W3CR-WP-2026-01 | Division I | Distributed Consensus & Relativistic Low-Latency Systems | Published 2026/11/23

Sub-Second Simplex BFT and Contention-Aware 2D-Nonce Parallel Execution for M2M Settlement

Institutional Attribution (COPE): Web3 Capital Research - Division I Consensus Working Group

ACM Reproducibility Badges: Artifacts Available | Artifacts Functional | Results Reproduced

ABSTRACT

Autonomous machine-to-machine (M2M) settlement exposes two structural bottlenecks in classical state-machine replication: multi-slot probabilistic finality permits reorganization double-spend hazards on sub-second API delivery, while one-dimensional sequential account nonces induce catastrophic head-of-line (HoL) blocking whenever multiple concurrent sub-agents share a sovereign account. This monograph formulates a unified consensus-and-execution model under Dwork-Lynch-Stockmeyer partial synchrony for n = 3f + 1 validators. At the consensus layer, we analyze a streamlined Simplex Byzantine Fault Tolerant (BFT) pipeline with unforgeable quorum certificates that achieves single-slot deterministic finality in 250 ms with zero reorganization probability (p_reorg = 0) after Global Stabilization Time (GST). At the execution layer, we formalize Type-0x76 two-dimensional account nonces (k_lane, s_seq) across L = 32 orthogonal lanes coupled with deterministic Optimistic Concurrency Control (OCC). We prove that L-lane partitioning reduces intra-account HoL contention failure exponentially while preserving strict serializability upon hot-slot conflict fallback. Empirical evaluation on a 3.0 Ggas/slot reference testbed confirms 100% completion of 20-transaction concurrent M2M bursts within 1,004 ms.

FORMAL THEOREM - Theorem 1.1 (Single-Slot Quorum Safety & L-Lane HoL Contention Bound)

Let a replicated state machine comprise n = 3f + 1 validators communicating over authenticated point-to-point channels under partial synchrony, where at most f validators behave arbitrarily (Byzantine). Any two slot-s commit quorums Q_1, Q_2 of cardinality 2f + 1 intersect in at least (2f + 1) + (2f + 1) - (3f + 1) = f + 1 validators, guaranteeing at least one honest validator whose monotone slot-lock prevents equivocating block finalization (p_reorg = 0). Furthermore, for M concurrent sub-agents dispatching independent transactions from a single sovereign account with per-transaction stall probability p_stall in (0, 1), partitioning sequence state into L = 32 disjoint Type-0x76 (k_lane, s_seq) registers isolates any stalled sequence k to a 1/L state slice rather than collapsing whole-account throughput to zero, while deterministic OCC validation guarantees state root equivalence against canonical topological order.

FALSIFIABLE EMPIRICAL BENCHMARK METRICS

[250 ms] 1-Slot BFT Deterministic Finality - Zero-reorg quorum certificate under n = 3f + 1 partial synchrony (ChainID 88888)
[3.0 Ggas] Per-Slot Execution Gas Ceiling - Equivalent to 12.0 Ggas/s sustained conflict-free state throughput
[32] Type-0x76 Parallel 2D-Nonce Lanes - Orthogonal (nonceKey, nonceSeq) registers eliminating intra-account FIFO HoL stalls

[1,004 ms] 20/20 Concurrent M2M Tx Burst - 100% burst completion with deterministic OCC fallback on hot storage slots

PROBLEM FORMULATION & SYSTEM MODEL

Classical blockchain execution engines inherit two implicit design assumptions tailored to low-frequency human signers: multi-block probabilistic confirmation horizons and strictly linear per-account transaction serialization. When autonomous software agents execute machine-to-machine (M2M) service settlement - such as streaming compute inference or algorithmic data procurement - both assumptions break down under adversarial load.

