

THE GLAUX

Wisdom In Complexity

The Ledger and the Line

Why the future of public money turns on what a payment system is allowed to remember—and what it is allowed to decide

THE GLAUX

Wisdom In Complexity

ISSUE 24

OCTOBER 2026

The Ledger and the Line

Why the future of public money turns on what a payment system is allowed to remember—and what it is allowed to decide

• • •

The Purchase That Does Not End

Money has always carried more than value. A coin carried the authority that minted it and a promise that the exchange would be recognised. Yet cash also contained a limitation that became easy to overlook: once the exchange was complete, the money did not carry its story forward. A baker could take payment without learning a stranger's other purchases. A state could know how much currency it issued without inheriting a continuous account of how every citizen used it.

Digital payment systems alter that limitation. They can make exchange faster, cheaper, more resilient, and more accessible. They can also make every exchange legible to an infrastructure. The essential question is therefore not whether money should become digital. Much of it already has. The question is whether the public's digital money should become a **rail**—a neutral means by which value moves—or a **window** through which private life can be made continuously visible and, eventually, conditional.

The same technical components can support both outcomes. A ledger can settle a payment, record a history, apply a rule, screen a user, or prevent a transaction. A wallet can be an instrument in someone's pocket or a permanent relationship with an administrator. The form is created by the permissions around it.

That is why the contest over central-bank digital currency is not principally a contest between modernity and nostalgia. It is a contest over whether the disappearance of physical cash will also mean the disappearance of ordinary zones in which a person can act without creating a usable institutional trace. The benefit of a more efficient payment system is real. But so is the change introduced when payment becomes a comprehensive sensor of social life.

James C. Scott described a recurring state temptation: to convert the complicated texture of lived reality into a form that can be seen, counted, and administered from above. Such simplification can be necessary for taxation, public health, and collective coordination. It becomes destructive when the legible map is mistaken for the life it represents. ^[1] A retail digital currency raises this old problem in unusually intimate form. It can make the map of economic life more exact. It can also make the map harder to escape.

The central tension is therefore not privacy versus efficiency, as if one simply chooses less of one for more of the other. It is a difference in shape. Efficiency accumulates gradually: a payment settles in seconds rather than days; a merchant pays lower fees; a cross-border transfer involves fewer reconciliations. A universal record of ordinary purchases, combined with a capacity to apply conditions, changes the relationship between citizen and issuer at a threshold. It creates a capability that can be repurposed long after the original policy has been forgotten.

• • •

The Difference Between a Rail and a Window

The distinction between wholesale and retail central-bank digital currency clarifies the problem. Wholesale systems are used by regulated financial institutions to settle among themselves. Retail systems reach the public: households, shops, charities, small businesses, and anyone making an ordinary purchase. The technology may overlap, but the constitutional terrain does not.

In the wholesale domain, greater programmability and richer auditability are often proportionate to the task. Banks already operate inside dense systems of identity, reporting, finality, and supervision. Cross-border settlement has long been slowed by incompatible databases, correspondent-bank chains, time zones, and

reconciliation between separate ledgers. The Bank for International Settlements' Project Agorá has shown that tokenised central-bank reserves and tokenised commercial-bank deposits can be combined on a shared platform to support atomic multi-currency institutional settlement. Its real-value testing demonstrated feasibility and improved visibility; it was a prototype, not a declaration that all payments should now be rebuilt this way.^[2]

Here, the ledger is doing institutional work among actors already constituted by law as institutions. Its expanded capacity does not create a new, intimate relationship between the monetary authority and a person buying vegetables, paying a neighbour, joining a local association, or helping a family member through a difficult week. This does not make wholesale infrastructure politically empty. Its governance, interoperability, and market structure still matter. But the freedom cost is not of the same order because citizens do not inhabit it as their daily payment environment.

Retail money is different because it is part of ordinary independence. It lets a person transact without first explaining the exchange to a platform, employer, bank, advertising system, or future government. Cash has never guaranteed innocence or virtue; it also enables fraud, evasion, and coercion. Yet its opacity supplies a practical boundary: the public can issue money without inheriting a complete narrative of the lives conducted through it.

The United States shows why the categories should not be made too neat. Its central-bank institutions have researched tokenised wholesale settlement, while no U.S. CBDC has been authorised or issued. Current federal policy is not a clean welcome for wholesale CBDC and a ban on retail CBDC. Research, issuance, and public legitimacy are different acts.^[3]

The useful line is not “technology for banks, no technology for people.” It is more exact: the closer public money comes to becoming a daily interface for everyone, the more it should resemble cash in its basic constitutional qualities. Its default form should be a means of exchange, not a standing account of the citizen.

