



STRATEGIC ESSAY

Editorial date: 25 September 2026

Who Holds the “Yes” When the Center Falls Silent?

A State That Can Continue Without Full Connectivity: Cash That Needed No Permission, and Authority That Can Be Distributed Before the Network Fails

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

MERIDIAN | Strategic Essay M02 | Editorial date: 25 September 2026 | Evidence cutoff: 25 September 2026 | Research horizon: 2026–2035

Opening: On the day large parts of Spain and Portugal went dark, a person could carry a bank card, a modern phone, and sufficient funds yet still be unable to complete a simple purchase. The money had not disappeared. What had disappeared was the path that allowed a distant authority to say “yes.” This essay asks a new question of the Saudi digital state: which decisions can we entrust in advance to a user, device, or employee, and which decisions must wait for a reliable connection to the center?

Editorial note: The accounts of Spain, the British Library, and European developments are grounded in published sources and specified dates. The thesis of “authority distributed before disruption” and its operational profile are research proposals, not descriptions of an existing Saudi system. The accompanying laboratory examines 25 limited synthetic computational states; it does not measure the Kingdom’s performance or the probability of attacks.

1. The Hour When Paper Became Faster Than Light

At **12:33 p.m. on Monday, 28 April 2025**, a widespread power outage began across the Iberian Peninsula. Much telecommunications traffic stopped, electronic payments failed, and some automated teller machines went out of service, while the banknotes already in people's hands remained usable in exchange. We need not invent a scene at a shop counter. In an account published in 2026, the Banco de España described how essential purchases such as food and medicine became harder when ordinary payment methods failed, and how some machines could not dispense the cash already inside them because they had lost power or connectivity. S01

There is a clean paradox here that needs no rhetorical decoration. Banknotes—an invention that some innovation discourse habitually consigns to the museum of economics—were among the few things that did not ask a server for permission to work. Paper did not prevail because it stored faster processors. It prevailed because **the authority to discharge its face value travelled with it before the lights went out.**

This is not a romantic celebration of everything old. People without enough cash did not benefit from its autonomy. Some cash-filled ATMs still failed. Commerce also needs power, security, supplies, a seller, and a buyer. The Banco de España itself documented that withdrawals collapsed during the outage, rose after service returned, and required logistical work to replenish machines. S01 Paper is no magic wand. It is a bounded example of **a right allocated in advance and usable without seeking fresh authorization each time.**

A European Central Bank (ECB) study adds quantitative evidence from the episode. In-person card spending in affected areas fell by about **41–42%**, based on the comparisons used in the studies it reviewed, and e-commerce in Spain fell by about **54%**. CaixaBank Research data estimated that consumer spending on the day of the outage fell by about **34%** against its comparison baseline, before a rebound over the next two days recovered much of the delay. These estimates are bounded by their sources and samples. They do not measure every transaction or every person. S02S04

As the lights returned, forms of payment gradually came back. On the morning of 29 April, the Banco de España reported that wholesale payment systems were operating normally and retail payments had resumed, while limited problems continued at some branches and ATMs. S05 These differences show that the phrase “payments failed” conceals layers of infrastructure, function, and place. But that is not the question pursued here.

The stranger question is this: **why can a banknote complete an economic act without real-time permission, while an application carrying the user's identity, balance, and trust history cannot act without a voice from afar?**

2. Connectivity Was Not the Only Absence; Permission Was Missing Too

We usually treat an outage as a problem of moving information. A network performs the work of a postal service: it carries messages between parties. Modern state institutions, however, use it for more than data. They also use it to carry **authority**: permission to pay, authentication of identity, confirmation that a right has not been used twice, or assurance that a delegation was not revoked a minute ago.

The distinction between “online” and “offline” is therefore insufficient. A device may retain a copy of a document without having the authority to determine whether it remains valid after revocation. An employee may know that an application arrived without having authority to approve it. A bank may store a payment instruction yet rightly refuse to call it money received by the beneficiary before settlement.

For this reason, I propose that Saudi digital services should not face a single question about whether they can operate **offline**. The question should contain four verbs: **what can we know, what can we receive, what may we promise, and what are we legally entitled to finalize?**

These acts carry radically different risks. A local employee can record an application for a new certificate and issue a receipt confirming provisional intake. Accepting a transfer of unique ownership, disbursing an entitlement that cannot be repeated, or making a decision whose effects are hard to reverse may require current information from a central register and explicit legal authority. Moving a request while offline is one thing. Creating final rights without verification is another.