We model the validator network over a metric communication graph [Formal Mathematical Expression] with [Formal Mathematical Expression] nodes under the Dwork-Lynch-Stockmeyer partial synchrony model. Prior to an unknown Global Stabilization Time ([Formal Mathematical Expression]), message delivery delays may be unbounded; after [Formal Mathematical Expression] , every message transmitted between honest nodes arrives within a known relativistic propagation bound [Formal Mathematical Expression] . Under Fischer-Lynch-Paterson (FLP) impossibility, no asynchronous deterministic protocol can simultaneously guarantee safety and liveness; hence safety must hold unconditionally across asynchronous partitions while sub-second liveness resumes deterministically once [Formal Mathematical Expression] .

- Probabilistic Finality Hazard: In longest-chain or multi-epoch delayed-finality ledgers where [Formal Mathematical Expression] , an adversarial caller can consume an irreversible off-chain compute response immediately upon block inclusion and subsequently orphan the settlement branch.

- One-Dimensional Nonce Collapse: In standard EVM state machines, account replay protection maps each address [Formal Mathematical Expression] to a single scalar [Formal Mathematical Expression] . If [Formal Mathematical Expression] concurrent workers sample the current scalar simultaneously, pairwise nonce collision occurs with probability [Formal Mathematical Expression] , and a single unincluded or reverted sequence [Formal Mathematical Expression] stalls every subsequent [Formal Mathematical Expression] .

FORMAL CONSTRUCTION & MATHEMATICAL PROOF

1. Streamlined Simplex BFT Pipeline: Following Chan and Pass (TCC 2023), we replace complex view-change sub-protocols with a single-phase dummy-block timeout mechanism per slot [Formal Mathematical Expression] . In slot [Formal Mathematical Expression] , designated leader [Formal Mathematical Expression] proposes [Formal Mathematical Expression] extending the highest certified parent. Honest validators cast at most one notarization vote per slot unless local timer [Formal Mathematical Expression] expires, upon which they cast a slot-nullification vote for sentinel [Formal Mathematical Expression] . By quorum intersection ([Formal Mathematical Expression]), it is algebraically impossible for both [Formal Mathematical Expression] and a finalized block [Formal Mathematical Expression] , or two distinct blocks [Formal Mathematical Expression] , to simultaneously gather [Formal Mathematical Expression] threshold signatures.

2. Type-0x76 Two-Dimensional Nonce State Space: Each envelope bearing EIP-2718 transaction type 0x76 carries tuple (nonceKey, nonceSeq) where [Formal Mathematical Expression] ([Formal Mathematical Expression] active concurrent lanes) and [Formal Mathematical Expression] . State validity requires [Formal Mathematical Expression] and atomically increments only lane [Formal Mathematical Expression] . Because read/write locations for distinct lanes occupy disjoint trie slots, concurrent sub-agents assigned to distinct lanes never contend on sender replay metadata.

3. Deterministic OCC Conflict Serializability: Following Kung and Robinson (TODS 1981), the block executor partitions a candidate batch into parallel worker threads, recording per-transaction read sets [Formal Mathematical Expression] and write sets [Formal Mathematical Expression] . Transaction [Formal Mathematical Expression] ([Formal Mathematical Expression]) commits directly if and only if [Formal Mathematical Expression] . Whenever a hot storage slot triggers a non-empty intersection, only the conflicting subset is deterministically re-executed in canonical index order, guaranteeing exact bit-for-bit state-root agreement across all honest validators.

EMPIRICAL EVALUATION & REFERENCE IMPLEMENTATION VERIFICATION

To falsify or corroborate the analytical bounds of Theorem 1.1, we evaluated an open-source clean-room reference testbed configured as a 4-validator Simplex BFT cluster (ChainID 88888 , tolerating [Formal Mathematical Expression] fault among [Formal Mathematical Expression] nodes across dual regional routing domains) with a per-slot execution ceiling of 3.0 Ggas .

- Sub-Second Slot Cadence: Across steady-state operation after [Formal Mathematical Expression] , single-slot quorum certificates finalized consistently at the configured 250 ms slot boundary, yielding an effective conflict-free ceiling of 12.0 Ggas/s with zero observed chain reorganizations.