• • •

The Map in the Till

Two absolutist responses arrive quickly. The first says that any retail CBDC is a surveillance state in waiting, so the only safe choice is refusal. The second says that any privacy constraint is an anachronism, because digital payments already exist and a public system can be more efficient, inclusive, and accountable than private alternatives.

Both see something real. Neither sees the whole terrain.

Refusal protects against a genuine danger, but it can imagine that the status quo is a landscape of cash. It is not. Cards, platforms, and mobile wallets already mediate a growing share of ordinary life. Their business models may reward the combination of payment data with behavioural, commercial, and social data. The decline of public cash can transfer the map from a public authority to a firm whose constitutional obligations are weaker.

The Bank for International Settlements has described how large technology firms can build a reinforcing loop between data, networks, and activities: more users produce more data; more data supports more services; more services make it harder to leave. The same loop can lower cost and widen access. It can also create concentration, self-preferencing, exclusion, and a deeper dependence on the company that sees the most. ^[4] A payment system is never only a way to pay. It is an ordering of who gets to observe patterns of life and who gets to set the terms of participation.

Yet a democratic institution is not harmless because it is public. It is constrained only to the extent that restraint survives a crisis, a change of government, a new security doctrine, or a persuasive promise that more data will make society safer. The question is whether tomorrow's authorities will possess a capability too useful to leave unused.

This is where the language of trust becomes inadequate. Trust matters, but the issue is not principally whether citizens trust a central bank or a technology company more. A monetary architecture should be judged by what it permits when trust weakens. Cash does not ask its holder to believe that every future official will

decline to look. It makes looking difficult by default. A digital public currency needs an equivalent discipline: rights should rest not only on assurances but on boundaries built into law, infrastructure, and institutional habit.

• • •

Two Kinds of Programmability

The word *programmability* is often treated as if it described one thing. It does not. It hides two very different capacities.

The first is **programmable money**: the unit itself carries a restriction imposed by its issuer or an authorised intermediary. It may expire, be spendable only on approved goods, be blocked from particular merchants, or be routed according to a policy objective. This is money becoming a rule. It can be presented as a tool for targeted aid, emergency support, tax compliance, or climate policy. In limited settings, such tools may have legitimate purposes. A food voucher is not inherently illegitimate. But a voucher is not general money. The line is crossed when the ordinary money of the public begins to inherit the logic of the voucher.

The second is a **conditional payment**: a person chooses terms for a specific transfer. Payment on delivery, escrow for a house purchase, automatic release after a verified service, or simultaneous exchange of an asset and its price can reduce fraud and coordination costs. In this case, the condition belongs to the arrangement between the parties; it is not a standing permission written into money itself.

The distinction may sound technical, but it is constitutional. It separates a citizen using money to form agreements from an issuer using money to pre-structure the field of permissible agreements. The proposed digital-euro framework makes this distinction explicit. It rejects money whose use is intrinsically restricted to designated purposes, while allowing user-agreed conditional payment services. ^[5] The proposal is not yet enacted, and design language is not the same as durable law. Still, it shows that the line can be named.

Naming it is only a beginning. A core protocol can be formally non-programmable while its wallet, payment-service provider, compliance layer, or merchant acquirer creates practical conditions around every payment. If every public wallet must query an updatable identity service or permission layer, a prohibition placed only in the monetary unit may be too narrow.

The deeper issue is therefore not whether code exists. Code will exist. It is whether a citizen has access to a **general-purpose means of payment** whose ordinary use does not require a remote authority to interpret the reason for the exchange. The more everyday money requires an interpretation, the more a society turns its payment layer into an administrative language.

• • •

The Boundary That Moves at Night

Every surveillance architecture begins with a reason easier to accept than its later use: fraud prevention, sanctions compliance, disaster relief, inclusion, or consumer protection. These are not trivial goals. But once a system can identify, rank, freeze, or direct transactions at scale, new uses arrive with lower marginal cost and a familiar vocabulary of necessity.

This is why a debate confined to declared intentions misses the mechanism. The decisive question is not, “Will the present government program the currency?” It is, “What permissions will be available to any government, regulator, court, contractor, or compromised administrator that can reach the system later?” An architecture that technically supports universal traceability needs more than a privacy policy. It needs a constitutional decision about who can alter that architecture, under what legal standard, with what public notice, and with what possibility of reversal.

The European digital-euro work provides an instructive, incomplete attempt to think in this direction. The ECB says an offline payment mode is being designed to offer a cash-like degree of privacy: payment details would remain with payer and payee, while anti-money-laundering checks occur at the funding and defunding boundary. Online payments would have a different privacy model: the Eurosystem

would not directly identify users, but payment-service providers would identify them for compliance. ^[6] This is not anonymity everywhere. It is a layered design that recognises that privacy has gradients and that the location of a check matters.

