Criptography
“Solana: DFuture?”

Ruben Teimas

m47753@alunos.uevora.pt

Departamento de Informática
Escola de Ciências e Tecnologia

January 13, 2022

UNIVERSIDADE DE ÉVORA

Introduction

Blockchain

- Structure
- Applications

Ethereum

- Smart-contracts
- dApps
- Running out of GAS

Solana

- Proof of History
- Proof of Stake

Web 3.0

Introduction

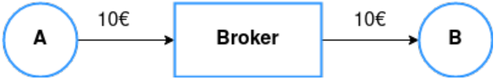

Figure: Money transaction using a broker.

Introduction

- It would work like a *P2P* system.
- *P2P* protocols were very popular.
  - BitTorrent.
  - Napster.
- *P2P* protocols at the time, hadn't solve the double spending problem.

Introduction

- In 2008, Satoshi Nakamoto, present a paper where it was proposed:

"an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party"

- *Bitcoin* was born!

Introduction

Blockchain

- Structure
- Applications

Ethereum

- Smart-contracts
- dApps
- Running out of GAS

Solana

- Proof of History
- Proof of Stake

Web 3.0

Blockchain

- Distributed storage, distributed over a network of peers that ensure the consistency of the chain
- Blocks of information, validated by the network of peers as trustworthy, are then recorded in the storage.
- Each block holds a list of transactions functioning like a public ledger, and a reference (hash) to the previous block

Blockchain structure

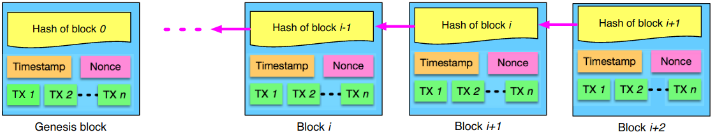

Figure: Blockchain representation.

Blockchain applications

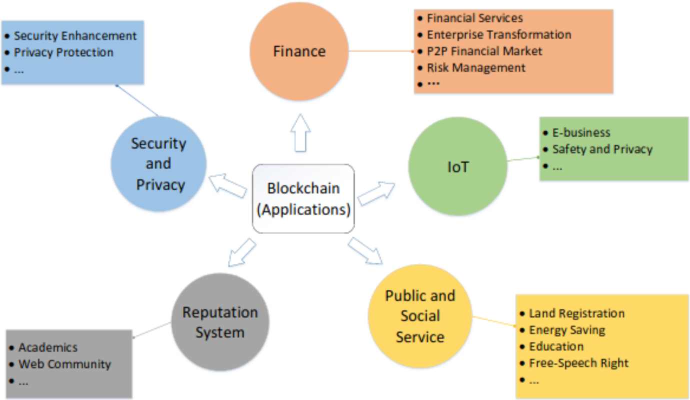

Figure: Blockchain applications.

Introduction

Blockchain

- Structure
- Applications

Ethereum

- Smart-contracts
- dApps
- Running out of GAS

Solana

- Proof of History
- Proof of Stake

Web 3.0

Ethereum

- Unlike *Bitcoin*, it wasn't focused on one task.
- Platform to build and deploy different types off applications rather than an application itself.
- Introduced *smart-contracts*.

Smart-contracts

- Code that is executed in the blockchain when specific conditions are met.
- Example:
  - We want Bob to send a coin to Alice, in Ethereum (with smart contracts) we can demand Bob to send an ether (the Ethereum currency) to Alice if the date is 1st of January and Alice's balance is less than 100 ether.
- Smart-contracts allow clients to create *dApps*.

dApps

- Decentralized application refers to an application that is built on top of blockchain technology.
- They benefit from all of its properties like immutability, security, tamper resistance and zero downtime.

Ethereum's scalability

- One of the problems pointed out to *Ethereum* is the scalability.
- It uses *Proof of Work* (*PoW*) as a consensus mechanism, just like *Bitcoin*.

Proof of Work

UNIVERSIDADE DE ÉVORA

- Requires miners to solve complex mathematical puzzles in order to validate transactions.

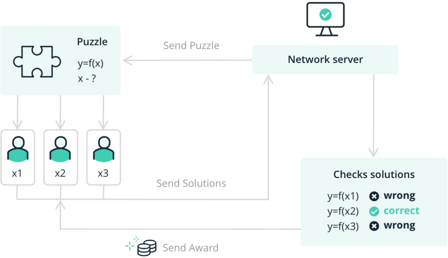

Figure: Proof of Work.

- It is very expensive energy-wise.
- Which makes the transactions fees (*GAS*) very high.

Introduction

Blockchain

- Structure
- Applications

Ethereum

- Smart-contracts
- dApps
- Running out of GAS

Solana

- Proof of History
- Proof of Stake

Web 3.0

Solana

- General purpose blockchain, like *Ethereum*.
- Proposed to solve the scalability *trilemma* presented by *Ethereum developers*.
- It uses an hybrid consensus algorithm, which is based on *Proof of History* and *Proof of Stake*.

