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 Comparison of Randomness Models in Consensus

Different blockchains use different approaches for randomness in validator or block proposer selection. The primary methods are:

2.1 Ethereum's Use of RANDAO

Ethereum's consensus layer (Casper FFG and Gasper) does not use VRFs but instead relies on **RANDAO**, a commit-reveal randomness scheme. In this approach:

- Each validator contributes to a shared randomness pool by submitting their own entropy.

- The randomness output is derived from the combined validator contributions.
- The scheme is vulnerable to **biasing attacks**, where adversaries can selectively reveal or withhold their entropy to influence results.

To mitigate biasing, Ethereum plans to introduce **Verifiable Delay Functions (VDFs)**, which enforce an irreversible computation delay before finalizing the randomness.

2.2 Filecoin's Use of VRF

Filecoin employs **Verifiable Random Functions (VRFs)** for leader election:

- Each miner generates a VRF proof to determine whether they are eligible to propose a block.
- The VRF output is unpredictable and cryptographically verifiable.
- Unlike RANDAO, VRF results are independently generated per participant, reducing opportunities for manipulation.

2.3 Cardano's Use of VRF in Ouroboros

Cardano's **Ouroboros** protocol also uses VRF for leader election, but in a stake-weighted manner:

- Each epoch is divided into slots, and slot leaders are chosen using a VRF.
- A validator (stake pool) runs a VRF function to determine if it has been selected as the slot leader.
- The probability of selection is proportional to the validator's stake, ensuring that larger stake pools have a higher chance of producing blocks.

Ouroboros differs from Filecoin's VRF in that it combines randomness with stake-weighting, making it more similar to how Solana selects validators in Proof-of-Stake.

2.4 Applying VRF to Solana

Given Solana's high-performance design, a hybrid approach leveraging **VRF-based subcommittee selection** (inspired by Filecoin and Cardano) along with **BLS aggregation** (used in Ethereum) could optimize consensus scalability.

3 VRF-Based Subcommittee Selection for Vote Reduction

A VRF-based subcommittee election process is introduced to reduce the volume of votes processed without compromising security. 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:

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

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
- D_i is a delegation bonus favoring well-reputed validators.

Unlike Ethereum's RANDAO, which relies on collective randomness, Solana's approach could leverage VRFs for subcommittee selection, ensuring validators are chosen independently without central coordination.

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.

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 real-time network latency prediction.
- Hardware acceleration for BLS verification to further reduce computational overhead.
- Further refinement of VRF-based selection based on Filecoin's and Cardano's implementation.
- Exploration of hybrid VRF + RANDAO models for unbiased randomness generation.

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.