The value of the design is not that it solves the problem once and for all. It is that it makes the boundary visible. Offline digital cash is a claim that there should remain a domain of ordinary exchange in which the central infrastructure has no transaction history to mine. Online compliance is a claim that some forms of digital payment cannot avoid identity obligations under current law. The tension has not disappeared; it has been put into a form that can be debated.

That is a better starting point than pretending that either perfect privacy or perfect control is available. Yet a boundary that exists only in a technical specification can move quietly. A budget line changes, a risk model is updated, an emergency measure is renewed, and a once-local exception becomes a default. The essential work is to turn the boundary into a public commitment that is difficult to amend without public attention.

• • •

The Merchant Beyond the State

The strongest case for a constrained public digital currency begins where the most confident critics of CBDC often stop: with the counterfactual.

Suppose a jurisdiction rejects a retail public option while cash recedes. Its payments may still become digital, instantaneous, and data-rich. The question is not whether anyone will operate the wallet, but which institution will: a bank consortium, card network, technology platform, or stablecoin issuer allied with the platforms that provide identity, messaging, and commerce.

These alternatives can deliver genuine benefits. They can innovate quickly, reduce frictions, provide useful interfaces, and serve people whom conventional banks have neglected. A well-designed private system can be less intrusive than a badly designed public one. The Bank of England and HM Treasury have therefore argued that any digital pound should not crowd out private innovation, and that regulated

private stablecoins could coexist with public money.^[7] The relevant comparison is not state purity against market corruption. It is an institutional comparison between concrete arrangements.

Still, private scale has its own politics. The Financial Stability Board's global recommendations for stablecoins call for accountable governance, risk management, data safeguards, transparent disclosure, recovery and resolution plans, and reliable redemption rights.^[8] These are not bureaucratic decorations. They are evidence that a widely used private monetary instrument also becomes a public-risk institution. The money may be issued by a company, but a run, a data breach, a dominant platform's exclusion rule, or a sudden change in terms does not remain a private event.

The question changes when private systems become the default. A public digital-cash option can then function less as a replacement for all private services than as a constitutional floor beneath them: a form of money that private interfaces may compete around but cannot fully enclose. Its purpose is not to give the state a larger role in every purchase. It is to ensure that the only digital alternative is not a commercial identity-and-data relationship.

But this argument has a limit. A public floor becomes a trap if it is built as a single compulsory doorway. The public option is defensible only when it remains one option among cash, bank money, and regulated private systems—and when its own protections are stronger, not weaker, than the protections demanded of its competitors. Public money should widen the field of exit, not become the only exit from private power.

• • •

A Constitution for Small Purchases

If a retail digital currency is explored, the relevant question is whether its design forms a coherent constitution for ordinary transactions. Four commitments matter more than promises about convenience.

First: make offline, cash-like transfer a core public function rather than an optional product feature. A token-like, device-to-device mode for modest proximity payments can preserve a zone in which neither issuer nor provider receives the transaction history. The ECB's design work points in this direction, but limits, hardware security, loss rules, and accessibility will decide whether the promise is real. ^[6] The failure mode is an "offline" option too small, inconvenient, rare, or dependent on prior identity checks to function as cash's analogue.

Second: prohibit purpose-restricted money in statute and extend the prohibition beyond the token itself. The law should bar public authorities from imposing expiry dates, merchant categories, product restrictions, or behavioural conditions on ordinary retail balances. It should also require that wallet providers and compliance layers cannot recreate those controls by another name. Conditional transactions voluntarily agreed by the parties can remain possible; issuer-defined spending permissions should not become a hidden feature of general money. The constraint is that legitimate court orders and narrowly defined fraud controls will still exist. The failure mode is vague exception language that gradually becomes a second operating system.

Third: place privacy thresholds and material design changes under democratic control. A central bank can provide expertise, but it should not alone decide how much ordinary economic life may occur without institutional observation. Parliament should set offline holdings and low-value privacy thresholds, with public reasons and review. Privacy authorities should audit data minimisation; courts should remain available when exceptional access is sought. The failure is either parliamentary micromanagement or a technical agency changing the social contract through a software release.

Fourth: build an expiry into the authority, not merely the software. A retail system capable of altering the relationship between money and citizenship should be re-authorised after a defined period. Reauthorisation would require public evidence: how often emergency powers were used, what data was retained, whether cash access improved or declined, whether the holding cap protected bank credit, which groups were excluded, and whether the public option reduced or intensified platform dependence. A sunset clause does not guarantee wisdom. It creates a moment at which a capability must make its case again before it becomes background infrastructure.

