Mowsie: Mass-Based Deterministic Ordering

A Stateless Sequencing Model for ZK-Native State Transition Fabrics

Velocity Enforced by Entropy

"Secret Sauce*: In a singularity, the heavy objects fall first."*

Abstract

Mowsie is a stateless, zero-knowledge monetary fabric for Bitcoin. Because the system retains no ledger, no mempool, no timestamps, and no transaction history, it requires a deterministic, metadata-free method of ordering state transitions. This paper introduces Mass-Based Deterministic Ordering (MBDO) — a sequencing model in which commitments collapse toward the global state root according to their mass, with ties broken by the infinitesimal asymmetry inside each note's commitment hash.

This creates a two-layer gravitational system:

Mass provides macro-scale gravitational order.
Commitment hash provides micro-scale quantum order.

Ordering is not constructed — it is discovered from the information already inside each cryptographic commitment.

1. Introduction

Stateless systems eliminate mempools, sequences, nonces, and block producers. In Mowsie, users create zero-knowledge proofs that update a global state root, but no history is kept. For multiple transitions to converge to the same root, they must respect a universal ordering rule.

MBDO solves this by assigning every commitment a mass, derived from the note's commitment and internal entropy. Higher-mass commitments "fall" into the singularity of the state root first. If two commitments share the same mass, their ordering is determined by an infinitesimal, deterministic property already present in their commitment hashes.

This produces a canonical, unavoidable order without metadata, timestamps, or sequencing values.

2. The Ordering Problem in Stateless Fabrics

Blockchains enforce order through blocks, timestamps, nonces, gas prices, mempools, leader election, and validator discretion.

Mowsie has none of these.

Any external ordering signal would leak metadata, create linkability, reintroduce history, enable MEV, require trust, and violate statelessness.

A stateless fabric requires an ordering mechanism that:
- uses no history
- uses no added metadata
- cannot be influenced
- is globally deterministic
- is ZK-verifiable

MBDO achieves this by treating commitments as gravitational bodies.

3. Mass: The Primary Gravitational Field

Each commitment has a scalar mass, determined by:

mass = H(commitment || internal_entropy)

Mass is deterministic, private, collision-resistant, ZK-efficient, uniformly distributed, impossible to grind, and unrelated to value or identity.

It is the macro-gravity of the fabric — the first layer of the ordering field.

3.1 Why Mass Works

Because mass is derived from randomness already embedded in the note, impossible to manipulate, globally comparable, and consistent across all verifiers, it acts as a natural ordering coordinate in the commitment universe.

4. Two-Layer Gravitational Ordering

The Mowsie universe has two gravitational fields.

4.1 Macro-Gravity: Mass → Singularity Interaction

Higher mass = stronger gravitational pull. Higher mass commitments must collapse into the state root before lower mass commitments.

This avoids reordering attacks, MEV, timing games, and mempool manipulation.

It provides a deterministic cosmic ordering.

4.2 Micro-Gravity: Hash → Object Interaction

If two commitments share the same mass, the commitment hash determines which object is infinitesimally closer to the singularity.

The ordering rule:

```
if mass(A) > mass(B): A first
if mass(A) < mass(B): B first
if mass(A) == mass(B):
    if commitmentHash(A) < commitmentHash(B): A first
    else: B first
```

This yields perfect determinism without adding any entropy or metadata.

5. Ordering Is Discovered, Not Constructed

Mowsie adds no additional randomness, no extra fields, no nonces, and no sequencing metadata.

Ordering emerges from the infinitesimal information already present in the commitments themselves.

Every commitment contains micro-structure. The protocol reads that structure instead of adding new information. The universe of commitments already encodes a natural order.

Mowsie merely reveals it.

6. Why Collisions Don't Matter

Mass is derived from a collision-resistant hash. Collisions are theoretically possible, astronomically unlikely, and harmless due to the micro-gravity tiebreaker.

If two commitments share the same mass, their commitment hashes differ. Hash ordering resolves the tie. The state root remains deterministic.

A full collision in both mass and commitment hash would require breaking modern cryptographic hashing at the level of 2^{512} entropy — equivalent to guessing an atom in a universe made of universes.

The gravitational pair (mass, hash) produces a strict total ordering over all commitments.

7. Entropy Expansion: $2^{256} \times 2^{256} = 2^{512}$

Bitcoin private keys inhabit a $2^{256} \approx 10^{77}$ space.

Mowsie ordering pairs (mass ‖ commitment hash) inhabit $2^{512} \approx 10^{154}$ possibilities.

This is not metaphoric — it is literal.

Bitcoin: guess one atom in the universe.
Mowsie ordering: guess one atom in a universe of universes.

Mowsie does this without adding any extra randomness. It uses the entropy already inside the commitment.

8. ZK-Friendliness

Comparisons of mass and hash interpreted as big-endian integers are trivial inside SNARK and STARK circuits.

This makes MBDO practical on mobile wallets, low-power devices, recursive proof systems, and Solana verification environments.

9. Convergence Without Consensus

Because ordering is absolute, all correct sequences converge to one global state. There are no forks, no leader election, no mempool, and no replication of history.

A stateless fabric achieves blockchain-like convergence without acting like a blockchain.

10. Implementation Details

Use a ZK-native hash (Poseidon/Rescue).

Mass derived as a field-friendly scalar.
Commitment hash compared lexicographically.
No timestamps.
No block space auctions.
No fee markets.
Alpha nodes may store snapshots; ordinary wallets do not.

11. Security Analysis

11.1 Mass Soundness: Manipulating mass requires breaking the hash or regenerating the entire commitment.

11.2 Tie-breaker Soundness: Hash ordering is unmanipulable and ZK-verifiable.

11.3 Collision Safety: Even if mass collides, commitment hash ordering resolves it.

11.4 No MEV Surface: Ordering depends only on commitment structure.

11.5 Quantum-Future-Proof: Even if quantum computing weakens one hash layer, the other remains protective.

12. Relationship to Paper 1 & Paper 3

Paper 1 defined stateless operation, commitments, nullifiers, and IMIB monetary mechanics.

Paper 2 defines universal ordering, deterministic collapse mechanics, and gravitational mass ordering.

Paper 3 will define metabolic cycles, pruning, wallet lifespan, tree trimming, and the Feast of Crumbs. Together they define the physics of the Mowsie fabric.

13. Conclusion

MBDO provides a deterministic, stateless, collision-safe ordering model for zero-knowledge monetary fabrics. Mass determines how notes interact with the singularity of the global state root. Commitment hash determines how equally massive notes interact with each other. These two fields form a deterministic gravitational structure that collapses state transitions without metadata or history.

Ordering is not constructed.
It is discovered — already encoded in the cryptographic universe.