Mowsie: A Monetary Fabric for Stateless Bitcoin Velocity

Money Without Memory

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

Abstract

Mowsie is an open-source, stateless cryptographic value layer enabling instant, private Bitcoin-denominated transfers without operating a blockchain, ledger, token, or consensus system. Users deposit native BTC into a vault on Bitcoin, generate zero-knowledge commitments, and move value inside a minimal, proof-verified fabric on Solana. The core mechanism—an infinite-mint, instant-burn engine—ensures value objects exist only long enough to complete a state transition, leaving no history, lineage, or transaction graph. Bitcoin anchors long-term value. Mowsie provides the microsecond store-of-value necessary for motion. The result is a monetary fabric where value exists only in the present state, enabling pure velocity, strong privacy, and a dramatically simplified attack surface.

1. Introduction

Blockchains preserve history. They store every transfer permanently as part of a ledger. This enables global verification but forces tradeoffs in speed, privacy, and complexity. Lightning improves speed but requires channels and routing assumptions. Privacy chains hide transactions, but still retain ledgers and heavy protocol surfaces.

Mowsie takes a different approach. Instead of optimizing a ledger, it removes the ledger entirely from the movement of value. The system consists of Bitcoin for settlement, Solana for proof verification, and a stateless zero-knowledge (ZK) monetary fabric that handles internal value transitions with no transaction history whatsoever.

No existing system achieves this level of statelessness. Ledger-based designs—including UTXO chains, account models, rollups, mixers, and Chaumian e-cash variants—retain some form of historical record or sequential linkage. Even systems that enhance privacy, such as Lightning or ZK rollups, preserve channels, routing structures, or batched transaction logs. Mowsie is distinct in that it eliminates persistence entirely: the fabric stores no addresses, balances, transactions, or lineage—only the current state root. To our knowledge, no deployed architecture removes history this completely while remaining cryptographically verifiable.

Mowsie follows a principle of radical minimization: remove every component that is not strictly necessary for value transfer. What remains is a fabric that treats money purely as motion, not storage. The goal is not to compete with Bitcoin as a ledger, but to provide the missing 'velocity layer' that a ledger cannot achieve.

1.1 Roadmap

This paper proceeds as follows:

Section 2 introduces the concept of a stateless monetary fabric and explains how Mowsie removes persistence from value.
Section 3 formalizes the infinite-mint / instant-burn engine and the conservation equation that enables value transitions without lineage.
Section 4 presents the economic model, including the absence of a token, market cap, or speculative surface, and explains how crumbs sustain the system.
Section 5 outlines the protocol architecture across Bitcoin, Solana, and the Mowsie fabric.
Section 6 defines the commitment structure used to represent value.
Section 7 describes the fixed proving circuit and verification constraints.
Section 8 develops the protocol's threat model.
Section 9 covers deposits and withdrawals.
Section 10 details Mowsie's privacy properties.
Section 11 explains the open-source requirements of the system.
Section 12 concludes with broader implications of stateless value consensus.

2. Monetary Fabric: Money Without Memory

In traditional systems, money is both a record and a balance. A UTXO or account entry is a persistent object with a past. Mowsie removes persistence. Inside the fabric, value is represented by commitments that exist only in the present moment. No addresses, no transactions, no lineage. Only a current state root.

This produces a monetary fabric rather than a ledger—a domain where value flows freely and instantaneously, constrained only by mathematical correctness. Value does not retain memory; it exists only as long as needed to move.

3. Infinite-Mint / Instant-Burn Engine

Every value object inside Mowsie follows a three-step lifecycle: it is minted as a fresh commitment, used as input to a state transition, and immediately burned. The old state is destroyed, replaced with a newly minted commitment. No commitments persist. No history accumulates.

This mechanism prevents inflation mathematically. The system enforces conservation of value and non-negativity, but does not retain any prior structure. A commitment has no parent, no children, and no ancestry. It exists only long enough to perform its role.

3.1 Conservation Without Lineage

Formally, the fabric guarantees strict conservation without preserving lineage:

$$\sum B_{old} = \sum B_{new} \qquad (1)$$

but no structural link is retained between the two sets. The burn is absolute; the mint is instantaneous.

This equation expresses the core of Mowsie's monetary model: value transitions must balance, but they do not inherit identity from previous commitments.

3.2 Stateless Root Evolution

Rather than maintaining a history of objects, Mowsie retains only a single state commitment that is updated exclusively by proof:

$$\text{Root}_{t+1} = \text{Update}\left(\text{Root}_t, \pi\right)$$

Here, t denotes the current state-transition index, and π is the zero-knowledge proof verifying the correctness of the transition.