These commitments would not make a digital currency innocent. They would establish something more modest: a set of friction points between temporary political pressure and permanent monetary power. Their effectiveness would depend on enforcement, technical competence, and a public culture willing to treat a small purchase as a constitutional event when the alternative is a system that makes no distinction between a payment and a disclosure.

• • •

What a Cap Cannot Protect

A holding limit is often proposed as the practical answer to the banking problem. Modest public balances reduce the risk that deposits move to the central bank at once; linked accounts can replenish a payment balance and return excess funds to a bank. The proposed digital euro includes this kind of mechanism, and ECB analysis has tested hypothetical limits to reduce disintermediation risk. ^[9]

This is sensible engineering. It is not the whole political question.

A cap can protect bank funding; it cannot protect the meaning of the payment layer. A citizen with a limited balance can still make every small purchase through a system that creates a record. A no-interest rule can make a public wallet less attractive as a savings instrument; it cannot ensure that its underlying rails remain unavailable for social scoring, commercial profiling, or policy conditionality. Conversely, a privacy-preserving cash-like mode can protect a domain of ordinary exchange while still leaving the macroeconomic question of bank credit unresolved.

The two problems must not cancel each other rhetorically. Financial stability is not a pretext; credit matters to households and firms. Privacy is not an ornament; an unobserved domain matters to democratic independence. A choice about bank funding, fraud control, convenience, or sovereignty does not settle every layer at once.

The limits themselves have a paradox. Set them too low, and the public system becomes a symbolic wallet that people rarely use; its promise of a public alternative remains mostly ceremonial. Set them too high, and it may accelerate deposit flight in a moment of stress. The economist's cap is therefore also a civic signal: it says

that public money is being offered as a means of payment, not as an invitation to relocate one's entire financial life to the central bank. Whether that separation can endure under crisis pressure remains an open design problem, not a number that can be discovered once and for all. ^[10]

• • •

The Money That Must Forget

A mature payment system will need to remember some things. It must settle correctly, resist fraud, recover from failure, and answer to law. A mature society will need to forget some things as well. It must preserve room for people to buy, give, help, experiment, and change their minds without every ordinary movement becoming an input to someone else's model of them.

The future of public money may depend on whether these two requirements can be held together without turning either into a slogan. Wholesale settlement can become more programmable, auditable, and interoperable because its participants already inhabit a world of institutional permissions. Retail money should become digitally usable without becoming a general account of the population. Private platforms should be allowed to innovate without becoming the only owners of the interfaces through which daily life is transacted. Cash should remain not as a relic but as a reminder that a public currency can serve everyone without knowing everyone.

The question is not whether a society trusts the current people who would operate a CBDC. It is whether it can build a payment architecture whose restraints remain intelligible when those people are gone. A faster rail may be useful. A window that cannot be closed is something else.

REFERENCES

1. Scott, James C. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Yale University Press, 1998.
2. Bank for International Settlements. "Project Agorá." 2026. <https://www.bis.org/project/agora>
3. Congressional Research Service. "Central Bank Digital Currencies." IF11471, updated 15 July 2026. https://www.congress.gov/crs_external_products/IF/HTML/IF11471.html
4. Bank for International Settlements. "III. Big tech in finance: opportunities and risks." *Annual Economic Report*, 30 June 2019. <https://www.bis.org/publ/arpdf/ar2019e3.htm>
5. European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro*, COM(2023) 369 final. 28 June 2023. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0369>
6. European Central Bank. "FAQs on the digital euro." 17 August 2026; Commission nationale de l'informatique et des libertés. "Confidentiality in the Digital Euro: Where are we?" 26 May 2026. https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html; <https://www.cnil.fr/en/confidentiality-digital-euro-where-are-we>
7. Bank of England and HM Treasury. *The digital pound: a new form of money for households and businesses? Consultation Paper*. 7 February 2023. <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf>
8. Financial Stability Board. *High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final report*. 17 July 2023. <https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-global-stablecoin-arrangements-final-report/>
9. European Central Bank. "Technical data on the financial stability impact of the digital euro." 10 October 2025. https://www.ecb.europa.eu/euro/digital_euro/timeline/proofuse/shared/pdf/ecb.deprep251010_technical_annex_financial_stability_impact_digital_euro.en.pdf
10. Demertzis, Maria, and Juan Mejino-López. "On the digital euro holding limits." Bruegel, 16 July 2024. <https://www.bruegel.org/analysis/digital-euro-holding-limits>