顾中描述了：常用支付手段中断后，食品和药品等必需品更难购买；一些取款机虽然内部已有现金，却因断电或断网无法出钞。[S01](#)

这里有一个无需修辞装饰的反差：纸币这个常被某些创新话语送进经济博物馆的发明，是少数不会先询问服务器（Server）“我能不能工作”的东西。它的优势并不来自更快的处理器，而在于：灯熄灭之前，按其面额完成支付的权力就已经随纸币一起交到了持有人手中。

这并非对一切旧事物的浪漫赞颂。没有足够现金的人无法受益于这种独立性；一些装有现金的取款机照样停摆；交易还需要电力、安全、供应、卖方和买方。西班牙银行还记录到，停电期间取款量骤降，服务恢复后随即回升，而为取款机重新补充现金需要后勤投入。^{S01} 纸币不是魔杖，它只是一个有限的例子：某项权利已经预先配置，使用时无须每次重新申请许可。

欧洲中央银行（European Central Bank；ECB）发表的研究为这次事件提供了量化观察。按其所评述研究采用的比较方法，受影响地区的线下银行卡支出下降约 41%—42%，西班牙电子商务下降约 54%。凯克萨银行研究部（CaixaBank Research）的数据则显示，停电当天估算的消费支出较比较基线下降约 34%，随后两天的反弹弥补了大部分延迟。这些估算受各自数据来源和样本范围约束，不能代表每笔交易或每个人。^{S02S04}

供电恢复后，不同支付方式逐步回归。4 月 29 日上午，西班牙银行表示，大额支付系统已正常运行，零售支付也已恢复，但部分网点和取款机仍有少量问题。^{S05} 这些差异说明，“支付中断”一句话掩盖了基础设施、功能和地点的多个层次。不过，本文要追问的还不是这个问题。

更奇怪的问题是：为什么一张纸可以在没有即时授权的情况下完成完整的经济行为，而一款掌握用户身份、余额和信用记录的应用，却不能在听不到远方回应时采取行动？

2. 消失的不只是连接，还有许可

我们通常把中断视为信息传输问题。网络（Network）像邮政系统一样，在各方之间搬运消息。但现代国家机构不只用它传输数据，也用它传输权力：允许付款、验证身份、确认某项权利没有被使用两次，或核实某项授权是否在一分钟前已被撤销。

因此，“在线”与“离线”的区分已经不够。设备可以保留一份文件副本，却无权在文件被撤销后判断其仍然有效；工作人员可以知道申请已经送达，却没有批准权；银行可以保存付款指令，同时有充分理由拒绝在结算前把它称为已经到达收款人的资金。

所以，每项沙特数字服务不应只回答一个问题：它能否**离线（Offline）**运行。问题应由四个动词构成：我们能够知道什么？能够接收什么？可以承诺什么？依法有权最终完成什么？

这些行为的风险截然不同。本地工作人员可以登记一份新的证明申请，并开具确认临时收件的回执。但要完成某项唯一财产的转移、发放不得重复领取的权益，或作出后果难以逆转的决定，可能需要中央登记簿的实时信息和明确的法定权限。申请能在离线时流转是一回事；未经核验就产生最终权利是另一回事。

本文提出的设计理念是有界本地权限（Bounded Local Authority）：明确获授权一方可在本地完成何种行为、时间与数量上限、可核验的证据、必须停止或转交的条件，以及恢复连接后如何审查后果。中断不会赋予任何人原本没有的新权力；它只会暴露出，某项具体权力是否已经在中断前以合法且安全的方式分配出去。

3. 五扇门，而非一把钥匙

以下是分析层级，并非沙特已经采用的技术标准：

层级	低连接或无连接时可做什么	决定行为安全性的条件	不得声称什么
查看（Observe）	显示本地保存的信息或许可副本	签名有效、来源明确、签发时间与有效期明确	登记信息没有在片刻前改变或撤销
接收（Receive）	收集申请并在本地记录提交时间	临时回执、防篡改、说明申请后续去向	申请已获最终批准或权利已经成立
预留（Reserve）	使用其他地点无法支用的预分配额度	本地额度相互隔离、存在上限、防止重复使用	额度足够覆盖所有请求，或能在地区之间即时转移
有限执行（Execute）	完成符合预先明确授权的行为	身份、权限与完整性核验，审计记录和测试	每项服务都适合脱离中心完成
转交（Refer）	暂停不可逆决定，并向受益人说明原因	接收通道持续可用，或存在其他援助路径	延期等于完成，或延期没有人的代价

WHO MAY DECIDE WHEN THE CENTER IS SILENT?