The design philosophy proposed here is **Bounded Local Authority**: define the type of act an authorized party may complete locally, its temporal and numerical limits, the evidence that can verify it, what must stop or be referred, and how its effects will be reviewed when communication returns. Disruption grants no one new authority. It reveals whether specific authority was distributed lawfully and safely beforehand.

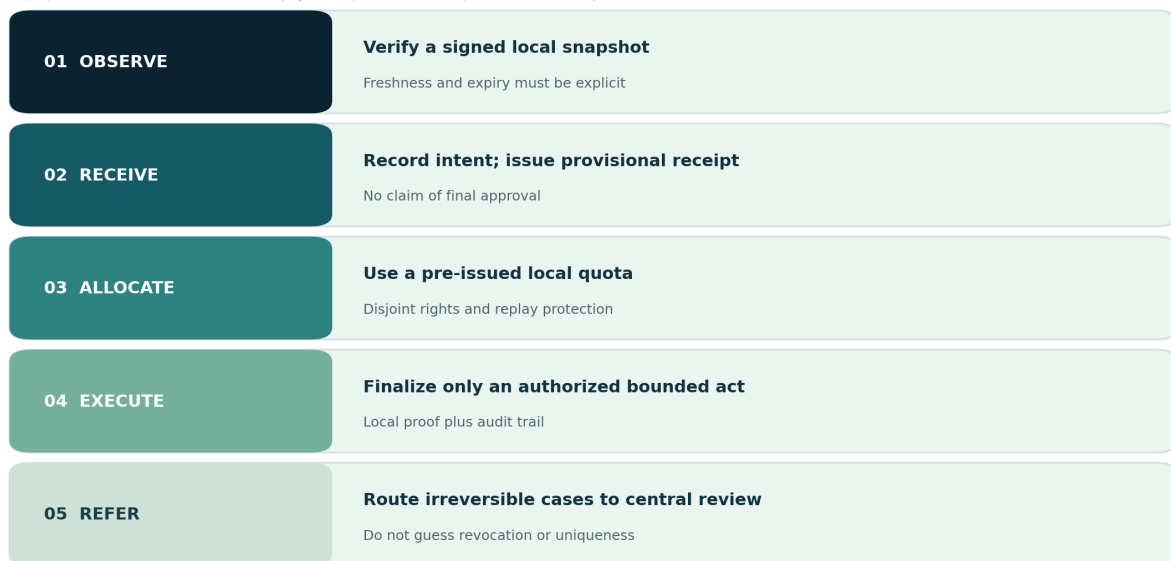
3. Five Doors, Not One Key

These are analytical levels, not an approved Saudi technical standard:

Door	What can be done with limited or no connectivity	Condition that determines whether the act is safe	What must not be claimed
Observe	Display a local copy of information or an authorization	Valid signature, identified source, issuance and expiry times	That the register was not changed or revoked moments ago
Receive	Collect a request and record its local submission time	Provisional receipt, tamper resistance, defined disposition of the request	That the request was finally accepted or the right was realized
Reserve	Use a preallocated share that another site cannot spend	Disjoint local right, maximum limit, replay prevention	That the share covers every claim or can be moved instantly between regions
Execute	Complete an act within a specific prior delegation	Verified identity, authority, integrity, audit log, and testing	That every service warrants execution without the center
Refer	Suspend an irreversible decision and give the beneficiary a clear reason	A continuing intake channel or an alternative route to help	That delay is completion or carries no human cost

WHO MAY DECIDE WHEN THE CENTER IS SILENT?

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



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

Conceptual ladder of proposed local authority

Figure 1 — A proposed conceptual ladder for delegating work during a connectivity failure. It does not represent actual authority in a Saudi system. Each function requires a defined legal basis, confidentiality and privacy limits, and security and operational validation.

The tradeoff cannot be resolved by saying, “design applications to work offline.” An application may operate and display data while remaining unable to know that someone else used the same right at a distant site. It may receive two conflicting requests and defer their resolution; that is appropriate for some work and disastrous for other work. **An offline interface is not necessarily an institution with authority to make a valid offline decision.**

4. What Does Mathematics Know About the Word “Yes”?

In distributed systems, maintaining an instantaneous shared truth can be difficult when two parties cannot exchange messages. This does not mean that everything requires the center. The need for coordination depends on **what an operation means**.

