

Draft for review. Not a locked spec. Architecture is a separate later note and may not join the protocol. Source of truth with version history: [Google Doc](#). [PDF](#). [Architecture requirements \(companion note\)](#). Previous versions: [v0.0002](#), [v0.0001](#).

Version 0.0003 · October 2026 · Draft

K0: A Peer-to-Peer Electronic Payment Protocol

Abstract

A purely peer-to-peer version of electronic payments allows value to move without a protocol-level custodian, without a card network in the middle, and without publishing every spend to the world. K0 is that protocol. It is defined by properties that must all hold at once: world scale, consumer-grade experience, regulatory compliance, security, and sufficient decentralization. A system that lacks any of these is not K0. Implementation follows the definition. The definition is not optional.

K0 settles in units of account that have a regulated issuer and one-for-one redemption — United States dollars as USDC today; other units later. The payer pays nothing. The merchant fee is always at most ten basis points (one basis point, 0.01%, is the published design point), and it is shown as its own line, separate from the payment itself. Privacy is cash-like by default and auditable under due process. **The protocol never holds the user's keys and takes no custody of its own. Balances are held by a Responsible Party under its own license.**

This paper states the protocol. Proposed machinery (wallets, chains, proofs) belongs in a separate architecture note and may or may not join K0. The requirements that note must meet are stated in §4A (the ledger) and §8 (incentives).

1. Introduction

Commerce on the internet still routes through institutions that take custody, delay settlement, price in percentages, and see too much — or, in public ledgers, show too much to everyone. Card networks, correspondent banks, and custodial wallets solved trust by inserting themselves. Open blockchains solved custody by publishing the books.

Neither is cash.

Cash settles at the moment of payment, names no intermediary, and leaves no public trail, yet a lawful authority can still investigate a person. That combination is the design target of a payment protocol, not of an application.

K0 is a payment protocol for the United States and for the world. A particular corridor (for example, a United States vendor paying an Indian one) may be used to test it. **The corridor is not the protocol.**

2. The problem

Seventeen years of public chains produced speculation, settlement experiments, and almost no everyday payment instrument. The failures are structural:



Custody. Wallets that hold keys for the user recreate the bank. The user is a balance on someone else's book.



Surveillance. Transparent ledgers make balances and counterparties public. Businesses will not run payroll or suppliers on a glass book. People will not.



Friction. Seed phrases, gas tokens, hex addresses, and multi-minute finality are not how people pay.



Law. Payments at scale attract money-transmission, sanctions, and travel-rule duties. Protocols that ignore this are pushed into custodial wrappers. Wrappers destroy the protocol.



Scale. A payment network must absorb peaks — not average throughput. Visa-class load is the floor, not a slogan.

These are one problem: a payment protocol that is not cash-like, not lawful, not usable, and not large is not a payment protocol.

3. Protocol definition

K0 is defined by the following, jointly. They are the DNA of the protocol. Implementation that ships without them has not implemented K0.

 **No protocol-level custody.** The protocol does not take possession of user keys and is never the customer's bank. Balances are held by a Responsible Party under its own license: a local bank, a reserve bank, or a government body. The Responsible Party is the regulated party, not the protocol. Fiat on and off the system is orchestrated through regulated issuers. Settlement units are units with a regulated issuer and one-to-one redemption: USDC at one-to-one with the dollar today; other units, whether another fully reserved stablecoin or a central-bank digital currency such as the e-rupee, when the same issuer and redemption properties hold. The protocol is not tied to any one unit; each payment settles in one unit.

 **Payer cost is zero.** The person sending money does not pay a protocol fee.

 **Merchant cost is basis points, not percents.** The published design point is 0.01% (one basis point). The fee is always at most ten basis points of the payment, in every settlement mode, and a rule that could charge more is not K0. Anything in card-network percents is not K0. The receiver chooses how the fee is settled: netted from the payment, prepaid, billed later, or another arrangement the rules allow. The mode changes when and how the fee is paid, never how much. The fee is a separate line from fulfilment: the merchant is credited the full payment, and the fee is recorded and reported as its own entry, so that both can be booked and audited apart. Because it is separate, the fee can be reduced or waived by rule, for a merchant, a corridor or a period. A waiver is a discount to the merchant, not a free ride on the network: someone funds it (§8).

 **Cash-like privacy by default.** Observers of the public record cannot read balances, counterparties, or amounts. Lawful authority can obtain audit under due process. Privacy that cannot be audited, or audit that is public, both fail.