A proposed ladder of bounded authority | conceptual, not an implemented Saudi system

01 OBSERVE	Verify a signed local snapshot Freshness and expiry must be explicit
02 RECEIVE	Record intent; issue provisional receipt No claim of final approval
03 ALLOCATE	Use a pre-issued local quota Disjoint rights and replay protection
04 EXECUTE	Finalize only an authorized bounded act Local proof plus audit trail
05 REFER	Route irreversible cases to central review Do not guess revocation or uniqueness

The design question is the scope of delegated authority, not merely whether a device has a cache.

拟议本地权限的概念阶梯

图 1——断网时授权工作的拟议概念阶梯。它不代表任何沙特系统的实际权限；每项功能仍需明确授权依据、保密与隐私边界，并接受安全和运行核验。

这项取舍无法靠“让应用支持离线”解决。应用可能能够运行并显示数据，却无法得知远方是否有人使用了同一项权利；它也可能接收两份相互冲突的申请，把冲突留待以后解决。对某些事务而言这很合适，对另一些事务却可能造成灾难。界面能够离线工作，不等于机构能够在离线时作出有效决定。

4. 数学对“可以”知道多少？

在分布式系统（Distributed Systems）中，两方无法交换消息时，有时很难维持一项实时共享事实。但这并不意味着“一切都需要中心”。是否需要协调，取决于操作的含义。

约瑟夫·赫勒斯坦（Joseph M. Hellerstein）与彼得·阿尔瓦罗（Peter Alvaro）通过“一致性即逻辑单调性”（Consistency as Logical Monotonicity; CALM）解释了这一点。简要地说，有些操作只是增加事实，后来收到的信息不会推翻先前决定的有效性，因此某些形式可以在没有持续协调的情况下执行。另一些操作则依赖于证明某件事没有在别处发生、某项权利具有排他性，或当前看到的是最新撤销状态；这些问题比单纯汇集信息困难得多。[S08](#)

设想两份现场笔记，分别记录两名技术人员走访过的地点：若两人各自增加独立记录，稍后可按明确政策合并。再设想库存里只有一件商品，而两个销售点都认为它“仍然有货”。事后成功合并两份记录，并不会凭空补回第二件商品。

这正是无冲突复制数据类型（Conflict-Free Replicated Data Types; CRDT）受到关注的背景。在特定条件下，这类结构能保证不同副本交换更新后收敛。但它不会自动让每项商业或行政操作变得安全。彼得·贝利斯（Peter Bailis）等人关于避免协调（Coordination Avoidance）的研究，明确区分了状态收敛与维护应用不变量（Application Invariants）。两个副本最终可能一致记录“同一项权益被领取了两次”；记录达成一致，并不能修复已经发生的损害。[S09S10](#)

由此得到一个比“永远在线”或“永远离线”更深的原则：分配那些能够自行保持正确条件的行为；对需要全局知识的行为，以授权边界或延后审查加以约束；无法安全保证的行为就应停止。