Joseph M. Hellerstein and Peter Alvaro explain this distinction through Consistency as Logical Monotonicity (CALM). In simplified terms, some operations add facts without later information invalidating what was previously established, and certain forms of those operations can be performed without continuous coordination. Other operations depend on proving that something has **not** happened elsewhere, on exclusive rights, or on the latest revocation state. Those are harder than merely collecting information. [S08](#)

Imagine two copies of a log in which two technicians record observations from fields they visited. If each adds an independent observation, the records may later be merged under a clear policy. Now imagine an inventory that contains one item and two points of sale, each of which believes the item is “still available.” Successfully merging the records later does not bring a second item into existence.

This is one reason for interest in Conflict-Free Replicated Data Types (CRDTs). Under specified conditions, these structures can ensure that certain replicas converge after exchanging their updates. They do not automatically make every business or administrative operation safe. Peter Bailis and collaborators, in their work on Coordination Avoidance, distinguish clearly between **state convergence** and preservation of **application invariants**. Two replicas may eventually converge on the fact that one entitlement was disbursed twice; convergence of the record does not repair the damage. [S09S10](#)

The result is a principle deeper than “always online” or “always offline”: **distribute acts whose validity conditions can be preserved; constrain acts that require global knowledge with delegated limits or deferred review; and stop what cannot be guaranteed safely.**

5. The 25-State Laboratory: When Two Sites Hold the Same Right

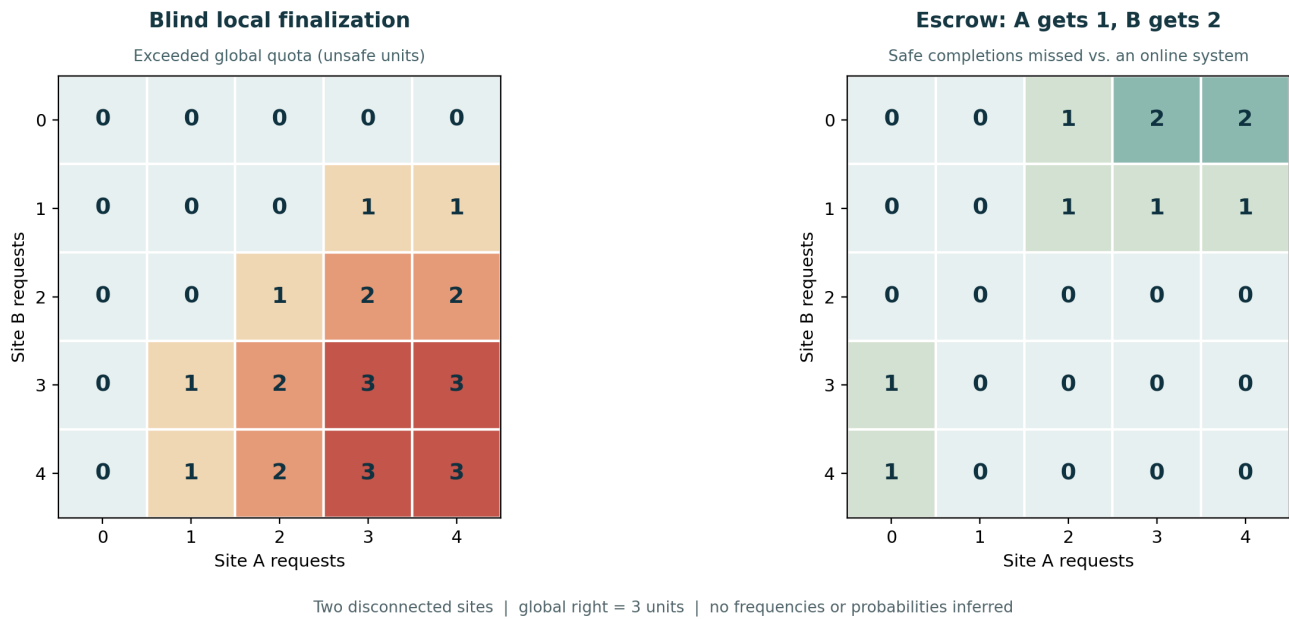
We can subject the idea to a small test, not as a prediction about a state, but as an explicit computational check of delegation logic. We ran a program that explores **25 possible combinations** of demand at two imaginary disconnected sites, A and B. Demand at each site ranges from zero to four, while the total right available to both sites is **only three synthetic units**.