 **Compliance in the protocol.** Identity attestation, large-value rules, and travel-rule data (where required) are protocol duties, not a company's afterthought. Compliance must not make the protocol itself a custodian.



World scale. Throughput and latency must exceed global card-network peaks: on the order of 65,000 transactions per second and above, with confirmation in human time (sub-second to the user). Linear scale-out is required. A chain that is fast in a lab and congested in a city is not K0.



Consumer experience. Sending value is as ordinary as existing payment apps: human names, not hex; no seed phrase on day one; no gas token in the user's hand. Complexity may exist beneath. It may not exist on the glass.



Security. Users cannot lose funds to protocol equivocation, trivial key theft as the default path, or silent inflation of the settlement unit. The settlement unit's reserves are not K0's to manage; they are the issuer's. K0 must not add a second reserve lie.



Sufficient decentralization. No single operator can freeze the protocol, rewrite history, or become the de facto custodian. “Sufficient” means users and merchants can leave an operator without leaving their money. A permissioned club that can halt payments is not sufficient, even if it is fast.

If a later architecture document proposes a mechanism, that mechanism is admitted only if it preserves all nine. Otherwise it is not K0.

4. Transfer without protocol custody

A payment is an instruction to move a settlement unit from one user to another such that:

- only the payer can authorize the spend;
- the payee receives final credit without trusting the payer after confirmation;
- neither party deposits funds with the protocol itself; balances stay with the Responsible Party;
- the issuer of the settlement unit remains the issuer, not K0.

Double-spend is prevented by the protocol's consensus over spends, not by a clerk. Finality for the user is the moment the protocol will not reverse the credit. Banking hours do not apply.

The protocol does not issue the dollar. It moves a dollar that already exists as a reserved token. Issuance, redemption, and reserve attestation stay with the regulated issuer. K0 that issued its own unreserved unit would be a different, worse protocol.

4A. The ledger

K0 requires a shared ledger that every participant can verify and no single operator controls. The ledger holds four kinds of thing and no others:

- **Accounts.** A named account is controlled by its holder's keys. An account records a position against a Responsible Party. It is not a deposit with the protocol (§3.1).
- **Attestations.** Proofs that a party has been verified to the standard a rule requires, and by whom. The ledger holds the attestation or a commitment to it, never the identity documents behind it (§6).
- **Transfers.** Signed instructions that move a settlement unit from one account to another, ordered and made final by consensus. A transfer records fulfilment and the fee as distinct entries, and both are final together.
- **Rules.** Programmable conditions that transfers must satisfy: thresholds, attestation checks, travel-rule attachment, and selective disclosure (§5, §6). Rules are code on the ledger, so compliance is a protocol duty and not a company's afterthought.

Anything else (a marketplace, a lending product, a loyalty scheme) may be built on K0. None of it is K0.

The ledger's mechanism (one chain or many, which consensus, which proofs) is for the architecture note. A mechanism is admitted only if it keeps all nine properties.

5. Privacy and lawful audit

Cash is private to bystanders and not private to a court with a warrant. K0 takes that as the rule.

Default. Amounts, balances, and counterparties are not on a public tape.

Exception. A party with lawful process can be shown what the law requires — no more. Selective disclosure is a protocol operation, not a database export from a company.

Prohibition. Mixing pools that exist only to defeat lawful process are not K0. Full-public ledgers are not K0.

The tension is real. It is not resolved by hoping. It is a constraint: privacy without a backdoor for operators, audit without a backdoor for the crowd.

6. Compliance without an intermediary

If compliance lives in a company, that company becomes the network. K0 therefore treats one-time identity attestation, thresholds, and travel-rule attachment as protocol rules over messages, not as terms of service.

The protocol does not need to read the user's life. It needs to know that a transfer which the law treats as covered is attested, and that required data can be delivered to required parties under the required conditions.

Users who will not attest may still be able to transact inside limits the law allows. Users who must attest, attest once; the protocol does not keep their documents.

K0 is software. The protocol itself does not hold balances. Balances are held by a Responsible Party, which is licensed for that role under the law of its own jurisdiction. The Responsible Party carries the licensed duties. The protocol carries the rules that the Responsible Party's regulator sets as checkpoints. The moment the protocol itself holds balances without a licensed party, it has failed its own definition.

7. Scale and experience

A payment protocol that cannot clear a stadium interval, a payroll Friday, or a holiday retail peak is a toy. Capacity must be above card-network peaks and must grow with use. Latency to the user must be a checkmark, not a spinner.