Scalability Trilemma

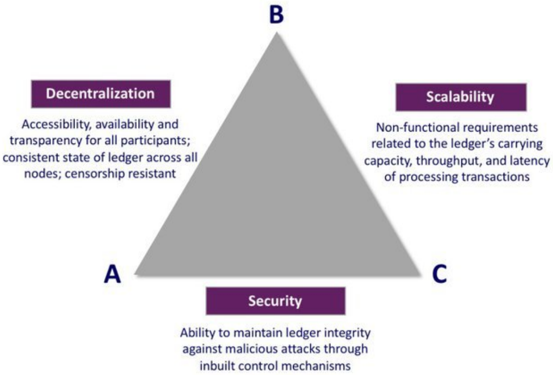
B
Decentralization
Accessibility, availability and transparency for all participants; consistent state of ledger across all nodes; censorship resistant
Scalability
Non-functional requirements related to the ledger's carrying capacity, throughput, and latency of processing transactions
A
C
Security
Ability to maintain ledger integrity against malicious attacks through inbuilt control mechanisms

Figure: Scalability trilemma.

Solana Network

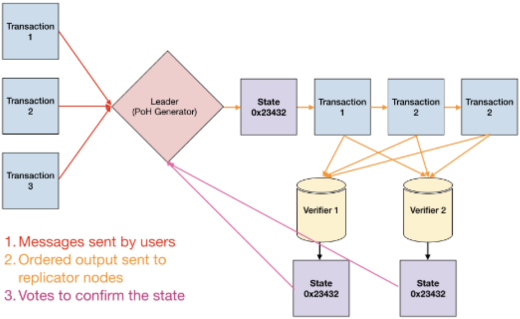

Figure: Solana Network.

Proof of History

- Is a sequence of computation that can provide a way to cryptographically verify passage of time between two event
- With a cryptographic hash function (e.g. sha256), run the function from some random starting value and take its output and pass it as the input into the same function again.
- Record the number of times the function has been called and the output at each call.

Proof of History

- The sequence is computed on a single threaded node, because there is no way of predicting the output of the function.
- This allows the verifiers not to worry about timestamps and internal clocks, which means there is no need to communicate in that regard, speeding up the process
- It can also be used to timestamp external actions. For instance, if a picture is taken and we want to store its metadata in the blockchain we simply append the sha256 of the metadata to the hash of the previous computation and pass it as input to the hash function. This will give us a chronological order of external event.

Proof of History

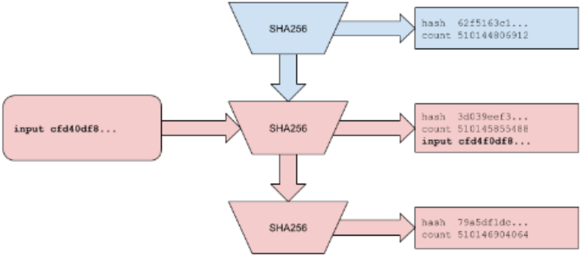

Figure: Inserting data into *Proof of History*.

Proof of History

- Even thought the sequence needs to be computed sequentially, the verification can be made on a multi-core (e.g. *GPU*) in significantly less time.
- *PoH* generators can also be synchronized.
- Given generators A and B, A receives a data packet from B, which contains the last state from Generator B, and the last state generator B observed from Generator A. The next state hash in Generator A then depends on the state from Generator B, so we can derive that hash1b happened sometime

Proof of History

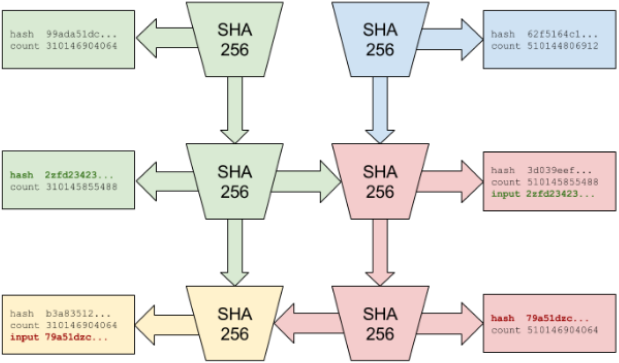

Figure: *PoH* generators syncing.

Proof of Stake

Designed for quick confirmation of the current sequence produced by the Proof of History generator, for voting and selecting the next Proof of History generator, and for punishing any misbehaving validators.

Introduction

Blockchain

- Structure
- Applications

Ethereum

- Smart-contracts
- dApps
- Running out of GAS

Solana

- Proof of History
- Proof of Stake

Web 3.0

Web 3.0

- Made of decentralized apps that run on the blockchain.
- These apps allow anyone to participate without monetising their personal data.
- In a decentralised web, each participant holds a secret key and can then use it to identify each other

Solana in Web 3.0

- Audius.
- Brave.
- So many more...

Thank you!

Thank you for your attention,

Ruben Teimas

GitHub github.com/TeimasTeimoso
LinkedId linkedin.com/in/ruben-teimas