TL;DR

We introduce a novel triadic consensus mechanism that achieves fast and resilient agreement on transaction ordering and state updates within shards, with $O(n \log_3 n)$

message complexity and $O(\log_3 n)$

time complexity.

Background

Traditional consensus protocols like PBFT suffer from high communication overhead, requiring $O(n^2)$

message complexity for n

validators. This limits scalability and performance in sharded blockchain architectures. There is a need for a more efficient and resilient consensus mechanism that can scale to large networks while maintaining security guarantees.

Proposal

Triadic consensus organizes validator nodes within each shard into a fractal data structure based on the Sierpinski triangle. Nodes are grouped into recursive “triads” of three nodes each. Consensus is reached by propagating votes across these triads in a recursive manner. Each node independently validates transactions and broadcasts votes to its triad peers. Votes are aggregated at each triad level, with the majority outcome determining the triad vote. If a triad commits a transaction, the vote is propagated to the parent triad at the level above. This process continues recursively until either a triad rejects the transaction or the root triad is reached, indicating global consensus.

Let $v_{i,j} \in {0,1}$

denote the vote of node j

in triad τ_i

, and let $V_{\tau_i} \in {0,1}$

denote the aggregated triad-level vote for τ_i

, defined as:

$$V_{\tau_i} = \begin{cases} 1 & \text{if } \sum_{j=1}^3 v_{i,j} \geq 2 \ 0 & \text{otherwise} \end{cases}$$

The overall shard-level consensus outcome V_{shard}

for transaction tx

is determined as:

$$V_{\text{shard}}(tx) = \prod_{i=0}^r V_{\tau_i}$$

where $r = \log_3 n$

is the height of the fractal topology for a shard with n

nodes.

Advantages

Triadic consensus offers several advantages over traditional consensus protocols:

1. Reduced message complexity: With $O(n \log_3 n)$

message complexity, triadic consensus significantly reduces communication overhead compared to $O(n^2)$

in PBFT.

1. Fast convergence: The recursive vote propagation allows the shard to reach a $2/3$

supermajority consensus on each transaction with minimal rounds of communication, achieving $O(\log_3 n)$

time complexity.

1. Byzantine fault tolerance: Triadic consensus ensures agreement on all valid transactions with up to $f < n/3$

Byzantine nodes, maintaining the same security threshold as PBFT.

Triadic consensus ensures agreement on all valid transactions with up to $f < n/3$

Byzantine nodes.

Consider a triad τ_i

with an honest supermajority (≥ 2

out of 3

nodes). If tx

is valid, then at least 2

nodes will broadcast $v_{i,j} = 1$

, and thus $V_{\tau_i} = 1$

. Conversely, if tx

is invalid, then at least 2

nodes will broadcast $v_{i,j} = 0$

, and thus $V_{\tau_i} = 0$

.

Since at most f

nodes are Byzantine, and each triad requires ≥ 2

matching votes to commit, a Byzantine node can only stall consensus if paired with ≥ 1

other Byzantine node in a triad. With $f < n/3$

, Byzantine nodes can comprise at most 1

node in each triad. Thus every honest supermajority triad will reach agreement, and every mixed triad (1

Byzantine node) will either agree with the honest nodes or deadlock. Any deadlocked triads will be eventually resolved by honest majority triads in subsequent rounds.

Applications

Triadic consensus can be applied in sharded blockchain architectures to enable fast and secure consensus within each shard. It is particularly well-suited for high-throughput applications that require low latency and scalability, such as decentralized finance (DeFi), supply chain management, and Internet of Things (IoT) networks. By organizing validators into a fractal topology and propagating votes efficiently, triadic consensus allows shards to process transactions in parallel while maintaining global consistency.

Conclusion

The triadic consensus mechanism introduced represents a significant advancement in consensus protocols for sharded blockchains. By achieving $O(n \log_3 n)$

message complexity and $O(\log_3 n)$

time complexity, it enables fast and resilient agreement on transaction ordering and state updates within shards. This scalable and efficient consensus mechanism has the potential to unlock new possibilities for high-performance decentralized applications and pave the way for more robust and scalable blockchain networks.