Mowsie: The Monetary Fabric

A Stateless Zero-Knowledge Value Layer for Bitcoin

Money Without Memory

"…and through the eyelet lay an absurdly small black hole, no larger than a mouse."

Abstract

Mowsie is a stateless, zero-knowledge monetary fabric enabling instant BTC-denominated transfers without operating a blockchain, ledger, address system, or consensus mechanism. Users deposit native BTC into a vault on Bitcoin, generate commitments inside a minimal ZK-verified fabric (executed on Solana), and transact using value objects created and destroyed in microseconds through an infinite-mint / immediate-burn engine. Only a single evolving global state root persists; no transactional history, graph, or metadata is retained.

This paper defines the monetary fabric itself. Broader economic analogs, including fiat velocity and QE/QT dynamics, are discussed separately in Appendix A.

1. Overview

The Mowsie monetary fabric is neither a blockchain nor a rollup. It is a stateless transition layer for Bitcoin-denominated value.

Users deposit BTC into a shared vault on the Bitcoin chain. Inside the fabric, value is represented as zero-knowledge commitments that can be created, consumed, and transferred without generating any persistent history. A single global state root—representing a Merkle commitment to unspent notes—is the only structure that evolves over time.

Solana serves as a high-performance proof-verification substrate, but it never sees amounts, identities, user relationships, or transaction data. It observes only cryptographic proofs and nullifiers.

The outcome is a Bitcoin-native monetary environment that records nothing about how value moves.

Note: The infinite-mint / immediate-burn model described here is unique to Mowsie and does not appear in any prior monetary architecture.

2. Statelessness

The defining property of Mowsie is that nothing about value motion is ever stored.

- No addresses
- No accounts
- No balances
- No transaction history
- No mempool
- No transaction ordering
- No timestamps
- No signatures on-chain
- No logs or receipts

The fabric retains only:

1. A global state root
2. A commitment tree of unspent notes

Nullifiers are not stored as a growing list. They are used ephemerally during proof verification to demonstrate consumption of a note within the active state horizon and then discarded. Nullifiers never enter global state and never accumulate over time.

Because there is no ledger, no graph exists for chain analysis or metadata inference. No relationship, identity, or transactional structure can be reconstructed.

2.1 No Addresses

Traditional systems rely on global addresses that reveal sender–receiver linkability and persist forever. Mowsie eliminates this entirely.

There are no addresses, no accounts, and no global identifiers within the protocol.

The fabric does not map senders to receivers, maintain an account space, or store routing information. Every state transition appears identical to the protocol:

- a commitment is created
- a commitment is consumed
- a proof verifies correctness

No wallet identities or user relationships are ever implied or observable.

2.2 Local Handles, Receive Descriptors, and Address Books

Although the protocol maintains no global identity layer, users still require a way to direct value. This is achieved without introducing addresses or persistent state.

Each wallet exposes a receive descriptor—a compact payload containing only the cryptographic information needed to construct an output note. Descriptors may be shared via:

- QR code
- URI
- direct transfer

When imported, the wallet stores the descriptor locally as a contact entry (e.g., “Alice,” “Bob”). These contacts:

- never leave the device
- never appear in proofs
- never touch the protocol
- never become part of global state

Each wallet maintains its own private address book, and the fabric remains completely unaware of user relationships, preserving strict statelessness.

3. Value Objects and State Transitions

Inside the fabric, value is represented as commitments—cryptographic notes bound to secrets known only to their owners.

A transfer proceeds as follows:

1. The sender proves control of a note without revealing its contents.
2. The sender constructs new commitments for the receiver.
3. A zero-knowledge proof validates the state transition.
4. The consumed note’s nullifier is revealed for this transition only.
5. The new unspent commitments are added to the global state.

Value objects exist only long enough to participate in a single transition. They are created, proven, and destroyed within one operation.

Only unspent commitments enter the global state. Spent notes leave no residue: once their nullifier is revealed, they are cryptographically burned and never stored or referenced again.

The global state contains only what is currently alive. No ledger or historical record is ever retained.

4. Deposits and Withdrawals

Users deposit BTC into a shared vault on the Bitcoin chain. All funds are pooled; no per-user segmentation exists.

To withdraw, a user presents:

- a ZK proof of control over an unspent note
- a withdrawal instruction
- a destination Bitcoin address

Solana validates the proof and authorizes a Bitcoin-side vault transaction.

The vault retains no transactional history. It relies solely on proof validity and amount consistency.

5. Privacy Model

Privacy arises from structural minimalism:

- no addresses
- no identity
- no transaction graph
- no history
- commitments that reveal nothing
- nullifiers that reveal one bit
- ZK proofs revealing only correctness

Because there is no graph, no relationship can be inferred. Because there is no history, no metadata can be analyzed. Because there are no addresses, nothing is linkable.

The protocol does not know:

- who sent
- who received
- when
- how often
- or how much

It knows only that a transition is valid.

6. Implementation Substrate

Solana is used for ZK-proof verification due to:

- predictable slot times
- high throughput
- low latency
- efficient global root updates
- minimal fee overhead

Solana stores no user data, amounts, identities, or history. It functions purely as a deterministic verification engine.

The monetary fabric remains substrate-agnostic.

7. Security Model

Security relies on:

- soundness of the ZK proving system

- collision resistance of the global commitment root
- Bitcoin vault security
- correct nullifier-domain design
- proper verification logic on Solana

Because Mowsie has no ledger, many traditional attack surfaces do not exist:

- mempool manipulation
- MEV
- ordering attacks
- replay attacks
- chain reorganizations
- graph analysis
- timing correlation

All sequencing arises from deterministic mass-based ordering, described in Paper 2: Mass-Based Deterministic Ordering.

8. Conclusion

Mowsie removes the ledger entirely. Validity replaces history. Proof replaces signature. Statelessness replaces accounts. A single evolving state root replaces transaction logs.

This produces a Bitcoin-denominated value system with:

- instant private transfers
- no addresses
- no accounts
- no balances
- no linkability
- no identity
- no memory
- no metadata
- extreme scalability

A genuinely stateless, zero-knowledge monetary fabric.

For economic context and analogs to monetary velocity, see Appendix A: Fiat Consequences.