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. Previous version (v0.0001).

Version 0.0002 · 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 stable units of account — United States dollars as USDC, one-for-one, today; other coins later. The payer pays nothing. The merchant fee is on the order of one to ten basis points (one basis point, 0.01%, is the published design point). 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.

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 fully reserved stablecoins: USDC at one-to-one with the dollar today; other coins when the same reserve and redemption properties hold.

- **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 acceptable band is one to ten basis points. Anything in card-network percents is not K0.

- **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 stable 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 stable 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.

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. What this paper is not

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

This is not an architecture. Mechanisms (accounts, proofs, topology, operators) will be proposed separately, 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 0.0002 is the definition, short on purpose. It changes how custody is stated; see Version history.

9. 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 Protocol Intro (hypothesis), https://kzero.org/protocol-intro/
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Version history

- **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.