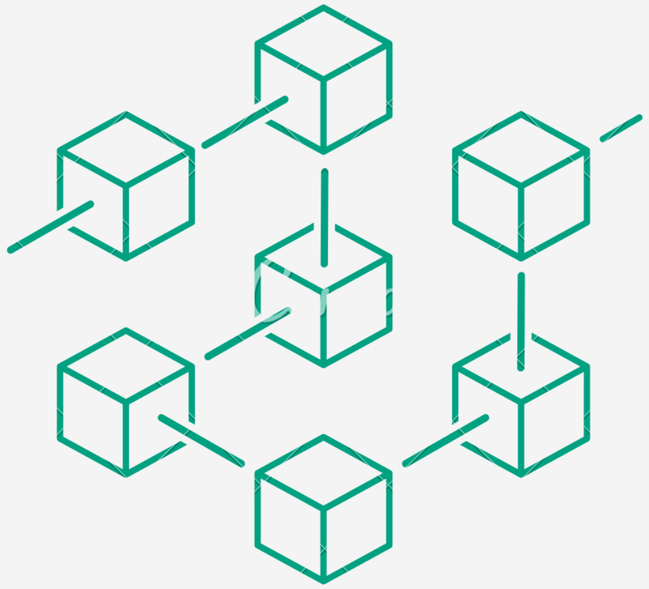
Blockchain
&
Smart Contracts



Blockchain & Smart Contracts

- Introduction to the Blockchain Technology
- What is the Blockchain
- Decentralization
- Smart Contracts
- Smart Contract Platforms
- Examples of the Blockchain Technology

Introduction to the Blockchain Technology

- In 1982, Cryptographer David Chaum proposed a protocol like the blockchain his dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups."

- In 1991, Stuart Haber and W. Scott Stornetta introduced the concept of a cryptographically secured chain of blocks

- In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees into the design, which improved its efficiency by allowing several document certificates to be collected into one block

Introduction to the Blockchain Technology

- The first decentralized blockchain emerged in 2008 with the Paper “Bitcoin: A peer-to-peer electronic cash system” by Satoshi Nakamoto

- Got its first adoption with the use of cryptocurrencies in the financial industry

What is the Blockchain?

- It's a type of distributed ledger technology (DLT) that consists of growing list of blocks

- Can be used as a distributed database that records all transactions that happened in a peer-to-peer network