We tested five policies:

1. **Central Stop:** No entitlement is finalized without connectivity.
2. **Provisional Intake:** Intentions can be recorded and a provisional receipt issued, without finalizing an entitlement.
3. **Escrow Allocation:** Site A receives the prior right to one unit and site B to two; neither may use the other's allocation until coordination returns.
4. **Reversed Escrow Allocation:** Two units for A and one for B, to test the effect of distribution.
5. **Blind Local Commit:** Each site sees the entire stale global balance and approves local requests against it. This is deliberately a bad policy designed to expose the error.

The exact result of this bounded example is that the fifth policy exceeded the global authorization budget in **13 of the 25 states**. Disjoint escrow allocation preserved the limit in every state **under the assumptions of honest local enforcement and no forgery or duplication of the allocation**. Across all example states, however, the allocation left ten units of safe completion unrealized that would have been available in a connected system. These figures remain **a mathematical count of states in an invented model, not an event probability or a real result from an institution**.

Twenty-five EXHAUSTIVE, SYNTHETIC request states



Synthetic computational check of the tradeoff between local authority and prior allocation

Figure 2 — The left panel shows the number of units above the budget in each state under blind approval. The right panel shows the number of safe completions forgone under a fixed (1, 2) allocation compared with full central knowledge. The heat-map colors refer only to model calculations.

In the example where site A requests three units and B requests none, the split design finalizes only one unit even though two units remain unused at the other site. This is **the cost of distributing authority in advance**: the entitlement remains safe, but the system loses the flexibility to move an allocation after the network closes. By contrast, if we tell each site that it is free to use the entire balance, an invalid sum creates an additional right.

A signed voucher presents a more deceptive problem. The two branches may each hold a digital token with a valid cryptographic signature, and each may successfully verify that signature locally. Yet if the same token can be copied and there is no strong way to prevent its redemption at two separate sites, a valid signature establishes its origin; **it does not establish that it has not been used twice**. The scientific companion includes a separate computational example of this case. It also states that stronger guarantees require protected hardware, carefully designed boundaries, key management, and replay prevention. We did not implement a real payment system.

This is the difference between delegating authority and distributing a copy of a message: **it is not enough for everyone to know what “yes” means; one “yes” must not become two merely because the telephone went silent.**

6. From the Banknote to the Euro That Has Not Yet Been Issued

This question has become part of research on future sovereign money. In May 2023, the Bank for International Settlements (BIS) Innovation Hub published a Project Polaris handbook for offline digital payments, followed by a more detailed design guide in October of that year. The project emphasized that this is not simply a matter of putting a wallet into airplane mode. The holding model, double-spending prevention, secure hardware, privacy, monetary limits, and reconnection process all affect feasibility. [S06S07](#)

In Europe, the European Central Bank announced in August 2026 a call for contributions on technical standards that might support an offline digital euro, including Secure Elements and embedded SIMs (eSIMs). Project documents made clear that the capability remained under development and testing, and that any issuance of the currency itself depended on a legal framework and later decisions. There is no basis for presenting the offline digital euro as a generally available payment instrument in September 2026. [S16S17](#)

The surprise is not that central banks are considering an alternative to cash. It is that **independent digital action needs a way to carry specific authority with it**, just as a banknote carries a promise made before its use. Bits are intrinsically copyable. Something easy to copy does not become scarce merely because it receives an elegant signature. To preserve scarcity, we must design constraints that enforce it rather than settle for an interface labelled “offline payment.”

Even the European project does not automatically solve the problem of a phone without power or a merchant unable to operate its equipment. “No internet,” “no electricity,” and “no institution capable of settlement” are three different conditions. Physical cash can therefore remain an important social complement even in a future with more intelligent digital wallets.

7. The Library That Kept Its Doors Open but Could Not Return All Its Books to Readers

Away from money, the British Library provides a different and necessary test of the idea. After the cyberattack in October 2023, its buildings remained open and study spaces remained available, while essential digital capabilities were disrupted and interim arrangements supported some services. In a review published in March 2024, the institution said that research services had been severely constrained and that the return of parts of the online catalogue did not restore all prior functions. [S14](#)

In a November 2025 update, the Library described the gradual restoration of functions, an interim ordering system and partial catalogues, and a longer path toward rebuilding secure digital infrastructure. [S15](#) Keeping reading seats available was a real achievement, but it did not give everyone access to everything they had once been able to request. This counters the idea that a manual or alternative plan must either save the whole institution or fail entirely.

