Synchronization

Fast, reliable synchronization is the biggest reason Solana is able to achieve such high throughput. Traditional blockchains synchronize on large chunks of transactions called blocks. By synchronizing on blocks, a transaction cannot be processed until a duration, called "block time", has passed. In Proof of Work consensus, these block times need to be very large(~10 minutes)to minimize the odds of multiple validators producing a new valid block at the same time. There's no such constraint in Proof of Stake consensus, but without reliable timestamps, a validator cannot determine the order of incoming blocks. The popular workaround is to tag each block with awallclock timestamp . Because of clock drift and variance in network latencies, the timestamp is only accurate within an hour or two. To workaround the workaround, these systems lengthen block times to provide reasonable certainty that the median timestamp on each block is always increasing.

Solana takes a very different approach, which it callsProof of History orPoH . Leader nodes "timestamp" blocks with cryptographic proofs that some duration of time has passed since the last proof. All data hashed into the proof most certainly have occurred before the proof was generated. The node then shares the new block with validator nodes, which are able to verify those proofs. The blocks can arrive at validators in any order or even could be replayed years later. With such reliable synchronization guarantees, Solana is able to break blocks into smaller batches of transactions calledentries . Entries are streamed to validators in realtime, before any notion of block consensus.

Solana technically never sends ablock , but uses the term to describe the sequence of entries that validators vote on to achieveconfirmation . In that way, Solana's confirmation times can be compared apples to apples to block-based systems. The current implementation sets block time to 800ms.

What's happening under the hood is that entries are streamed to validators as quickly as a leader node can batch a set of valid transactions into an entry. Validators process those entries long before it is time to vote on their validity. By processing the transactions optimistically, there is effectively no delay between the time the last entry is received and the time when the node can vote. In the event consensus isnot achieved, a node simply rolls back its state. This optimistic processing technique was introduced in 1981 and calledOptimistic Concurrency Control . It can be applied to blockchain architecture where a cluster votes on a hash that represents the full ledger up to someblock height . In Solana, it is implemented trivially using the last entry's PoH hash.

Relationship to VDFs

The Proof of History technique was first described for use in blockchain by Solana in November of 2017. In June of the following year, a similar technique was described at Stanford and called averifiable delay function orVDF .

A desirable property of a VDF is that verification time is very fast. Solana's approach to verifying its delay function is proportional to the time it took to create it. Split over a 4000 core GPU, it is sufficiently fast for Solana's needs, but if you asked the authors of the paper cited above, they might tell you(and have)that Solana's approach is algorithmically slow and it shouldn't be called a VDF. We argue the term VDF should represent the category of verifiable delay functions and not just the subset with certain performance characteristics. Until that's resolved, Solana will likely continue using the term PoH for its application-specific VDF.

Another difference between PoH and VDFs is that a VDF is used only for tracking duration. PoH's hash chain, on the other hand, includes hashes of any data the application observed. That data is a double-edged sword. On one side, the data "proves history" - that the data most certainly existed before hashes after it. On the other side, it means the application can manipulate the hash chain by changingwhen the data is hashed. The PoH chain therefore does not serve as a good source of randomness whereas a VDF without that data could. Solana'sleader rotation algorithm , for example, is derived only from the VDFheight and not its hash at that height.

Relationship to Consensus Mechanisms

Proof of History is not a consensus mechanism, but it is used to improve the performance of Solana's Proof of Stake consensus. It is also used to improve the performance of the data plane protocols.

More on Proof of History

- water clock analogy
- Proof of History overview Previous Stake Delegation and Rewards Next Turbine Block Propagation