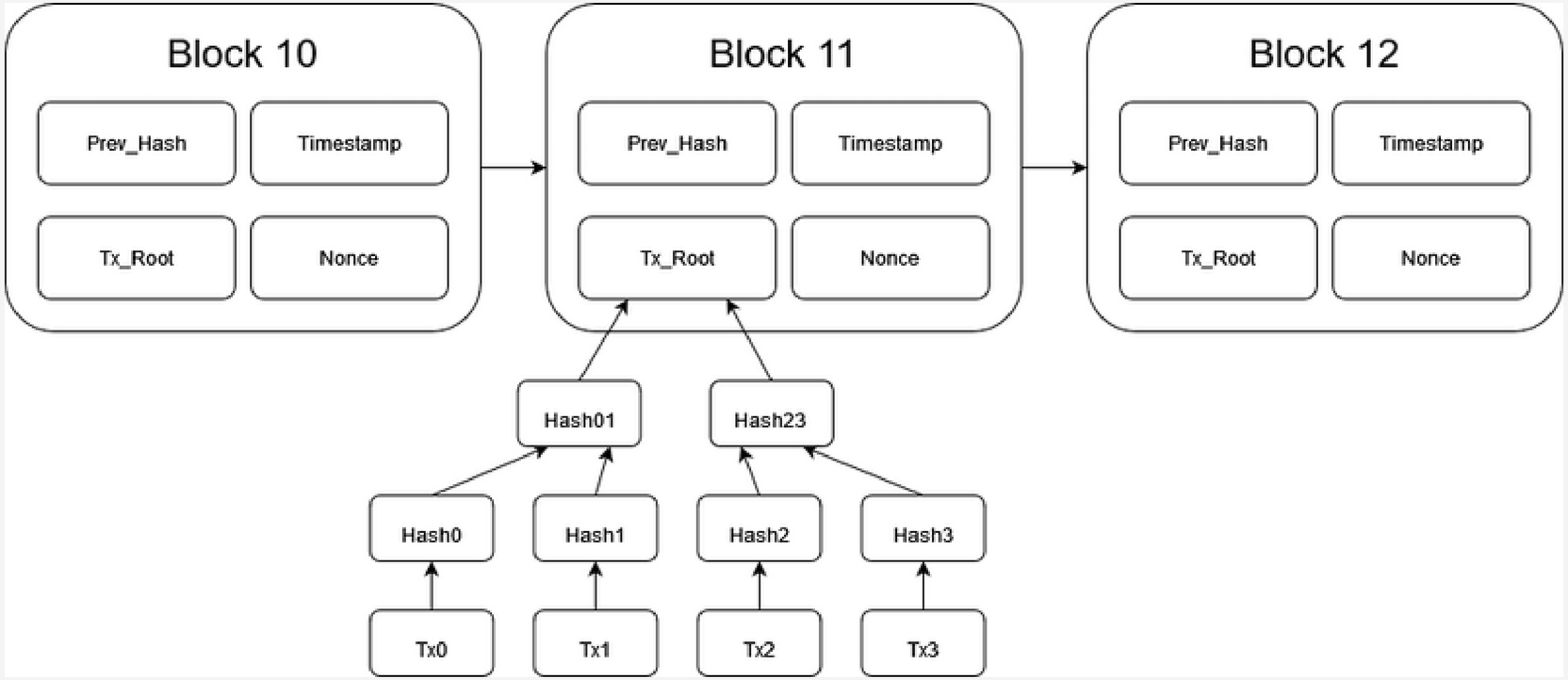
What is the Blockchain?

- Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as a public distributed ledger

- Each node collectively adheres to a consensus algorithm protocol to add and validate new transaction blocks

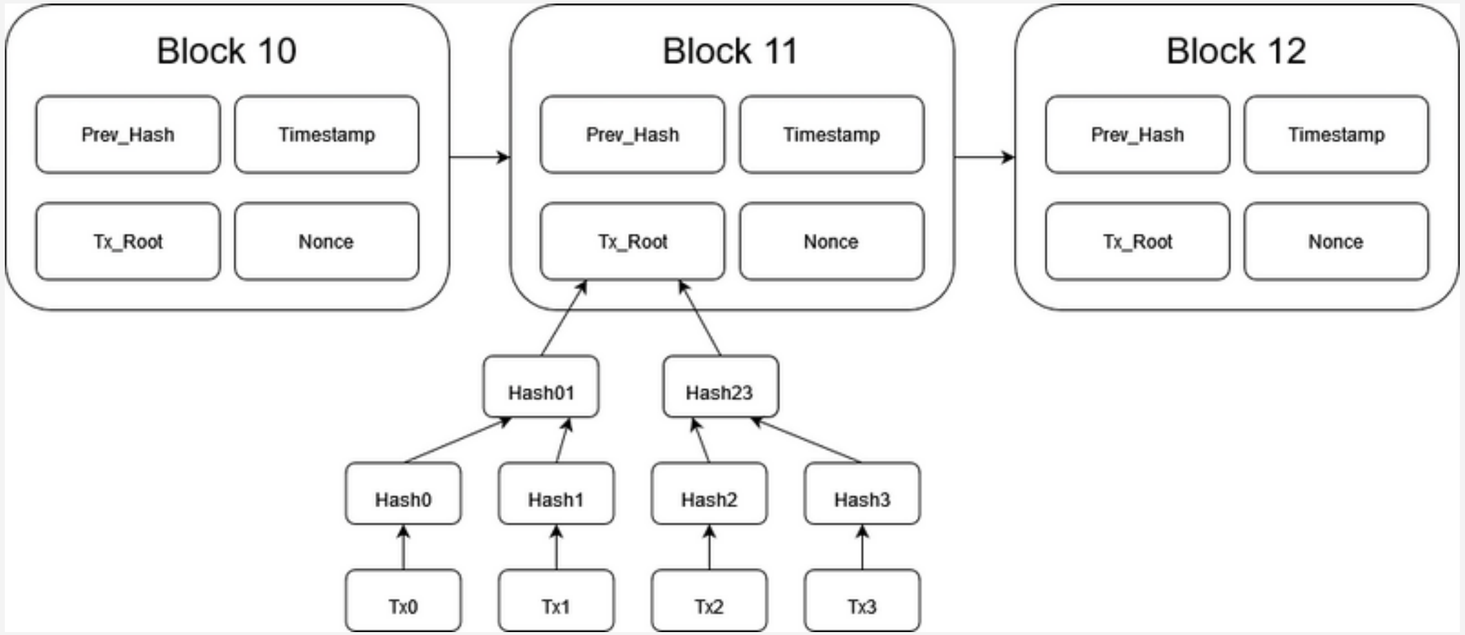
What is the Blockchain?

