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, timestamp-free proof of chronological transaction ordering. To resolve asynchronous network latency, Null-State implements Deterministic Geometric Sorting (DGS) over a Directed Acyclic Graph (DAG), 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, effectively eliminating the throughput bottlenecks of algorithmic hashing.

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 ($A(BC) \neq (AB)C$) and non-commutative ($AB \neq BA$), it possesses native zero-divisors—non-zero geometric elements whose product evaluates to an absolute zero vector.

3 The Sedenionic Digital Signature Algorithm (SDSA)

In a naive geometric trapdoor ($T_{key} \times L_{pub} = 0$), the broadcasted key acts as a static password, leaving the protocol vulnerable to replay attacks. To function as a true standalone digital signature, the Null-State Protocol implements Payload Binding via the Sedenionic Digital Signature Algorithm (SDSA).

3.1 Key Generation & Payload Binding

Every network account is defined by a 16-dimensional **Public Lock Vector** (L_{pub}), geometrically derived from a hidden Private Seed (K_{priv}). To authorize a specific **Payload Vector** (P), the sender must generate a one-time **Signature Vector** (S) that mathematically ties their Private Seed to the exact payload.

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

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

3.2 Geometric Verification

The sender broadcasts the tuple: $[S, P]$. Any node in the network can verify the signature in $O(1)$ time by evaluating the trapdoor:

1. Calculate the target trajectory: $X = P \times L_{pub}$
2. Evaluate the zero-divisor: $V = S \times X$

If the magnitude $\|V\| = 0$, the signature is valid. If an attacker intercepts S and attempts to attach it to a forged payload (P_{evil}), the strict non-associativity of the algebra ensures that ($P_{evil} \times L_{pub}$) will completely alter the cross-terms of the target vector. The intercepted signature S will fail to annihilate the forged trajectory ($\|V\| > 0$), instantly exposing the forgery and mathematically preventing replay attacks.

4 Replacing Blocks and Hashes: The Continuous State Stream

Because Null-State trapdoor validation evaluates in microseconds, the concept of a batched block is obsolete. The network operates as a **Continuous State Stream**. Instead of securing timelines by placing the SHA-256 hash of Block 1 into Block 2, Null-State relies on the non-associative geometry of the Sedenions as a continuous cryptographic accumulator:

1. **Payload Mapping:** Verified raw transaction data (Sender, Receiver, Amount) is deterministically mapped to the unique 16D Payload Vector (P).
2. **Geometric Accumulation:** The network maintains a single, shared 16D **Global State Vector** (G). For each verified transaction, 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 lightweight mathematical fingerprint representing the absolute, timestamp-free chronological history of the network.

5 Canonical Ordering in a Blockless Stream

In a blockless architecture, network latency guarantees nodes will receive broadcasts in different chronological orders, causing Global State Vectors to diverge. Null-State resolves this without relying on timestamps or voting by utilizing a Geometric Directed Acyclic Graph (DAG) and Deterministic Geometric Sorting (DGS).

5.1 Geometric Anchoring

A broadcast must include a reference to the sender's locally observed Global State, termed the **Anchor State** (G_{anchor}). This creates a topological DAG where payloads are mathematically bound to the state from which they originate.

5.2 Deterministic Geometric Sorting (DGS)

If two transactions, Tx_A and Tx_B, reference the exact same G_{anchor} but arrive asynchronously, nodes establish a canonical order via a strict, protocol-wide algebraic sorting rule based on the Euclidean norm of the payload vectors:

$$\|P\| = \sqrt{\sum_{i=0}^{15} P_i^2} \tag{4}$$

If $\|P_B\| > \|P_A\|$, the protocol dictates that Tx_B mathematically precedes Tx_A. In the event of equal magnitudes, vectors are sorted lexicographically.

5.3 Algebraic Re-Accumulation

Because SDSA validation ($S \times (P \times L_{pub}) = 0$) is entirely independent of the Global State G, a node that receives transactions out of canonical order is not required to drop them. If a node processes P_A and then receives the canonically prior P_B, it performs an $O(1)$ algebraic re-accumulation:

$$G_{resolved} = G_{anchor} \times P_B \times P_A \tag{5}$$

This mathematically guarantees that all honest nodes will deterministically converge on a single, totally-ordered 16-dimensional trajectory without a centralized sequencer.

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:

$$D = \sqrt{\sum_{i=0}^{15} (G_{A,i} - G_{B,i})^2} \tag{6}$$

If $D > 0$, a network partition occurred. The nodes query each other for the missing raw transaction data payloads, verify the SDSA signatures, and replay the geometric accumulation to effortlessly resynchronize their states.

7 Hardware Acceleration & Conclusion

By translating the Cayley-Dickson multiplication into parallelized CUDA tensor operations, validation transcends standard CPU bottlenecks. Initial stress testing mapping 10^6 randomized forged keys against a target broadcast evaluated in approximately 3 milliseconds on consumer GPU hardware. The steep algebraic rejection gradient secures the Null-State Protocol natively at the hardware level. By merging the Sedenionic Digital Signature Algorithm with Deterministic Geometric Sorting, Null-State presents a viable, high-throughput, and energy-efficient alternative to legacy blockchain consensus mechanisms.