Experience is not decoration. If ordinary people cannot pay, the protocol does not exist in the market, and then it does not exist.

Scale that requires a central operator, or experience that requires a custodian, is rejected by §3.

8. Incentives

A ledger no one is paid to run is not decentralized, it is a hobby. Validators, operators and Responsible Parties carry cost and liability, and the protocol must pay for them without charging the payer (§3.2) and without charging percents (§3.3).

K0 may therefore carry a native coin. If it does, the following rules bind it:

1. **Incentive, not currency.** The coin secures the ledger and pays the parties who run it. It is not the unit of account. Prices, balances and settlement stay in the settlement unit (§3.1, §4).

2. **Never on the glass.** No payer and no merchant is required to hold, buy or spend the coin. Users do not see it (§3.7). Fees are charged to the merchant in the payment's own settlement unit and itemized apart from the payment (§3.3); conversion to the coin, where needed, happens beneath.
3. **Fees fund the network.** Rewards come mainly from the basis-point merchant fee. Issuance of new coin is bounded by published rule and decreases as fee volume grows. Where a fee is waived or reduced, the difference is paid by a named, published source (a sponsor, the treasury, or bounded issuance), so that operators are paid in full and the merchant sees the discount.
4. **Stake carries consequence.** Operators put stake at risk, and provable misbehavior is penalized by rule. Governance cannot exempt an operator from the penalty (§3.8, §3.9).
5. **No promise of return.** The coin is not marketed as an investment, and K0 makes no statement about its price. Whether, where and to whom it may be offered is a matter of law, decided before any issuance, not after.
6. **No second reserve lie.** The coin is never presented as backing, collateral for, or a substitute for the settlement unit's reserves (§3.8).
7. **Exit stays free.** No coin lock-in may stop users or merchants leaving an operator (§3.9).

The coin's supply, emission, staking and distribution are for the architecture note. The rules above are the test they must pass.

9. What this paper is not

This is not a product brief for a corridor, a wallet brand, or a token offering.

This is not an architecture. Mechanisms (accounts, proofs, topology, operators, coin economics) are proposed separately in the architecture note, with the caveat that they may never join the protocol.

During the pilot, K-0 acts as the Responsible Party. This is an interim step. The path is to hand that role to licensed parties: local banks, reserve banks, or government bodies. Until then the pilot operates within the limits the law allows for K-0 in that role. In that role K-0 works as a gateway, the way token-swap protocols do. The difference is that compliance is built into the protocol.

This is not a claim that a live network already meets §3. Implementation is in progress. The protocol is the test the implementation must pass.

Version 0.0003 is the definition, short on purpose. It adds the ledger (§4A) and the incentive rules (§8); see Version history.

10. Conclusion

K0 is cash for the internet that can still live with the law: no protocol-level custody, private to the public, auditable under process, cheap to the payer, cheap enough for the merchant, large enough for a country, simple enough for a person.

We have proposed the properties. We have not proposed the machine. **The machine is allowed only if it keeps the properties.**

References (working)

- K0 Architecture Requirements v0.1 (companion note), [architecture/](#)
- K0 Protocol Intro (hypothesis), <https://kzero.org/protocol-intro/>
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Version history

- **0.0003 (October 2026).** Settlement generalized from stablecoins to any unit with a regulated issuer and one-for-one redemption (USDC today; e-rupee and others later). §3.3: the fee is a separate line from fulfilment and may be waived or reduced by funded rule; the merchant fee is always at most ten basis points in every mode, and the receiver chooses how it is settled (netted, prepaid, billed later or otherwise). Adds §4A, the ledger: accounts, attestations, transfers and rules, no mechanism specified. Adds §8, incentives: a native coin may exist only as a security and operator incentive, never as unit of account, never required of payer or merchant, never as reserve. Former §§8 and 9 become §§9 and 10. The nine properties are unchanged. Architecture is stated in the companion note.
- **0.0002 (October 2026).** Custody restated. "Non-custodial" (Abstract, §3, §4, Conclusion) becomes "no protocol-level custody": balances are held by a Responsible Party (a local bank, a reserve bank, or a government body) under its own license. §6 replaces "K0 is software. It is not a money transmitter." with software-plus-licensed-operator wording. §8 states that K-0 acts as the Responsible Party during the pilot, as an interim step. Throughput target unchanged.
- **0.0001 (October 2026).** First published definition.

K0 Protocol Whitepaper v0.0003. Architecture is out of scope; see the companion requirements note.