5. 25 种可能性的实验室：两个地点拥有同一项权利时

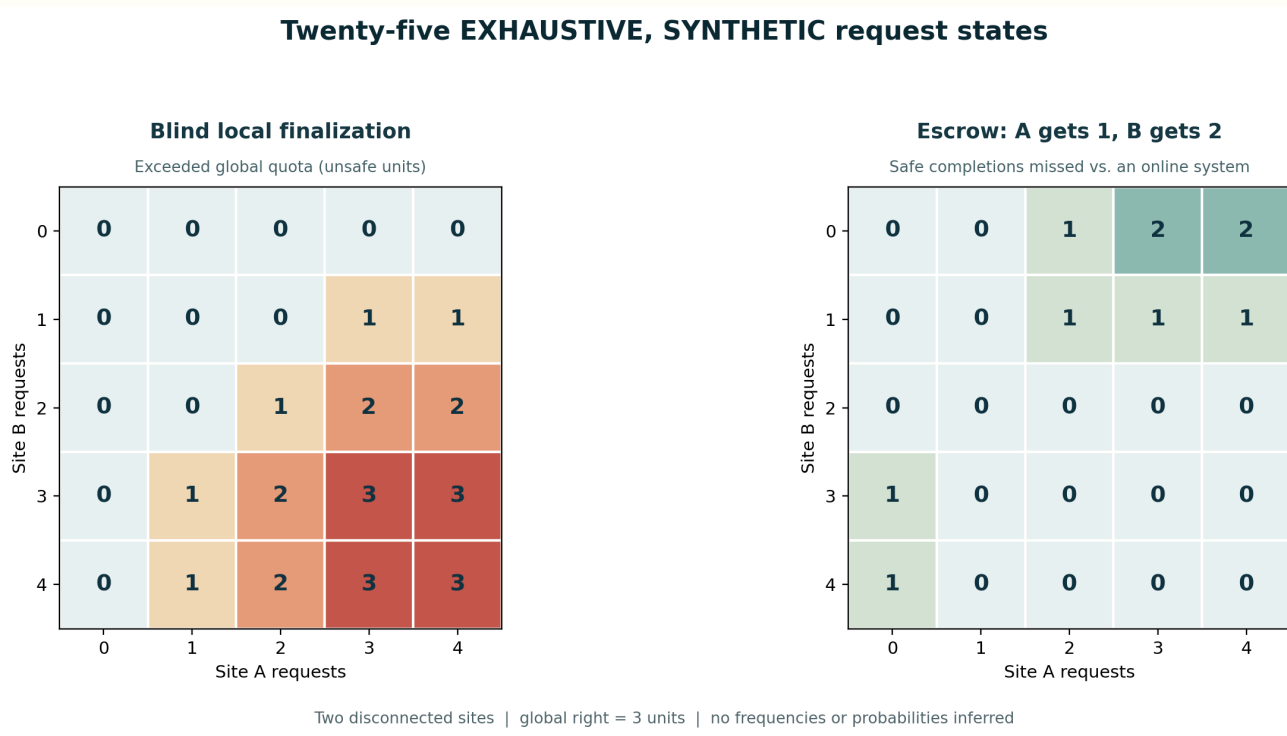
我们可以用一个小测试检验这一想法。它不是对国家的预测，而是对授权逻辑的明确计算检查。程序穷举了两个互不通信的虚拟地点 A 与 B 的 25 种请求组合。每个地点的请求数可以是 0 至 4，两地可用的共同权利总量只有三个合成单位。

我们测试了五项策略：

1. 中央停止（Central Stop）：没有连接时，不最终完成任何权益。
2. 临时接收（Provisional Intake）：可以记录意向并发出临时回执，但不最终发放权益。

- 3. 分割授权（Escrow Allocation）：A 预先获得一个单位的权利，B 获得两个单位；协调恢复前，任何一方都不得使用另一方的额度。
- 4. 反向分割授权：A 获得两个单位，B 获得一个单位，用来检验额度分配方式的影响。
- 5. 盲目本地提交（Blind Local Commit）：每个地点都看到完整的旧全局余额，并据此在本地批准。此策略被故意设计得很差，用于暴露错误。

这个有限例子的确切结果是：第五项策略在 25 种状态中的 13 种突破了共同权利上限。分割授权则在所有状态中都遵守上限，前提是授权在本地得到诚实执行，且未被伪造或复制；但把所有状态的差额相加，固定分配方式少完成了十个在联网条件下本可安全完成的单位。这些数字只是对人为构造模型状态的数学计数，不是发生概率，也不是任何真实机构的结果。



本地授权与预分配取舍的合成计算检查

图 2——左图显示盲目批准时各状态超出上限的单位数，右图显示固定按（1，2）分配时，相对于具备完整中央信息而错失的安全执行机会数。图中颜色只对应模型计算。

当 A 请求三个单位而 B 没有请求时，分割设计只允许 A 完成一个单位，尽管另一端仍有两个未使用单位。这就是预先分配权限的成本：我们可能保住权益安全，却失去断网后转移额度的灵活性。反过来，如果告诉每一方“你都可以使用全部余额”，就会因为错误的加法制造出额外权利。

