Ephemeral Quorum Subnets and Quorum Attestation: A First-Class Primitive for Resolving the Blockchain Scalability Trilemma

Irina Guberman

Keyboard Expressions LLC · irina.guberman@gmail.com · May 5, 2026

Associated project: April Gate (aprilgatehq.com)

ABSTRACT

The blockchain scalability trilemma — the claim that no distributed ledger can simultaneously achieve decentralization, security, and scalability — is not a law of nature. It is a consequence of a single architectural assumption: that consensus, witnessing, and settlement must occur at the same protocol layer. We introduce the *Ephemeral Quorum Subnet* (EQS) as the primitive that dissolves this assumption. An EQS is a temporary, task-scoped group of L1-registered participants that self-organizes around a specific witnessing task, coordinates internally using any protocol suited to the task, produces a single compact cryptographic artifact — a *Quorum Attestation* (QA) — posts it to a base-layer chain, and dissolves. The L1 verifies the QA and settles incentives. It never observes the subnet's internal deliberation. Participants are indistinguishable from ordinary L1 nodes; subnet membership is a layered concern invisible to the rest of the network. We formalize the primitive, analyze its security properties, and demonstrate its generality across four instantiations spanning pharmaceutical compliance, medical AI, scientific computation, and financial regulation.

1. The Problem

The trilemma holds for any single protocol layer asked to simultaneously provide decentralization (many independent validators), security (attack resistance), and scalability (high throughput). Increasing validator count increases decentralization but reduces throughput. Reducing validation requirements increases throughput but weakens security. The tension is real — but only within a single layer.

The insight this paper develops is simple: *most conditions that participants need to attest to do not require global ordering or global visibility.* A sensor cluster verifying pharmaceutical

compliance, a group of hospitals training a shared AI model, a subnet of exchange nodes auditing an algorithm — none of these need every L1 validator to observe each internal step. What the broader network needs is a compact, verifiable proof that the condition was genuinely witnessed by a sufficient quorum of registered, independently-incentivized participants. The rest is a subnet concern.

2. Prior Art and Its Shared Flaw

Every major scaling approach shares one structural assumption: computation must remain visible at the base layer, at least in principle.

- **Sharding** partitions state across validator subsets, increasing parallelism but dividing the validator set and weakening per-shard security. Cross-shard communication introduces new failure modes.
- **Rollups** move execution off-chain but keep a sequencer on the critical path. Optimistic rollups introduce fraud-proof windows. ZK rollups are promising but currently centralized at the prover level and difficult to generalize.
- **Persistent subnet models** (Avalanche, Polkadot, Cosmos, Filecoin IPC) support customizable sub-chains with swappable consensus. But they treat subnets as permanent sovereign chains requiring their own validator sets, token economics, and ongoing governance. The bootstrapping overhead is prohibitive for task-scoped witnessing. Persistence is the wrong default.

None of these approaches asks the more fundamental question: *does the witnessing need to happen on a persistent chain at all?* The answer, for most real-world tasks, is no.

3. The Ephemeral Quorum Subnet Primitive

3.1 Definition

An *Ephemeral Quorum Subnet* (EQS) is a tuple (P, W, C, QA, L1) where:

P — a set of participants whose identities are anchored to L1, whether through stake, hardware attestation, or any other L1-registered credential. From L1's perspective, participants in P are ordinary nodes.

W — a bounded witnessing task with a well-defined condition and completion criterion. The condition may be physical, computational, financial, or protocol-level.

C — an internal coordination protocol chosen by the subnet to fit W. L1 imposes no constraints on C.

QA — a Quorum Attestation: a succinct cryptographic artifact proving that W was witnessed correctly by a sufficient quorum of P. The QA is the only artifact that crosses the subnet boundary.

L1 — the base-layer chain that verifies the QA and settles incentives. L1 never observes C or the individual observations of participants in P.

3.2 The Internet Analogy

The internet did not scale by making IP smarter. It scaled by keeping IP minimal — just move packets — and letting heterogeneous protocols flourish above it. HTTP, SMTP, SSH, and video streaming all speak different languages that IP never needs to understand.

