Null-State Cryptography: A Geometric Consensus Protocol via Sedenionic Trapdoors

Aaron M. Schutza

February 23, 2026

Abstract

Traditional distributed ledger technologies rely heavily on computationally expensive Proof-of-Work (PoW) hashes or capital-intensive Proof-of-Stake (PoS) mechanisms to achieve network consensus. This paper introduces the Null-State Protocol, a bare-metal, geometric consensus architecture that leverages the non-associative and non-commutative properties of the 16-dimensional Sedenion algebra. By utilizing Cayley-Dickson zero-divisors as native cryptographic trapdoors, Null-State achieves $O(1)$ validation complexity, rendering batched "blocks" obsolete. Furthermore, the protocol utilizes algebraic path-dependence as a continuous geometric accumulator, producing an unforgeable proof of chronological transaction ordering. To resolve asynchronous network latency and mitigate Sybil attacks, Null-State implements Deterministic Geometric Sorting (DGS) bound by Geometric Proof-of-Stake (G-PoS), ensuring Byzantine fault tolerance without centralized sequencers. Hardware benchmarks demonstrate that a batched tensor architecture can evaluate over 1,000,000 cryptographic states in approximately 3 milliseconds.

1 Introduction

Distributed networks require robust mechanisms to prevent Sybil attacks and ensure the integrity of a shared global state. While existing architectures guarantee security through cryptographic hash functions (e.g., SHA-256) and digital signatures (e.g., ECDSA), they suffer from scalability limitations and heavy computational overhead. Null-State Cryptography bypasses traditional algorithmic hashing by mapping network state and transaction validation directly into a 16-dimensional topological space. This provides a highly scalable, hardware-accelerated substrate for decentralized networks, entirely replacing iterative computation with single-step geometric evaluation.

2 The Sedenionic Algebra

The protocol operates within the Sedenions ($\mathbb{S}$), a 16-dimensional non-division algebra constructed via the Cayley-Dickson process from the Octonions ($\mathbb{O}$). A Sedenion S is represented as a pair of Octonions (A, B). The multiplication of two Sedenions $X = (x_a, x_b)$ and $Y = (y_a, y_b)$ is defined as:

$$X \times Y = (x_a y_a - y_b^* x_b,\ y_b x_a + x_b y_a^*) \tag{1}$$

where * denotes the conjugate. Because $\mathbb{S}$ is strictly non-associative and non-commutative, it possesses native zero-divisors—non-zero geometric elements whose product evaluates to an absolute zero vector.

3 The Sedenionic Digital Signature Algorithm (SDSA)

To function as a true standalone digital signature, the Null-State Protocol implements Payload Binding via the Sedenionic Digital Signature Algorithm (SDSA). Every network account is defined by a 16-dimensional **Public Lock Vector** (L_{pub}). To authorize a specific **Payload Vector** (P), the sender generates a one-time **Signature Vector** (S).

Because the Sedenions are strictly non-associative, the product of the Payload and the Public Lock ($P \times L_{pub}$) creates a specific geometric trajectory. The sender calculates S such that it annihilates this trajectory:

$$S \times (P \times L_{pub}) = 0 \tag{2}$$

If an attacker intercepts S and attempts to attach it to a forged payload, the strict non-associativity of the algebra ensures the intercepted signature S will fail to annihilate the forged trajectory ($\|V\| > 0$), mathematically preventing replay attacks.

4 Replacing Blocks: The Continuous State Stream

Because Null-State trapdoor validation evaluates in microseconds, the network operates as a **Continuous State Stream**. Verified raw transaction data is deterministically mapped to the unique 16D Payload Vector (P). The network maintains a shared 16D **Global State Vector** (G). Nodes update their local state via:

$$G_t = G_{t-1} \times P \tag{3}$$

Because multiplication is non-commutative, the exact sequence of transactions irreversibly alters the trajectory of G. The current 16D Global State Vector functions equivalently to a Merkle Root: a mathematical fingerprint representing the absolute chronological history of the network.

5 Canonical Ordering & Geometric Proof-of-Stake (G-PoS)

In a blockless architecture, network latency guarantees nodes will receive broadcasts in different chronological orders, causing states to diverge. Null-State resolves this via Deterministic Geometric Sorting (DGS).

If two transactions reference the exact same anchor state but arrive asynchronously, nodes establish a canonical order based on the Euclidean norm of the payload vectors: $\|P\| = \sqrt{\sum_{i=0}^{15} P_i^2}$. If $\|P_B\| > \|P_A\|$, the protocol dictates that Tx_B mathematically precedes Tx_A.

5.1 Sybil Resistance via Stake-Bounded Magnitudes

To prevent malicious actors from dominating the DGS canonical ordering by broadcasting payloads with artificially infinite magnitudes, Null-State implements a strict cryptoeconomic constraint. The maximum allowable Euclidean magnitude of a Payload Vector ($||P||$) cannot exceed the sender's verified staked token balance in the global ledger.

If a malicious node broadcasts a payload magnitude exceeding its economic stake, the transaction is instantly rejected by honest nodes prior to sorting. Consequently, an adversary would need to acquire $> 50\%$ of the entire network's token supply to consistently manipulate the chronological trajectory of the ledger.

6 Network Synchronization and Fork Resolution

At fixed intervals, nodes gossip their current Global State Vector (G). If Node A receives Node B's state (G_B), it computes the Euclidean distance. If $D > 0$, a network partition occurred. The

nodes exchange missing payloads, verify the SDSA signatures, and perform an $O(1)$ algebraic re-accumulation ($G_{resolved} = G_{anchor} \times P_B \times P_A$) to effortlessly resynchronize their states without voting mechanisms.

7 Hardware Acceleration & Conclusion

By translating the Cayley-Dickson multiplication into parallelized CUDA tensor operations, validation transcends standard CPU bottlenecks. Initial stress testing evaluated 10^6 cryptographic states in approximately 3 milliseconds on consumer GPU hardware. By merging the Sedenionic Digital Signature Algorithm with Stake-Bounded Deterministic Geometric Sorting, Null-State presents a viable, high-throughput, and energy-efficient alternative to legacy blockchain consensus mechanisms.