更具迷惑性的是签名凭证问题。两个分支可能都拿到一个具有有效密码学签名的数字令牌（Digital Token），并各自在本地成功验证签名。但若同一令牌可被复制，又没有强有力的机制阻止它在两个隔离地点重复兑换，那么签名只证明其来源，无法证明它没有被使用两次。科学附文给出了这一情形的独立计算示例，也说明更强保证需要受保护硬件、边界设计、密钥管理和防重放措施。我们并未实现真实支付系统。

这就是授权与复制消息之间的区别：仅让所有人都知道“可以”是什么意思还不够；不能让一个“可以”仅因电话沉默就变成两个。

6. 从纸币到尚未发行的欧元

这个问题已经进入未来主权货币研究。2023 年 5 月，国际清算银行（Bank for International Settlements; BIS）创新中心在“北极星项目”（Project Polaris）下发布离线数字支付手册，同年 10 月又发布了更深入的技术指南。项目强调，这不是简单地把钱包切到飞行模式：价值的持有方式、防止双重支付、安全硬件、隐私、金额限制和重新联网方式，都会影响能否实施。[S06S07](#)

在欧洲，欧洲中央银行（European Central Bank; ECB）于 2026 年 8 月征求意见，讨论离线数字欧元可能采用的技术标准，包括安全元件（Secure Elements）和嵌入式 SIM 卡（eSIM）。项目文件明确，这项能力仍处于开发与测试之中，数字欧元未来是否发行还取决于法律框架和后续决定。因此，截至 2026 年 9 月，没有依据把离线数字欧元说成已经普遍投入使用的支付工具。[S16S17](#)

真正值得注意的，并不是中央银行在思考现金替代方案，而是：自主完成数字操作，需要让设备随身携带一项界限明确的权力，如同纸币携带预先签发的承诺。然而，比特（Bits）天然可复制。容易复制的东西，不会因为盖上漂亮的签名就变得稀缺。若要保持稀缺性，就必须设计能够落实它的限制，不能满足于一个写着“离线支付”的界面。

即使欧洲项目本身，也不会自动解决手机没电或商户设备无法启动的问题。“没有互联网”“没有电力”和“没有能够结算的机构”是三个不同条件。因此，即使未来数字钱包更加智能，实物现金仍可能是重要的社会补充手段。

7. 一座大门仍开着、却无法把所有书还给读者的图书馆

英国图书馆（British Library）提供了一个与货币不同、也不可缺少的案例。2023 年 10 月发生网络攻击（Cyberattack）后，馆舍和阅览空间继续开放，关键数字能力却陷入中断，部分服务只能依靠临时安排。该机构在 2024 年 3 月发布的复盘称，研究服务受到严重限制，在线目录部分恢复也不等于过去功能全部回归。[S14](#)

在 2025 年 11 月的更新中，英国图书馆谈到功能逐步恢复、临时申请系统、部分目录，以及重建安全数字基础设施所需的更长路径。[S15](#) 阅览座位仍可使用是一项真实成果，却没有让所有人都能取得以往可以申请的资料。这个反例提醒我们，人工或替代方案很少是“挽救整个机构”与“彻底失败”之间的二选一。

有时，机构需要一种在热情过度的应用中日渐罕见的诚实：明确告诉用户，“我今天可以接收你的申请，但现在不能批准；这里是延期原因，也是你继续追踪权利的方式。”这种运行上的诚实本身就有价值：它减少猜测，也让人能够安排优先次序。它不会消除损害，更不能免除机构为无法等待的人提供公平方案的责任。

这起事件没有证明临时运行能让图书馆所有服务安全延续，也没有证明某一套预案本可避免损害。它只让**优雅降级（Graceful Degradation）**变得具体：在公开边界内维持部分功能，同时不假装缺失的部分依然存在。