Sometimes we need a kind of institutional honesty that has become rare in overeager applications. A service should be able to say: **“I can receive your request today. I cannot approve it now. Here is the reason for the delay, and here is how to follow the status of your right.”** In many cases, operational honesty is useful in itself. It reduces guesswork and supports triage, even though it neither removes the harm nor eliminates the need for equitable solutions for people who cannot wait.

The incident did not prove that interim operation moved every Library service into a safe state, or that a particular plan would have prevented the harm. It makes **graceful degradation** tangible: some functions continue within declared limits, without pretending that missing parts are present.

8. Saudi Arabia: We Are Not Starting from Nothing, and Having a Plan Is Not Enough

This question is different from advocating the purchase of more devices or data centers. Saudi regulations themselves offer starting points. The Saudi Central Bank (SAMA) issued its Business Continuity Management Framework in 2017. Instructions published in 2021 directed banks to prepare alternatives for electricity loss and to test the capacity and maintenance of backup generators. The Digital Government Authority (DGA) has also issued standards, controls, and reference guides for digital-government business continuity and risk management. [S11 \(related 2025 guide\)](#)[S12](#)[S13](#)

These sources establish a **regulatory framework for continuity**. They are not published evidence that a particular Saudi service can complete a sensitive offline transaction or automatically resolve a conflict. We must distinguish the existence of a policy, its implementation, the outcome of its testing, and the meaning of safety for the function allowed to continue.

I propose an **Offline Authority Profile (OAP)** as a research and design tool for government-service architecture. It would contain seven fields for each sensitive function:

1. **Right to be exercised:** Is this observation, intake, limited disbursement, or a final decision?
2. **Authorized party:** Who holds the power under law and policy, and what authority exists to delegate it locally?

3. **Local evidence:** Which signed data can be verified offline, and how old may it be?
4. **Delegation limit:** What value, count, period, region, or beneficiary class may not be exceeded?
5. **Stop condition:** Which state of doubt, conflict, or revocation requires refusal to proceed?
6. **Disposition of the request:** Is it finally completed, provisionally accepted, retained for review, or rejected?
7. **Reconciliation:** Who repairs conflicts, who bears the cost of error, and how does the applicant receive an explanation and appeal?

Calling this profile “artificial intelligence” would not make it intelligent. A model that predicts a user is **probably** eligible does not by itself create legal authority to finalize an entitlement. Artificial intelligence (AI) may help prioritize queued requests or detect conflicting records after connectivity returns, but a probabilistic estimate does not replace a rule of delegation or accountability for the decision.

Nor is this an argument for abolishing the center. In some services, **stopping well** is the highest form of responsibility. Two distant applications should not be allowed to approve a final surrender of a unique right against two stale copies and then tell the rightsholder that “synchronization will fix everything.” Synchronization may repair the record. The consequences of the decision may already have left the server and entered people’s lives.

9. Empowerment That Can Become Discrimination

An ethical and social paradox deserves to enter the engineering at the front door: people who retain cash, a charged battery, a document, and a modern phone do not represent everyone. The Banco de España observed that banks increased ATM replenishment after power returned, and that the usefulness of cash during a crisis also depends on prior access and distribution. S01 Carrying the same limit into digital authority raises uncomfortable questions. Can an older person without a protected device use the delegation? Can a request be received on paper with a number and tracking record? What happens to a user who loses a phone during the crisis or needs human assistance?

A serious test asks more than how many operations the system completed. It asks **for whom it completed them, who had to wait, and who bore the result of an invalid final decision**. A technically efficient architecture may be unfair if it restricts independent action to people with particular devices or a favorable connectivity history. An absolute stop policy may look cautious in institutional records while multiplying immediate social harm for people whose service cannot wait.

Every delegation therefore needs an **auditable cost**. What harm do we prevent by suspending a decision, and what harm do we create? Can we accept a provisional request with evidence and a reasonable review date? Does the intake employee treat the provisional receipt as a bounded promise rather than a certificate of final completion? These are not questions of public relations. They are operational definitions and conditions of rights.

When a crisis reaches a boundary beyond which the decision cannot be delegated, the institution should appear clearly: an alternative emergency channel where available, a declared order of priority, a means of appeal, and a record in which the applicant does not disappear merely because they have left the internet.