Blockchain has tried to do the opposite: build one layer that does everything. That is precisely why the trilemma exists. The EQS model applies the IP lesson to consensus: L1 does three things only — register identities, verify QAs, settle incentives. Subnets do everything else, each speaking whatever internal protocol its task requires. The trilemma dissolves not by clever engineering tradeoffs but by refusing to conflate concerns that were never meant to be conflated.

3.3 Five Key Properties

- **Transparent to L1.** Subnet participants are ordinary L1 nodes. They hold the same stake, follow the same rules, and appear identical to non-subnet nodes from the chain's perspective. Subnet membership is an additional concern layered on top of normal participation — not a change in L1 status. Decentralization at L1 is fully preserved.
- **Internally sovereign.** The subnet chooses its own coordination protocol C. A temperature sensor mesh uses lightweight BFT suited to embedded hardware. A hospital federated learning subnet uses gradient aggregation. A financial audit subnet uses threshold signatures. L1 does not constrain or observe C.
- **Incentive-decoupled.** Participants' stake, rewards, and slashing conditions are defined entirely at L1. The subnet produces no tokens, no governance, no side effects visible to L1 except the QA. A node can simultaneously serve as an ordinary L1 validator and participate in multiple subnets without conflict.
- **Single-artifact settlement.** The QA is the only thing that crosses the subnet boundary. Not checkpoints, not intermediate state, not individual votes — one proof. L1 state grows with the number of completed tasks, not their internal complexity.
- **Ephemeral by design.** The subnet exists for exactly the duration of W. No persistent state, no ongoing governance, no long-term validator commitment. Upon QA submission the subnet dissolves. This is not a limitation — it is the architecture.

4. Quorum Attestation

The QA encodes one claim: *a sufficient quorum of L1-registered, independently-incentivized participants witnessed condition W and agreed on the result.* Its security rests on two orthogonal trust roots:

- **Economic trust root.** Participants have stake at risk on L1. Attesting falsely means forfeiting that stake. Collusion requires corrupting a supermajority by stake — and all colluders must be willing to sacrifice it.
- **Physical trust root.** Where hardware attestation is used (e.g., tamper-resistant cryptographic elements such as the ATECC608A), the private key never leaves the chip. Device identity is physically unforgeable. An attacker must compromise both the economic incentive structure and the physical hardware simultaneously.

The quorum is not evidence of the attestation — **the quorum is the attestation.** If enough independently-anchored participants agree, that agreement is the cryptographic and economic guarantee. The ZK proof or aggregate BLS signature encoding the QA is the compact representation of that agreement for L1 consumption — not the source of the trust.

Current cryptographic tools suitable for QA encoding include Groth16 on BN254 (≈128 bytes, O(1) verification, native support on EVM and Solana), BLS aggregate signatures for public-condition witnessing, and PLONK for tasks requiring flexible circuit structure. The proof system is a subnet design parameter. L1 needs only a standard verification interface.

5. Subnet Lifecycle

- **Form.** Participants whose identities are L1-anchored advertise availability. A formation protocol selects a set P satisfying the task's requirements. Each participant posts collateral to L1.
- **Witness.** Participants observe the condition W using internal protocol C. This phase is entirely invisible to L1. No transactions, no state changes, no coordination from the chain.
- **Attest.** The subnet generates a QA encoding the result. The format depends on the task: a ZK proof for private conditions, a BLS aggregate signature for public ones.
- **Post.** The QA is submitted to L1 as a single transaction. L1 verifies it — constant time regardless of task complexity — and records the result. Rewards are distributed.
- **Dissolve.** The subnet releases connections, participants reclaim collateral plus rewards, and return to the available pool. No persistent state remains outside the QA record on L1.

A gap in the on-chain QA sequence is not a system failure — it is a tamper signal. April Gate is designed so that the absence of proof is itself evidence. Continuous QA = integrity intact. Proof gap = investigate immediately.

6. Security Analysis

6.1 Byzantine Fault Tolerance

Internal subnet BFT is parameterized by the choice of C. For synchronous protocols, safety and liveness are guaranteed when fewer than one-third of nodes are Byzantine. The subnet only

needs to tolerate adversarial behavior consistent with the task's risk profile and the collateral staked. High-value tasks recruit more nodes and require higher collateral.