No intermediate commitments persist; only the evolving root is preserved. This root serves as the canonical state of the system—no addresses, transactions, balances, or historical artifacts remain.

By removing lineage entirely, the system collapses to a minimal, proof-driven state.

This microsecond lifespan is not a limitation—it is the final form of money. In the end stages of hyperinflation, fiat currencies accidentally behave this way: they store value only for the instant it takes to spend them. Mowsie achieves this intentionally and without economic collapse, reducing the store-of-value function to the precise minimum required for movement. Value persists for the duration of the transition and no longer. This is money stripped to its mathematical essence: a momentary carrier of value that cannot inflate, cannot accumulate, and cannot leave a footprint.

4. Economic Model

Mowsie has no token, no market cap, no circulating supply, no inflation schedule, and no governance layer. The only measurable quantity is the amount of BTC present in the vault at any moment—the value currently inside the fabric. Mowsie cannot inflate because it cannot store value beyond a microsecond. Inflation is a time-based phenomenon; Mowsie removes persistence from money, leaving Bitcoin to serve as the long-term store of value.

4.1 Incentive Landscape and Why This Space Was Unexplored

This design space has remained largely unexplored because it cannot be monetized in conventional crypto terms. A stateless system with no token, no market cap, and no persistent balances offers no speculative surface and no mechanism for extracting value from users. Crypto platforms typically optimize for assets that appreciate, accumulate TVL, or generate narrative-driven liquidity. Mowsie does none of these. Its value objects disappear instantly, and the protocol retains no internal capital to leverage. By removing persistence, Mowsie eliminates not only inflation but also the incentive structures that have

historically motivated firms to build financial primitives—leaving a class of monetary architectures that simply went unexplored.

4.2 Fee Model: Crumbs as Self-Sustaining Infrastructure

Mowsie charges a single satoshi for a deposit, withdrawal, internal send, or wallet renewal. These crumbs sustain infrastructure, replenish the faucet for new wallets, and fund development through aggregated usage. Because the protocol is so light, even such crumbs are sufficient.

4.3 Wallet Expiration and the Feast of Crumbs

Each Mowsie wallet has a two-year lifespan and may be renewed for a single crumb. If a wallet expires, its commitments become invalid inside the fabric, but the corresponding BTC inside the unified Bitcoin vault remains intact. Any unrenewed crumbs automatically revert to the protocol and are swept into the DAO's internal Mowsie wallet.

Because the vault is a single consolidated on-chain UTXO pool, these crumbs do not require any Bitcoin consolidation transaction and incur no Bitcoin network fees. The DAO wallet accumulates orphaned crumbs continuously and may periodically withdraw them once its balance reaches a meaningful threshold. This automated sweep—informally known as the protocol's Feast of Crumbs—ensures that no BTC is ever lost while allowing the system to self-fund maintenance, development, and faucet replenishment.

5. System Architecture

Mowsie consists of three cooperative layers:

- Bitcoin Settlement Layer
- Solana Verification Layer
- Mowsie Monetary Fabric

5.1 Bitcoin Settlement Layer

All value originates as native BTC deposited into a vault on the Bitcoin blockchain. Bitcoin secures the long-term store of value. Mowsie does not create synthetic assets or wrapped tokens.

5.2 Solana Verification Layer

Solana verifies zero-knowledge proofs and stores the current state root. It does not hold funds or execute arbitrary application logic. It simply enforces correctness of each state transition.

5.3 Mowsie Monetary Fabric

Inside the fabric, value exists only as commitments. Users hold secrets locally. The system holds only a single Merkle root representing the live commitments. No history, no addresses, no transactions.

6. Stateless Value Commitments

$C = \text{Commit}(sk, r, B)$

sk: secret key
r: randomness
B: balance

Users generate proofs showing knowledge of a commitment included in the state, authorize updates, and mint new commitments. The old commitments burn and the state root updates. Nothing persists.

7. Proving System and Fixed Circuits

Mowsie uses a minimal fixed circuit responsible only for commitment hashing, Merkle verification, authorization, balance updates, and conservation. No VM, no scripting, no transaction format. The attack surface is extremely small and easy to audit.

8. Threat Model

Mowsie maintains security by minimizing state, minimizing assumptions, and minimizing the attack surface. The system's stateless design removes entire classes of attacks present in ledger-based systems but introduces unique considerations around proof verification and root evolution. This section outlines the threats Mowsie defends against, the assumptions it relies upon, and the boundaries of the model.

