Web3 Solana Blockchain - 07

ALBUS SECURITY

Proof Of History

Consensus Protocol

A consensus protocol is a set of rules and procedures that govern how participants in a distributed network agree on the validity and ordering of transactions or changes to the network's state. It ensures that all participants reach a common agreement on the state of the network, even in the presence of malicious actors or unreliable nodes.

Ex- POW,POS,POH

Problem with Standardized time

Other Blockchain rely on standardized time to assign time stamps to validate transactions in the order that they were received.

Standardized time is centralized, so use a centralized things this make defeats of a decentralized system, and so on

But Solana decided that didn't use standardized time, Solution make your own time???

Instead of relying on a centralized clock solana has timestamps build into the blockchain.

Validate nodes using a Verifiable Delay function (VDF)
Every Block Producer has to go through this VDF. VDF is the consensus algorithm

Cryptographic Timestamps

Cryptographic timestamps are a way to securely record and verify the time when a particular event or piece of information occurred. They use special mathematical techniques to ensure that the timestamp cannot be tampered with or forged.

Imagine you have a document that you want to prove was created at a specific time. With cryptographic timestamps, a unique code, called a hash, is generated based on the content of the document and the current time. This hash is like a digital fingerprint of the document.

This fingerprint is then encrypted, which means it's scrambled using advanced mathematical algorithms. The encrypted timestamp is like a sealed envelope containing the fingerprint, and it can only be opened with a special key.

The encrypted timestamp is then securely stored in a trusted system, such as a blockchain or a secure server. This ensures that the timestamp cannot be altered or manipulated by anyone, including the person who created the document.

Later, if someone wants to verify the timestamp, they can use the same cryptographic techniques to check if the fingerprint matches the original document. If the fingerprint matches, it means that the document existed at the time recorded in the timestamp, and it has not been tampered with since then.

Cryptographic timestamps provide a way to prove the integrity and authenticity of digital information, such as documents, files, or transactions, by securely recording the time of their creation.

Validating nodes

Uses hash,count and other data and through the VDF, sets an upper bound on time.

While VDF won't tell you it's 10:00 PM or 6:00 PM, it will tell you exactly in the past and future of the global state machine a transaction occurred.

On Solana, any individual node can validate the entire chain with just a small piece of information.

Proof of History is a concept that helps computers and systems agree on the order of events in a secure and reliable way. It's like a digital timeline that everyone can trust.

Think of it as a clock that ticks at a constant rate and records every single tick. In Proof of History, instead of a physical clock, we use a special cryptographic algorithm that generates a unique and verifiable sequence of numbers called a "proof."

This proof is created in such a way that it takes time to generate, and it's practically impossible to fake or cheat. Each new proof is based on the previous one, forming a chain of proofs that represents the passage of time.

When a computer or system wants to prove that a certain event happened before another, it can simply show the corresponding proofs. Since the proofs are generated in a sequential and time-based manner, it becomes easy for everyone to verify the order of events.

The great thing about Proof of History is that it doesn't require a central authority or a single trusted source. Instead, it relies on cryptographic principles and the consensus of multiple participants in a decentralized network.

By using Proof of History, systems can establish a reliable and agreed-upon order of events, which is crucial for various applications like cryptocurrencies, distributed ledgers, and even ensuring fairness in online games. It helps create a trustworthy timeline that everyone can rely on.