6.2 Admission and Sybil Resistance

Registration of a device pubkey on L1 is necessary but not sufficient for admission. Hardware-attested devices must pass a formation challenge — a fresh signature over a recent chain state value — proving physical liveness. Software-simulated keys can respond; cloned hardware cannot respond simultaneously at scale. This rate-limits DDOS attacks to the physical signing capacity of real hardware.

For high-value public subnets, formation additionally requires participants from multiple independent staked operators, raising the cost of subnet capture beyond hardware alone. This is an open design parameter, not a fundamental limitation.

6.3 Parent Chain Independence

Subnet failures cannot compromise L1 security. An invalid QA is rejected by the verification function. A failed subnet produces no QA — the task simply does not complete and collateral is distributed per pre-agreed rules. The L1 validator set is never divided or weakened by subnet activity.

7. Four Instantiations

7.1 Pharmaceutical Cold Chain (April Gate)

Hardware-attested sensor nodes (ATECC608A + DS18B20) form an EQS during a pharmaceutical shipment. They reach local consensus on temperature readings using signed majority vote over short-range wireless links, operating entirely without internet connectivity. Upon reconnection, a ZK proof is generated proving all readings remained within compliance bounds [T_min, T_max] throughout the shipment. The QA is posted to an L1 blockchain. Insurers and regulators query only the compliance verdict. Raw sensor readings never touch the chain. A gap in the proof sequence is itself an auditable tamper signal.

7.2 Federated Medical AI Training

A consortium of hospitals needs to train a shared diagnostic model without any hospital exposing patient data to others or to a central server. An EQS forms across participating hospitals, each running gradient computation locally. Internal protocol: privacy-preserving federated averaging. The QA proves the model converged correctly over the distributed dataset without revealing any individual hospital's contribution. Regulators get cryptographic proof of compliant training. Patients' data never leaves the institution.

7.3 Distributed Scientific Computation

A research institution submits a protein folding or climate simulation job to a public EQS network. Volunteer compute nodes form an ephemeral subnet, partition the computation, and collectively produce a QA proving the simulation was executed correctly over the committed input dataset. The result is permanently recorded on L1, providing cryptographic provenance for the scientific finding — without requiring trust in any central institution or infrastructure. This is what distributed scientific computing should have been.

7.4 Algorithmic Trading Audit

A financial regulator requires proof that a trading algorithm did not engage in wash trading or front-running during a session. An EQS of exchange nodes witnesses the order flow and produces a ZK QA proving behavioral compliance without revealing the proprietary trading strategy. The regulator receives a mathematically binding audit result. The trader retains IP. No trusted third-party auditor required.

8. Open Problems

- **Subnet formation protocol.** Stake-weighted random selection via VRFs is the most promising approach but formal security analysis under adversarial formation conditions remains an open problem.
- **Recursive proofs for long sequential tasks.** Tasks with deep sequential dependencies require recursive proof systems (Nova, Supernova) to remain succinct. Application to large training runs is an active research area.
- **Cross-chain QA standards.** For the interoperability use case, multiple L1 chains must recognize the same QA format. This is as much a coordination problem as a technical one.
- **Hardware anchor limits.** Hardware attestation reduces but does not eliminate Sybil attack surface. High-value public subnets require additional formation constraints. The right combination of hardware anchoring and economic collateral for different risk profiles is an open design question.

9. Conclusion

The blockchain scalability trilemma was never a law of nature. It was an assumption — that consensus, witnessing, and settlement must share one layer. When that assumption is removed, all three properties become independently achievable: L1 provides decentralization and security at minimal throughput cost; subnets provide scalability and task-specific efficiency; the QA is the only artifact that crosses the boundary between them.

The internet did not scale by making IP smarter. Blockchain will scale the same way — not by making L1 do more, but by giving it less to do. The EQS primitive is the mechanism that makes this separation concrete, implementable, and secure. April Gate is its first production instantiation. The general architecture is the contribution this paper offers to the field.

References

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org/bitcoin.pdf

[2] Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.

[3] Groth, J. (2016). On the size of pairing-based non-interactive arguments. EUROCRYPT 2016. IACR ePrint 2016/260.

[4] Boneh, D., Lynn, B., Shacham, H. (2001). Short Signatures from the Weil Pairing. ASIACRYPT 2001.

[5] Castro, M. and Liskov, B. (1999). Practical Byzantine Fault Tolerance. OSDI 1999.