10. From Today to 2035: A State That Distributes Its Decisions Wisely

Three conditional paths can be imagined. They are not numerical forecasts:

Path one: a state with extensive interfaces and silent central authority. Some applications can display stored data, but most acts await the central server. The outage becomes a test of people's tolerance for delay rather than the institution's capacity to distribute safe action. Its sign is a proliferation of services with offline interfaces but no approved definition of a valid local procedure.

Path two: a state that delegates everything with premature enthusiasm. It issues broad temporary powers without clear invariants or guarantees against replay and key revocation. The numbers may look attractive on the first day of a crisis, only for disputes that are hard to repair to emerge after connectivity returns. Its sign is a set of final local decisions whose boundedness or legal basis cannot be demonstrated after reconciliation.

Path three: a state that knows how to distribute “yes” and define “not yet.” Sensitive services retain central authority over final rights where necessary, while distributing observation, intake, and limited delegation through prior evidence, valid signatures, validity windows, and clear recovery paths. They do not treat refusal of an unsafe act as a defect when they give people a channel that preserves their request and their right to review. Its sign is a body of authorized tests that demonstrate invariant safety, aggregate published reconciliation times, and known differences between groups and regions.

We need not predict a war to test whether the center can delegate a decision before it disappears. A national technology industry can build tools for this purpose: verifiable delegation policies, provisional receipts with audit integrity, non-repeating quota mechanisms, classification engines for acts that may proceed, and reconciliation systems that expose error

and give the affected person a clear remedy. Announcing a laboratory does not turn this into an export industry. It must prove itself in authorized real-world trials and find institutions that buy it, then buy again because of its results.

When Spain restored power, the definition of money did not change. What changed for a time was **the ability to use it through a particular medium**. The crisis revealed that people carry the right to complete some decisions with them, while other decisions reside inside a network that must answer. S01S02

The more important future question for the Saudi digital state may therefore be more precise than how many services work offline: **does every right know where it can be exercised, with what evidence, to what limit, and who bears the consequence when the center cannot be heard?**

Connectivity looks like a technical service. Permission—the bridge from “I want” to “I may”—is an institutional design. When the state builds that distinction into its architecture, it becomes capable of a rare virtue under pressure: saying “yes” when it holds the authority, “we have received your request” when it can preserve it, and “not now” when delayed certainty is kinder than a decision that cannot be undone.

Evidence and Inference Notes

- **Opening evidence:** The Banco de España published a 2026 review of the 28 April 2025 outage with evidence on payments and cash withdrawals. We also draw on the ECB account and a private-sector payment analysis, within the stated denominators and limitations. S01S02S04
- **Technical basis:** The distinction between monotonic operations and invariants governing valid rights comes from distributed-systems literature. The Offline Authority Profile is proposed by this essay and is not a published standard. S08S09S10
- **Saudi context:** The existence of continuity controls is a regulatory fact. It is not field validation that a service can grant offline authority. S11S12S13
- **Scientific experiment:** The figure 13 of 25 denotes violation states in a deliberately simplified bounded model. It cannot estimate the frequency of national risk or select a real delegation allocation.
- **European investigation report:** An expert panel investigated the Iberian outage and published a final report in March 2026. The incident is not used to establish that any Saudi service has a particular vulnerability. S03

Principal Sources

The complete list of sources, full URLs, publication dates, and limits on inference appears in [sources.md inside the downloadable bundle](#) and the [sanitized source register.csv in the same bundle](#). The [Sxx] references in both versions of the essay are clickable.

References That Extend the Question

1. Banco de España, *How do we pay when the power goes out? Spain's blackout experience*, 27 April 2026. [S01](#)
2. European Central Bank (ECB), *Keep calm and carry cash*, a 2025 study that includes payment-data analysis from the outage. [S02](#)
3. CaixaBank Research, *The economic impact of the blackout in detail*, 18 June 2025. [S04](#)
4. Joseph M. Hellerstein and Peter Alvaro, *Keeping CALM: When Distributed Consistency is Easy*, 2019. [S08](#)
5. Peter Bailis and collaborators, *Coordination Avoidance in Database Systems*, 2014, on data and decision invariants. [S09](#)
6. Bank for International Settlements (BIS), *Project Polaris: A Handbook for Offline Payments with CBDC*, May 2023. [S06](#)
7. European Central Bank (ECB), consultation on hardware standards for an offline digital euro, 18 August 2026. [S16](#)
8. Saudi Central Bank (SAMA), the Business Continuity Management Framework and the circular on alternative electricity arrangements for banks. [S12S13](#)