- Each of the blocks contains: a cryptographic hash of the previous block, a timestamp, and transaction data



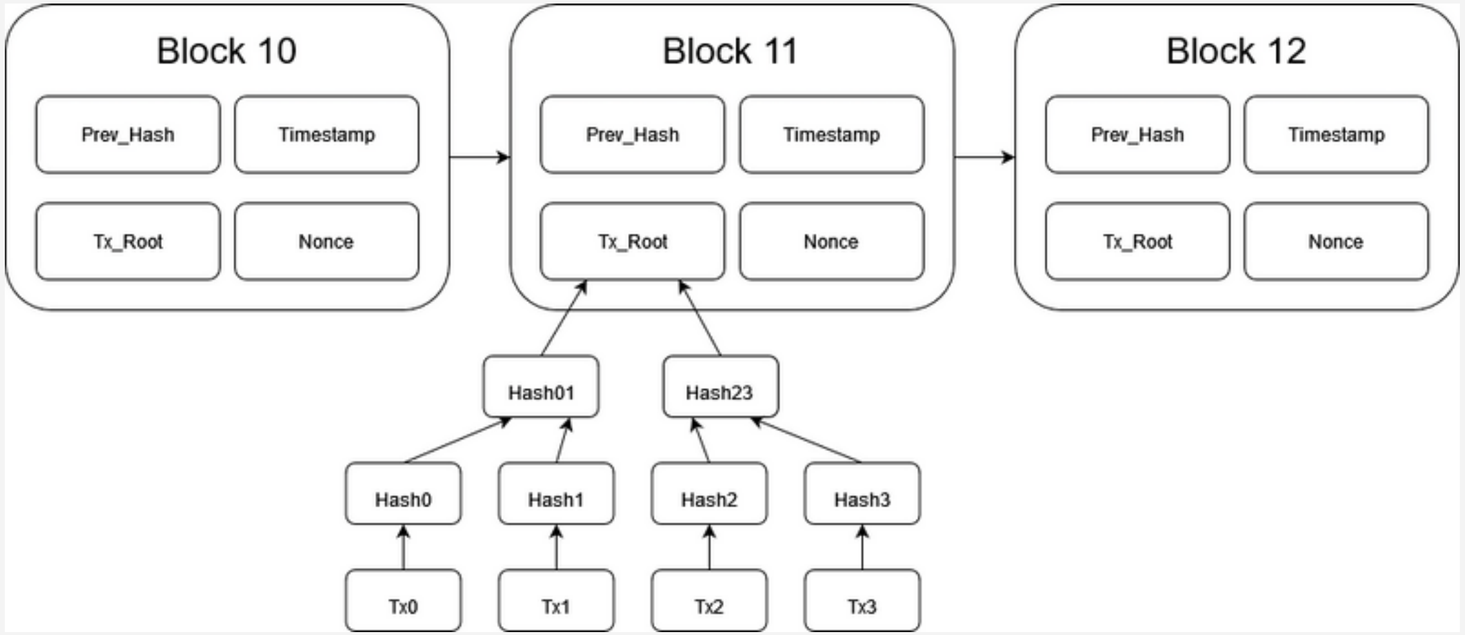
What is the Blockchain?