8. 沙特：并非从零开始，但有预案还不够

这个问题不同于呼吁购买更多设备或建设更多中心。沙特现有监管体系本身已经提供了起点。沙特中央银行（Saudi Central Bank; SAMA）于 2017 年发布业务连续性管理框架（Business Continuity Management Framework），并在 2021 年公布的指引中要求银行为断电准备替代方案，测试备用发电机及其容量并做好维护。数字政府管理局（Digital Government Authority; DGA）也发布了数字政府业务连续性和风险管理的标准、控制要求与参考指南。[S11](#)（[相关的 2025 年指南](#)）[S12S13](#)

这些资料证明连续性监管框架确实存在，却不是沙特某项具体服务能够在断网时完成敏感交易或自动解决冲突的公开证据。政策是否存在、是否落实、测试结果如何，以及获准持续的功能是否安全，是四个必须分开的问题。

本文建议把“离线权限档案（Offline Authority Profile; OAP）”作为一项拟议的研究与设计工具，加入政府服务架构。每项敏感功能应填写七个字段：

1. 拟执行的权利：是查看、接收、有限发放，还是最终决定？
2. 获授权主体：根据法律和政策，谁有权实施该行为？其权限能否下放到本地？
3. 本地证据：哪些已签名数据可在断网时核验？可接受的陈旧程度是多少？
4. 授权上限：不得超过的金额、数量、时间、区域或受益人类型。
5. 停止条件：哪种不确定、冲突或权限撤销状态要求拒绝继续？
6. 申请去向：已最终完成、初步接收、保留待审，还是拒绝？
7. 后续对账：谁解决冲突、谁承担错误成本，申请人如何获得解释并提出异议？

把这张卡片称为“人工智能”并不会让它自动变得聪明。模型预测某位用户很可能符合资格，并不会凭空产生依法发放权益的权力。人工智能（Artificial Intelligence; AI）可以协助排列待处理申请、在恢复连接后发现相互矛盾的记录，但概率判断不能替代授权规则，也不能免除决策责任。

本文也没有主张取消中心。在某些服务中，知道何时停下是最高程度的负责。不应允许两个相距甚远的应用根据两份过时副本，最终处分同一项唯一权利，然后告诉权利人“同步会解决一切”。同步也许能修正记录，但决定的后果早已离开服务器，进入真实生活。

9. 赋权也可能变成歧视

一个社会与伦理上的悖论必须进入工程核心：拥有现金、电池、证件和新式手机的人，并不代表所有人。西班牙银行指出，供电恢复后银行加强了取款机补钞，而现金在危机中的有效性也取决于现金是否事先到达并得到分配。[S01](#) 把同样的限制带入数字权限，会产生令人不安的问题：没有受保护设备的老

人能否使用这项授权？可否用带编号和跟踪记录的纸张接收申请？在危机中丢失手机、或需要人工协助的用户怎么办？

严肃的测试不只统计系统完成了多少操作，还要问：为谁完成，谁被迫等待，谁承担错误完成的后果。如果自主运行只面向持有某类设备或拥有特定连接历史的人，一套技术效率很高的架构也可能是不公平的。全面停止策略在机构记录里看似谨慎，却可能让无法推迟服务的人承受更大的紧急社会损害。

因此，每项授权都需要一份可审查的代价清单：暂停决定避免了什么损害，又造成了什么损害？能否用证据和合理复核期限先接收申请？接待人员是否把临时回执当作界限明确的承诺，而不是最终办结证明？这些不是公共关系问题，而是运行定义和权利条件。

当危机严重到必须作出一项不得下放的决定时，机构应明确现身：若有备用紧急通道，就公开通道；说明优先顺序；提供申诉机制；并保留记录，不能因为申请人断网就让其从流程中消失。

10. 从今天到 2035 年：谨慎分配决定权的国家

可以设想三条有条件的路径；它们不是量化预测：

路径一：界面无处不在，中央权限保持沉默。一些应用能显示保存的数据，但多数行为仍须等待中央服务器。中断考验的是公众承受延期的能力，而非机构安全分配行为的能力。其征兆是：许多服务有离线界面，却没有一项获批准的有效本地操作定义。

路径二：过早热衷于下放一切。系统发放范围过大的临时权限，却没有明确不变量，也无法保证防止重复支用或及时撤销密钥。危机第一天的数字可能很好看，恢复连接后却出现难以修复的争议。其征兆是：本地作出最终决定，而事后无法证明其排他性或合法性。

