

# Statelessness Reframed: Why Partitioned, Relationship-Local State Escapes the a16z Lower Bound and How DSM Compares to INTMAX

Brandon "Cryptskii" Ramsay

October 2025

## Abstract

Christ & Bonneau (a16z Crypto) formalize an information-theoretic impossibility for “stateless blockchains”: when validators keep a succinct commitment to a *global* state, user witnesses must refresh frequently—even for inactive users—by a Shannon-style counting bound. We prove a clean separation. We define the *Partitioned, Relationship-Local State Machine* (PRLSM) model, instantiated by DSM, in which there is no succinct *global* commitment; verification and ordering occur via bilateral hash chains and device-local authenticated structures (Per-Device SMT and Device Tree). We show the a16z bound does not apply to PRLSM: witness churn for an inactive user is zero for transitions disjoint from that user’s relationships, and in general scales with the user’s touch-degree rather than global throughput. We contrast with rollup designs like INTMAX which optimize within the a16z model (bytes/tx, DA minimization) yet preserve a global commitment and thus the witness-refresh tradeoff.

## 1 Background: Revocable Witnesses & Global Succinctness

**Definition 1.1** (Global-Succinct Commitment Model (GSCM)). *A system is in GSCM if (i) there exists a global application state  $\text{State}_t$  after  $t$  transitions; (ii) validators maintain a fixed-size commitment  $\text{Root}_t = H(\text{State}_t)$  independent of  $|\text{State}_t|$ ; (iii) a user proving a fact  $f$  about  $\text{State}_t$  supplies a witness  $\text{wit}(f, \text{Root}_t)$  which validators verify against  $\text{Root}_t$ .*

**Definition 1.2** (Revocable Witness System (RWS)). *An RWS augments GSCM with a witness refresh rule: when  $\text{State}_t \rightarrow \text{State}_{t+1}$ , previously valid  $\text{wit}$  may be revoked; users must refresh to  $\text{wit}'$  consistent with  $\text{Root}_{t+1}$ . A scheme is refresh-light if the expected number of users who must refresh per transition is sublinear in the number of accounts.*

**Theorem 1.1** (Christ–Bonneau impossibility, informal). *In any RWS where validators keep a constant-sized commitment  $\text{Root}_t$  to a global state, there exists a distribution of transactions for which the expected number of users requiring witness refresh over  $T$  steps is  $\Omega(T)$ , even if many users are inactive.*

*Sketch (Shannon counting).* Alice encodes a subset  $S \subseteq [n]$  of accounts by applying transactions and broadcasting the constant-sized update  $\text{Root}_{t+1}$ . Bob, with pre-update witnesses, detects which witnesses revoked and thereby recovers  $S$ . Since there are  $2^n$  possible  $S$ , Alice would need  $\geq n$  bits to communicate  $S$ , contradicting the constant-size update unless many users’ witnesses revoke each step. (See [1] for the full argument.)  $\square$

## 2 DSM as a Partitioned, Relationship-Local State Machine

DSM does not maintain a global monolithic state. Each device  $D$  maintains: (i) a Device Tree root  $R_G$  binding device identities to genesis; (ii) a Per-Device SMT root  $r_D$  mapping each bilateral key  $(D, \overline{D})$  to the tip  $h_{D, \overline{D}}$  of a straight hash chain; (iii) stitched receipts proving inclusion under  $r_D$ ,  $r_{\overline{D}}$ , and membership in  $R_G$ , with per-step SPHINCS+ signatures. (See [5, 6] for protocol invariants and anti-cloning.)

**Definition 2.1** (PRLSM). *A system is a PRLSM if (i) the application state factors as disjoint per-relationship chains  $\{\mathcal{C}_{i,j}\}$ ; (ii) user  $i$  authenticates only  $\{\mathcal{C}_{i,j}\}_j$  under a device-local root  $r_i$ ; (iii) correctness of a transition on  $\mathcal{C}_{i,j}$  requires only inclusion proofs into  $r_i$ ,  $r_j$  and membership of  $\text{DevID}_i, \text{DevID}_j$  in  $R_G$ ; (iv) ordering is enforced by adjacency (successor commits parent) and fork-exclusion (Tripwire).*

## 3 Separation from the a16z Lower Bound

**Lemma 3.1** (Non-interference of disjoint relationships). *Let  $u$  be a user and let  $\mathcal{T}$  be any sequence of transitions that touch no chain  $\mathcal{C}_{u,*}$ . Then  $r_u$  and the proofs  $\text{wit}_u$  maintained by  $u$  remain valid across  $\mathcal{T}$ ; no refresh is required for  $u$ .*

*Proof.* Transitions on  $\mathcal{C}_{k,\ell}$  with  $k, \ell \neq u$  do not modify leaves keyed by  $(u, *)$  under  $r_u$ . Inclusion paths for  $(u, *)$  remain stable;  $R_G$  is unaffected. Hence  $\text{wit}_u$  persists across  $\mathcal{T}$  without refresh.  $\square$

**Lemma 3.2** (Locality of verification). *For a transition on  $\mathcal{C}_{u,v}$  from tip  $h$  to  $h'$ , correctness is decidable from: (i) inclusion of  $h$  under  $r_u$  and  $r_v$ ; (ii) inclusion of  $\text{DevID}_u, \text{DevID}_v$  under  $R_G$ ; (iii) a stitched receipt carrying these proofs and per-step signatures. No facts about any  $\mathcal{C}_{x,y}$  with  $\{x, y\} \cap \{u, v\} = \emptyset$  are required.*

