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

X1 Research Team

March 11, 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. 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. This VRF-based approach ensures unbiased randomness while maintaining decentralization and security.

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 Subcommittee Assignment

Ethereum's consensus layer (Casper FFG and Gasper) assigns validators to attestation subcommittees based on a pre-determined randomness source:

- The beacon chain uses an epoch-based randomness source to shuffle active validators.
- Validators are assigned to attestation committees per slot in a fair and decentralized manner.

- The randomness ensures unbiased committee formation while preventing validator collusion.

2.2 Filecoin's Use of VRF

Filecoin utilizes VRFs for leader election in its consensus mechanism:

- Each miner runs a VRF function to determine whether they are eligible to propose a block.
- The probability of selection is proportional to the miner's storage power.
- The VRF ensures that leader selection is cryptographically fair and unpredictable.

2.3 Cardano's Ouroboros and VRF

Cardano's Ouroboros consensus employs VRF-based leader election in a stake-weighted manner:

- Each epoch is divided into slots, and stake pools determine their eligibility to produce blocks using VRFs.
- The VRF output provides a provable, unbiased random draw, reducing manipulation risks.
- The probability of selection increases with stake delegation, promoting decentralized security.

2.4 Solana's Proposed VRF-Based Subcommittee Assignment

Solana can adopt a similar committee assignment strategy using Verifiable Random Functions (VRFs) to ensure fairness. Instead of using epoch-based randomness, Solana can:

- Use a VRF output to assign validators to subcommittees dynamically.
- Ensure randomness is unbiased by incorporating stake weighting into the selection process.
- Prevent validator predictability by ensuring committee assignments change periodically.

This model ensures that no single validator can manipulate committee assignments while maintaining Solana's high-performance constraints.

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:

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

where:

- S_i is the validator's stake weight
- 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.

3.1 VRF-Based Subcommittee Assignment

The VRF ensures unbiased randomness in validator subcommittee assignments. Each validator generates a VRF proof using their private key and a block-specific seed:

$$VRF_{output} = VRF_{sign}(sk_i, H(block_{seed})) \tag{3}$$

The output is then mapped to a subcommittee index:

$$Subcommittee_i = (H(VRF_{output}, S_i) \mod N) \tag{4}$$

where S_i is the validator's stake weight, and N is the total number of subcommittees. The function H represents a cryptographic hash function, ensuring deterministic yet unpredictable mapping of VRF outputs and stake weights to subcommittee assignments. This guarantees fairness and prevents manipulation of committee selection.

By incorporating stake weighting, the probability of a validator being assigned to a subcommittee is adjusted based on their performance score and stake:

$$P(assignment) = \frac{S_i \cdot A_i}{\sum S_j \cdot A_j} \tag{5}$$

This ensures that validators with higher stake and better performance metrics have a greater likelihood of participating in consensus while maintaining fairness.

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:

$$\sigma_i = H(M)^{sk_i} \tag{6}$$

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:

$$\sigma_{agg} = \prod \sigma_i \tag{7}$$

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

$$e(\sigma_{agg}, g) = e(H(M), \sum pk_i) \tag{8}$$

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 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.

- Further refinement of VRF-based selection based on Ethereum's attestation subcommittee approach.
- Exploration of hybrid models to improve randomness distribution efficiency.

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.