- 20-Transaction Concurrent Burst Benchmark: Using 32 disjoint Type- 0x76 2D-Nonce lanes dispatched simultaneously from a single smart account, 20/20 concurrent M2M settlement transactions achieved full finality in 1,004 ms end-to-end, whereas an identical uncoordinated 1D-nonce workload suffered immediate mempool sequence rejection on 19 of 20 envelopes.

- Hot-Slot Graceful Degradation: Under synthetic 100% write-set contention against a single shared counter slot, the OCC validator detected every read-after-write hazard and deterministically serialized re-execution with zero state divergence across all four validators.

- Ingress AST Hardening: At the RPC ingress boundary, structural JSON-RPC AST canonicalization capped batch cardinality at 10 and neutralized Unicode-escaped namespace bypass attempts before mempool admission.

VERIFICATION PROVENANCE & COMPETING INTERESTS DISCLOSURE

COPE & ACM Verification Provenance Statement: In accordance with the Web3 Capital Research Authorship and Scientific Integrity Charter, no fictional individual names or synthetic academic titles are attributed to this monograph. Problem formulation, partial-synchrony assumptions, and empirical thresholds were established under Principal Investigator oversight and verified by the Division I Consensus Working Group using deterministic Node.js conformance harnesses and browser-executable WebCrypto capsules (capsuleType: "nonce-2d").

Competing Interests & Reference Implementation Disclosure: Web3 Capital Research operates in the Republic of Singapore (https://research.web3.capital/) strictly as an independent, open-access, non-advisory, zero-fundraising scientific research institute within Singapore SFA 2001, FAA 2001, and PSA 2019 safe-harbor boundaries. Empirical measurements labeled BENCHMARKED_TESTBED were reproduced against the open-source reference implementation engineered by MYRILUM LIMITED (Hong Kong UBI 80912065 ; https://myrilum.org/research and https://myrilum.io/) on testbed ChainID 88888 using non-transferable synthetic state-machine units (S_token === 0 , r_holder === 0). All conformance vectors are published under royalty-free open licenses so any independent consensus client can reproduce or challenge these measurements.

VERIFIED REFERENCES

[DLS88] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer (1988). "Consensus in the Presence of Partial Synchrony." Journal of the ACM (JACM), Vol. 35, No. 2, pp. 288 - 323. https://doi.org/10.1145/42282.42283

[CL99] Miguel Castro and Barbara Liskov (1999). "Practical Byzantine Fault Tolerance." Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI '99), USENIX, pp. 173 - 186. https://pmg.csail.mit.edu/papers/osdi99.pdf

[FLP85] Michael J. Fischer, Nancy A. Lynch, and Michael S. Paterson (1985). "Impossibility of Distributed Consensus with One Faulty Process." Journal of the ACM (JACM), Vol. 32, No. 2, pp. 374 - 382. https://doi.org/10.1145/3149.214121

[CP23] Benjamin Y. Chan and Rafael Pass (2023). "Simplex Consensus: A Simple and Fast Consensus Protocol." Theory of Cryptography Conference (TCC 2023), LNCS Vol. 14372, pp. 452 - 479 (IACR ePrint 2023/463). https://eprint.iacr.org/2023/463

[KR81] H. T. Kung and John T. Robinson (1981). "On Optimistic Methods for Concurrency Control." ACM Transactions on Database Systems (TODS), Vol. 6, No. 2, pp. 213 - 226. https://doi.org/10.1145/319566.319567

[EIP4337] Vitalik Buterin, Yoav Weiss, Kristof Gazso, Namra Patel, Dror Tirosh, Shahaf Nacson, and Tjaden Hess (2021). "ERC-4337: Account Abstraction Using Alt Mempool." Ethereum Improvement Proposals. https://eips.ethereum.org/EIPS/eip-4337