- Timestamp: proves that the transaction data existed when the block was created;
- Cryptographic hash: a way to secure the message block and is used to connect the blocks in a chain

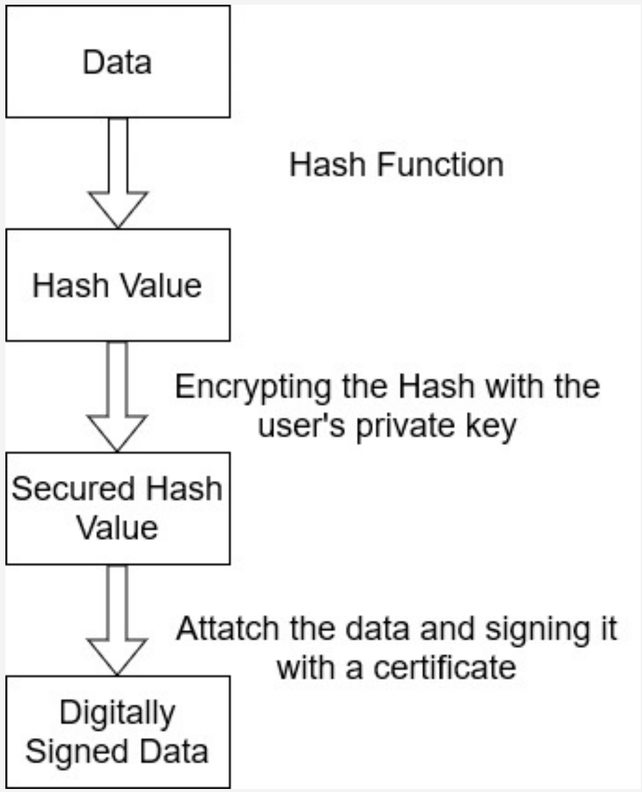


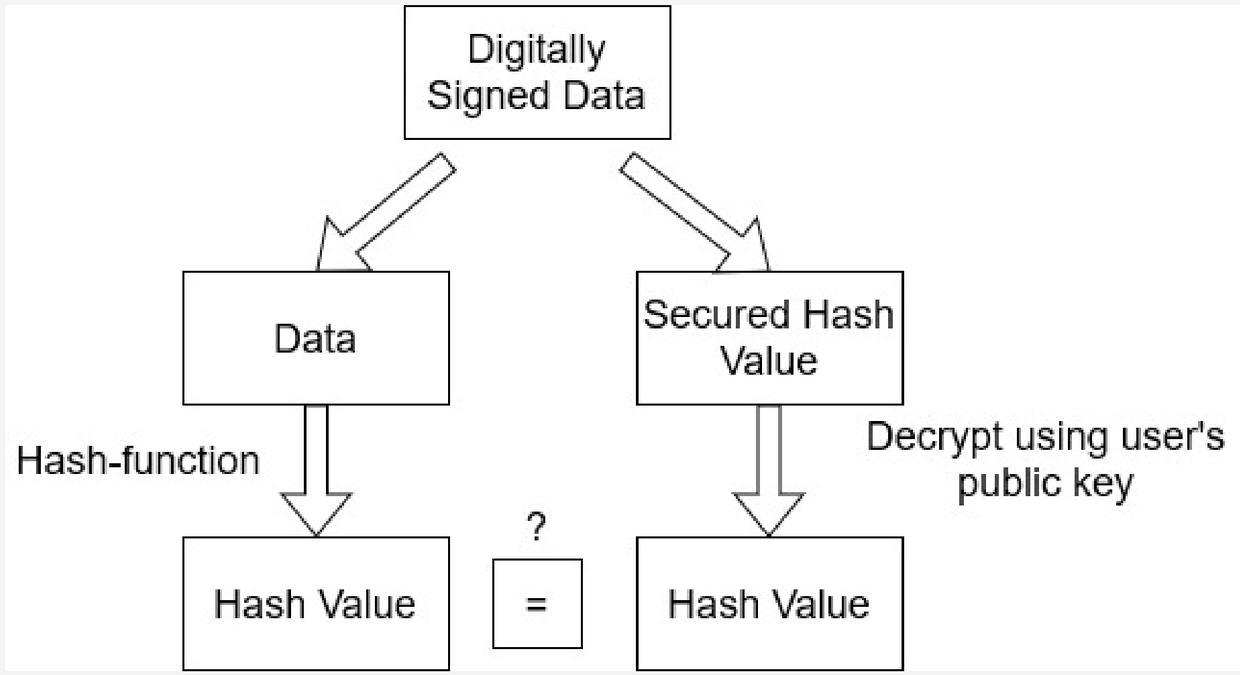
What is the Blockchain?