**Theorem 3.1** (Separation). *In a PRLSM, for any inactive user  $u$  and any sequence  $\mathcal{T}$  of  $T$  transitions disjoint from  $\mathcal{C}_{u,*}$ , the number of required witness refreshes for  $u$  is 0. In general,  $u$ 's refresh work is  $O(\#\{\text{steps on } \mathcal{C}_{u,*}\})$ , independent of global  $T$ .*

*Proof.* Immediate from Lemma 3.1. Since PRLSM has no succinct global  $\text{Root}_t$ , the Shannon encoding in Theorem 1.1 never arises: there is no constant-size global update that implicitly communicates arbitrary subsets of unrelated changes to  $u$ .  $\square$

**Remark** (No contradiction). *The a16z impossibility constrains schemes with succinct global state. PRLSM removes that premise. We do not “beat” the bound; we step outside its domain while preserving safety via partitioned authenticated structures and the Tripwire invariant [5].*

## 4 Security Invariants (DSM)

**Theorem 4.1** (Pending-Online Lock). *If an accepted but unsynchronized online projection exists for  $(A, B)$ , initiating a new offline transaction for  $(A, B)$  is invalid until synchronization clears the pending item. Transactions on  $(A, C)$ ,  $C \neq B$ , proceed unaffected.*

*Sketch.* Without the lock, two successors could attempt to consume the same parent tip, violating adjacency. Modal locking preserves single-successor semantics; disjoint relationships commute. (See protocol notes in [5].)  $\square$

**Theorem 4.2** (Atomic Interlock Tripwire). *Assuming EUF-CMA for SPHINCS+ and collision resistance for  $H$ , the probability of two distinct accepted successors to the same parent tip is negligible.*

*Sketch.* Two accepted successors imply either a signature forgery or a collision in the chained commit path (hash adjacency / Merkle path). Both are assumed infeasible [5].  $\square$

## 5 INTMAX vs. DSM (Model-Theoretic)

**Definition 5.1** (Rollup Commitment Model (RCM)). *An RCM system periodically publishes a commitment  $\text{Root}_t$  to a batch of off-chain transactions/state; users later prove inclusion against  $\text{Root}_t$  for exits/bridges.*

**Proposition 5.1** (RCM  $\subset$  GSCM). *Any rollup with a single on-chain commitment per batch instantiates GSCM: validators (L1) keep  $\text{Root}_t$ ; users supply witnesses against  $\text{Root}_t$  for withdrawals/verification.*

**Corollary 5.1** (Witness refresh persists under rollups). *RCM systems inherit Theorem 1.1: unless users obtain fresh inclusion data (or rely on proof-serving/DA committees), withdrawal/interaction witnesses go stale as unrelated rollup activity proceeds.*

**Interpretation.** INTMAX optimizes within RCM/GSCM: it minimizes on-chain data (e.g.,  $\sim 4$ – $5$  bytes/tx via short nullifiers) and frames itself as a “stateless, client-driven” rollup [2, 3, 4]. That reduces byte growth and DA cost but does not remove the global-commitment premise; the information-theoretic witness churn still follows the a16z model [1]. DSM (PRLSM) eliminates the premise entirely.

## 6 Operational Consequences

**Inactive-user burden.** In GSCM/RCM, inactive users’ witnesses still change; in PRLSM, they do not.

**Offline UX.** GSCM/RCM requires online access to global commitments; PRLSM supports offline bilateral finality with later deterministic stitching.

**Economics.** GSCM/RCM couples costs to DA/aggregation; PRLSM aligns costs with storage/availability subscriptions and client-side verification.

## 7 Conclusion

We formalized a separation: a16z’s impossibility binds schemes with succinct *global* state and revocable witnesses. DSM’s PRLSM avoids any global commitment and confines verification to relationship-local proofs and receipts. Consequently, the witness-refresh lower bound does not apply. Rollups like INTMAX optimize bytes and privacy within GSCM, but remain bound by the same information-theoretic tradeoff. Partitioned state is the robust, scalable, future-proof path.

## References

- [1] M. Christ and J. Bonneau. On the impossibility of stateless blockchains. a16z crypto (Aug. 24, 2023). <https://a16zcrypto.com/posts/article/on-the-impossibility-of-stateless-blockchains/>.
- [2] INTMAX. No State, No Trace: Stateless Systems and the Future of Digital Privacy (Jan. 28, 2025). <https://intmax.io/blog/no-state-no-trace-stateless-systems-and-the-future-of-digital-privacy>.
- [3] INTMAX. INTMAX – Stateless Layer for Billions (site overview; nullifiers 4–5 bytes/tx). <https://intmax.io/>.
- [4] INTMAX. Rollup Architecture (developer docs). <https://docs.network.intmax.io/developers-hub/core-concepts/rollup-architecture>.
- [5] B. Ramsay. *Cryptographic Stateless Stitching: Sparse Merkle Trees & Bilateral Relationships — Achieving Unbreakable Network Integrity Through Mathematical Tripwires* (June 19, 2025). <https://decentralizedstatemachine.com/TripwireTheorem.pdf>.
- [6] B. Ramsay. *DBRW: Dual-Binding Random Walk for Anti-Cloning Locally/Offline* (May 14, 2025). <https://decentralizedstatemachine.com/DBRW-combined.pdf>.
- [7] *DSM: Decentralized State Machine — The Missing Trust Layer of the Internet*, IACR ePrint 2025/592 (2025). <https://eprint.iacr.org/2025/592>.