Scaling Solana's Consensus with VRF-Based Subcommittees and BLS Aggregation

X1 Research Team

March 8, 2025

1 Introduction

Solana's Tower BFT consensus protocol is optimized for low-latency, high-throughput execution, but faces scalability challenges as the set of validators expands. The current design requires that each validator independently sign and transmit votes, leading to increasing network congestion and signature verification overhead as validator participation grows. In its current form, the system does not scale linearly as the computational and bandwidth requirements increase proportionally.

To address these challenges, we propose a Verifiable Random Function (VRF) based subcommittee selection mechanism combined with geographic and performance aware aggregation relays. This approach reduces voting frequency by a factor of 1/100 or 1/1000, ensuring that consensus remains efficient while maintaining decentralization and security. Instead of all validators transmitting votes in every round, subcommittees are dynamically formed based on stake-weighted selection, liveness, performance metrics, latency, block skip rates, and delegation from well-known addresses.

2 Problem Statement: Signature and Bandwidth Overhead in an Expanding Validator Set

Solana's fast block times (400ms slots) require validators to propagate votes rapidly to ensure the block finality. Each validator submits an Ed25519 signature for every vote, which must be individually verified by the leader and forwrded by other validators. As the validator count grows, the network faces quadratic overhead in both network bandwidth and computational verification costs.

The primary scalability constraints include:

- **Network Congestion**: Every validator independently broadcasting votes leads to exponential growth in the number of messages propagated. At

1,000,000 validators, the unoptimized model results in prohibitive bandwidth usage.

- **Signature Verification Bottleneck**: The leader is required to verify thousands or millions of signatures per round. Since Ed25519 signature verification is computationally expensive, excessive validation overhead could compromise block finalization speed.
- **Geographic Latency Variability**: Validators are distributed globally, leading to non-uniform message arrival times and delayed vote aggregation in worst-case scenarios.

These constraints necessitate a mechanism that both reduces the number of votes processed per slot and ensures optimal relay selection for efficient vote aggregation.

3 VRF-Based Subcommittee Selection for Vote Reduction

To reduce the volume of votes processed without compromising security, a VRF-based subcommittee election process is introduced. The VRF generates a pseudo-random selection of validators, ensuring fairness and unpredictability while allowing the protocol to dynamically adjust voting participation.

The VRF selection mechanism is stake-weighted, but incorporates additional scores that factor in the reliability and efficiency of the validator. The selection probability P_i for the validator i is computed as:

$$P_i = \frac{S_i}{\sum S_j} \cdot F \cdot A_i \tag{1}$$

where:

- S_i is the validator's stake weight
- F is the global vote reduction factor (e.g., 1/100 or 1/1000)
- A_i is an adjustment coefficient based on performance metrics, computed as:

$$A_i = \frac{L_i + R_i}{2} \times (1 - K_i) \times (1 + D_i) \tag{2}$$

where:

- L_i is the liveness score (uptime, missed votes, block proposal success rate)
- R_i is the performance score (latency, compute efficiency)
- K_i is the block skip penalty (penalizing validators with excessive skipped blocks)

- D_i is a delegation bonus (favoring validators with delegation from high-reputation wallets)

Validators with higher stakes and strong historical performance have a higher likelihood of selection but are not guaranteed selection, ensuring fairness and randomness.

4 BLS Signature Aggregation for Efficient Vote Compression

BLS (Boneh–Lynn–Shacham) signature aggregation is used to merge multiple validator votes into a single signature, significantly reducing both transmission size and verification costs.

Each validator in a subcommittee generates a BLS signature σ_i on the vote message M:

$$\sigma_i = H(M)^{sk_i} \tag{3}$$

where sk_i is the validator's secret key, and $H(M)$ is the hash of the vote message.

The relay node aggregates all signatures within the subcommittee:

$$\sigma_{agg} = \prod \sigma_i \tag{4}$$

which is then submitted to the leader. The leader verifies the aggregated signature in constant time using:

$$e(\sigma_{agg}, g) = e(H(M), \sum pk_i) \tag{5}$$

where pk_i are the public keys of the participating validators. Instead of verifying n individual Ed25519 signatures, the leader verifies a single BLS signature per subcommittee, reducing signature verification complexity from $O(n)$ to $O(1)$.

5 Conclusion and Future Work

A VRF-based subcommittee election combined with stake-weighted performance selection and BLS aggregation provides a scalable mechanism for Solana's consensus. This approach enables support for millions of validators while maintaining high performance and decentralization.

Future optimizations could explore:

- Adaptive vote frequency scaling based on network congestion levels.
- Optimized relay selection using machine learning models for real-time latency prediction.

- Hardware acceleration for BLS verification to further reduce computational overhead.

By implementing this approach, Solana can future-proof its consensus model, ensuring it remains the most performant, decentralized blockchain capable of sustaining high validator participation at scale.