- Transaction data (generally represented as a Merkle tree): data nodes are represented by leaves



Signing and verifying messages in the Blockchain





1. Signing the message with a Private Key

2. Verifying the message with a Public Key

Decentralization

- Data is stored in a peer-to-peer network
- We remove the need of a third-party organization or with a central administrator
- All decisions are made by its participants
- By not relying in a third-party organization, both parties can avoid operational costs

Uses for the Blockchain Technology

Cryptocurrencies

- Most of cryptocurrencies (such as Bitcoin Ethereum) use the blockchain technology to record its transactions
- Various entities have shown interest in having a crypto currency of their own:
  - Facebook announced its cryptocurrency Diem;.
  - China has developed a national digital currency in 2020

Financial Services

- Many banking institutions have shown interest in using distributed ledgers for banking and cooperating with other companies through the use of private blockchains.

- The use of this technology has potential to speed up back-office settlement systems.

Smart Contracts

- Computer protocols designed to facilitate, verify, and automatically enforce the negotiation and agreement among multiple untrustworthy parties
- Executable code that uses the Blockchain in order to “facilitate, execute, and enforce an agreement between untrustworthy parties without the involvement of a trusted third-party”, as stated by Naheed Khan S.
- The big difference between traditional written contracts is that agreements transactions are now automated and occur without the need of a central authority

Smart Contract Platforms

- Bitcoin: The platform used for cryptocurrencies transactions allows smart contracts, but has limited computing capabilities;

- Ethereum: Supports advanced and customized smart contracts with the help of a Turing-complete virtual machine, called the Ethereum virtual machine (EVM). Contracts are written in the Solidity high level programming language, compiled into the EVM bytecode and deployed into the blockchain to be executed;

Smart Contract Platforms

- Hyperledger Fabric: an open-source enterprise-grade distributed ledger technology platform from the Linux foundation, proposed by IBM and supports smart contracts

Use cases for the Blockchain Technology

Lygon: a Bank guarantees consortium

- Australia and New Zealand have 11,500 retailers that use paper guarantees, being susceptible forgery
- Managing these guarantees is costly and hard to monitor for both the banks, landlords and managers
- AZN and IBM concluded that the Blockchain could be key component in implementing a solution to transform the guarantee lifecycle
- ANZ and IBM were joined by Westpac Banking Corporation and the Commonwealth Bank and formed the Lygon 1B Pty Ltd consortium

Lygon: a Bank guarantees consortium

- Moving to a digital workflow for the creation of guarantees, these can now be issued in sometimes less than a day by banking institutions
- Using Lygon, guarantees can be accessed securely by all parties (such as landlords, tenants and the bank) digitally using Distributed Ledger Technoly provided by the Hyperledger Fabric platform
- All parties have a private and secure way to have access their banking guarantees