8.1 Assumptions

1. **Bitcoin is secure as a long-term settlement layer.**
   The vault UTXO pool inherits Bitcoin's consensus security and immutability.
2. **Solana continues to provide a high-throughput, censorship-resistant proof-verification environment.**
   Solana does NOT store value, execute user logic, or hold balances; it only enforces correctness of zero-knowledge proofs.
3. **The proving system is sound.**
   Zero-knowledge proofs correctly enforce commitment validity, balance conservation, and authorization rules.
4. **Users manage their secrets securely.**
   Loss of a secret means loss of control over its commitment — as with any cryptographic money system.

These are the minimal assumptions required for a stateless monetary fabric.

8.2 Threats Removed by Statelessness

The following classes of attacks do not exist in Mowsie due to the absence of ledger state, addresses, or history:

1. **Transaction graph analysis**
   No transaction graph exists.

2. **Address clustering**
   Mowsie has no addresses.
3. **Temporal correlation or mempool surveillance**
   Internal movements have no timestamps or mempool presence.
4. **State-bloat or history-rewriting attacks**
   Mowsie stores a single Merkle root; there is no ledger to rewrite.
5. **Replay attacks**
   Commitments burn immediately after use; nothing can be replayed.
6. **Front-running or MEV extraction**
   There are no transactions, ordering keys, or mempools to exploit.

Statelessness dramatically reduces the attack surface.

8.3 Threats Mitigated by Construction

Mowsie includes built-in safeguards against attacks that DO apply to stateless systems:

1. **Fake-balance creation via invalid proofs**
   Prevented by Solana-verified zero-knowledge proofs enforcing non-negativity and balance conservation.
2. **State-root corruption**
   Only proofs accepted by the on-chain verifier can update the root. Invalid transitions cannot be appended.
3. **Commitment forgery**
   Commitments require knowledge of the secret key and randomness and must pass Merkle inclusion checks.
4. **Infinite-mint attacks**
   The mint-burn cycle is mathematically limited by the conservation equation; see Equation (1).

No commitment can create new value without burning an equal amount of old value.

8.4 Threats Remaining Out of Scope

The following classes of threats are outside the scope of Mowsie's trust model:

1. **Compromised user devices or malware**
   If a device leaks secrets, an attacker may authorize transitions.
2. **Coercion or social engineering**
   Mowsie cannot protect against users being forced to reveal secrets.
3. **Bitcoin L1 compromise**
   If Bitcoin consensus is captured or its cryptographic primitives fail, the vault is vulnerable.
4. **Solana halting or long-duration network partitions**
   Users may be unable to submit proofs, but no value can be stolen.
5. **Cryptographic failures of primitives (hashes, curves, circuits)**
   As with any ZK system, the breaking of a primitive is catastrophic.

These risks are common across all systems built on cryptographic commitments.

8.5 Summary

Mowsie's primary defense is radical minimization: no transaction history, no ledger, no addresses, no persistent objects, and no scriptable state. The system's security reduces to the soundness of its proofs and the correctness of the single state-root transition. This minimal state model eliminates entire categories of attack while keeping the remaining threats well-bounded and easy to reason about.

9. Deposits and Withdrawals

Deposits occur on Bitcoin and produce a fresh commitment in the fabric after settlement. Withdrawals destroy a commitment and release corresponding BTC. Inside the fabric, all movements are instant and unrecorded.

10. Privacy Properties

Mowsie provides privacy by structural absence. No ledger, no transaction graph, no mempool, no addresses. Only the current root exists. Deposits and withdrawals cannot be linked. Internal value movements leave no trace.

11. Open Source Philosophy

Mowsie must be open-source. The protocol's design—minimal circuits, stateless transitions, and instant burns—relies on transparency as a security guarantee. With no ledger to audit, the correctness of the system depends entirely on public inspection of the circuits, hash logic, commitment scheme, and on-chain verifier. A closed implementation would contradict the fabric's core principle: nothing persists except mathematical truth. Open code ensures every user, auditor, and researcher can validate the system without trusting any developer or institution.

12. Conclusion

Mowsie introduces a new monetary primitive: a stateless fabric where Bitcoin flows without history. The infinite-mint, instant-burn engine removes persistence, eliminates graphs, and achieves pure velocity while relying on Bitcoin for long-term value. Value inside the fabric becomes microsecond money—existing only long enough to move. The design is simple, verifiable, and naturally suited for open-source development.