路径三：懂得分配“可以”，也懂得定义“暂时不行”。必要时，敏感服务把最终权利留在中心；查看、接收和有限授权则依据预先证据、有效签名、有效期窗口与明确恢复路径分配出去。只要为公众保留提交申请和复核权的通道，拒绝不安全行为就不应被视为缺陷。其征兆是：经授权测试证明不变量得到维护；结算时间以汇总形式发布；不同群体和地区之间的差异得到识别。

我们无须预测战争，才去检验中心能否在失联前下放决定权。沙特技术产业也可以为此开发工具：可核验的授权政策、具备审计完整性的临时回执、防重复额度方案、判断哪些行为可以执行的分类引擎，以及既显示错误又为受影响者提供明确路径的对账系统。不过，成立一个实验室不会自动产生出口产业；产品必须在真实且获授权的实验中证明效果，并让机构因其结果持续购买和复购。

西班牙恢复供电时，货币的定义没有改变。暂时改变的是人们通过某种方式使用货币的能力。危机暴露出：有些决定的完成权可以由人随身携带，另一些决定则住在一个必须回应的网络里。[S01S02](#)

因此，对未来沙特数字国家更重要的问题，可能比“多少服务可以离线运行”更精确：每一项权利是否知道自己能在哪里行使、凭什么证据、到什么限度，以及中心听不到时由谁承担后果？

连接看起来是一项技术服务，但让人从“我想要”跨到“依法可以”的许可，是制度设计。当国家把这一区别写进架构，它就能在压力下实践一种罕见的克制：有权时说“可以”；能保存申请时说“我们已经收到”；而当一项延期后的确定性比不可撤回的错误更仁慈时，说“现在不行”。

证据与推断说明

- 开篇证据：西班牙银行于 2026 年发布对 2025 年 4 月 28 日停电的回顾，其中包含支付和取款影响数据；本文也采用欧洲中央银行的研究和一项私人支付数据分析，并保留各自分母与限制。[S01S02S04](#)
- 技术来源：对单调操作、权限与权利不变量的区分来自分布式系统文献；“离线权限档案”是本文提案，不是已经发布的标准。[S08S09S10](#)
- 沙特背景：连续性控制文件的存在，不等于某项服务在断网时授予权限的能力已经通过现场核验。[S11S12S13](#)
- 科学实验：25 种状态中的 13 种只指这个刻意简化的有限模型中出现违规的状态数，不能据此估计全国风险发生频率，也不能据此选择真实授权分配方案。
- 欧洲调查报告：专家组调查了伊比利亚停电，并于 2026 年 3 月发布最终报告。本文不以此事件证明任何沙特服务存在特定弱点。[S03](#)

主要来源

带完整链接、发布日期与推断边界的来源清单见可下载资料包内的 [sources.md](#) 和同一资料包内经清理的 [source_register.csv](#)；文章与科学附文中的 [Sxx] 引用均可点击。

延伸阅读

1. 西班牙银行（Banco de España），*How do we pay when the power goes out? Spain's blackout experience*，2026 年 4 月 27 日。[S01](#)
2. 欧洲中央银行（European Central Bank; ECB），*Keep calm and carry cash*，2025 年发表，包含停电期间支付数据分析。[S02](#)
3. 凯克萨银行研究部（CaixaBank Research），*The economic impact of the blackout in detail*，2025 年 6 月 18 日。[S04](#)
4. 约瑟夫·赫勒斯坦（Joseph M. Hellerstein）与彼得·阿尔瓦罗（Peter Alvaro），*Keeping CALM: When Distributed Consistency is Easy*，2019 年。[S08](#)
5. 彼得·贝利斯（Peter Bailis）等，*Coordination Avoidance in Database Systems*，2014 年，讨论数据与决策的应用不变量。[S09](#)
6. 国际清算银行（Bank for International Settlements; BIS），*Project Polaris: A Handbook for Offline Payments with CBDC*，2023 年 5 月。[S06](#)

7. 欧洲中央银行 (European Central Bank; ECB) , 离线数字欧元硬件标准咨询, 2026 年 8 月 18 日。
S16
8. 沙特中央银行 (Saudi Central Bank; SAMA) , 业务连续性框架及关于银行备用供电方案的通函。
S12S13