Java Meetup 2021
- Blockchain concepts -

CN GROUP

Topics

What is a blockchain

- Definitions
- Db vs blockchain
- Short History
- Use cases

Types of blockchain

- Public
- Private
- Federated

Ecosystem

- Components
- Architecture

Core concepts

- Merkle tree
- Hashing
- Nonce value
- Block
- Wallets
- Transaction flow
- Mining
- Longest chain rule
- Consensus

CN GROUP

What is blockchain?

Definitios

- Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a **digital ledger of transactions** that is duplicated and distributed across the entire network of computer systems on the blockchain.

- You can think of the blockchain as a **specific type of database**. It is storing data using blocks that are chained together. New data is entered into new blocks, and once the block is filled with data, this is chained onto a previous block and this makes the data chained together in chronological order.

- Simplified, is a **list of data blocks** that are linked together with a timestamp.

CN GROUP

What is blockchain?

The main difference between a blockchain and a database

- A key difference consists in **the way data are structured**. Blockchain collects and group data in blocks, that have certain capacity in terms of storage. When a block is filled, then it is linked to the previous block, using a hash of the entire previous block content.

- Another key difference is that the blockchain is **distributed**, it does not store data in a single place and does not have a single point of failure.

- There is one more key difference; and this makes blockchain technology so famous and revolutionary — it **makes data immutable**.

CN GROUP

What is blockchain?

Short history

- Satoshi Nakamoto wrote Bitcoin: A Peer-to-Peer Electronic Cash System in 2008

- P2P has a history since ARPANET in 1969

- Predecessors:
  - DigiCash, 1989
  - HashCash, 1997
  - B-Money, 1998
  - E-Gold Ltd, 1996
  - Bitgold,1998

CN GROUP

What is blockchain?

Use cases

- Banking and Finance
- Currency
- Healthcare
- Data privacy
- Records of Property
- Smart Contracts
- Supply Chains
- Voting

CN GROUP

Types of blockchain

Public blockchain

- Permissionless
- Anybody can access and read, write or participate
- A pulblic blockchain is decentralized and has no single netwrok-controlled entity
- It has more complex rules and consensus algorithms for better security
- It is computational expensive

CN GROUP

Types of blockchain

Permissioned (private) blockchain

- Only the members of the network can read/write/audit
- Consensus is based on a multi-party consensus algorithm
- There are critics that do not consider private blockchain as “real” blockchain technology.
- With its centralized and exclusive nature, it defeats the purpose of blockcain original idea.

- This model is faster and more cost effective, because it is hard to tamper data and easy to validate transactions.

Types of blockchain

Federated/Consortium blockchain

- It is also a private and permissioned blockchain where entities can become members of the network by prior approval or voting
- This type provide all benefits of private blockchain, but adds another major one: removing the consolidation of power to only one company.
- This is a good model for organisational collaboration.

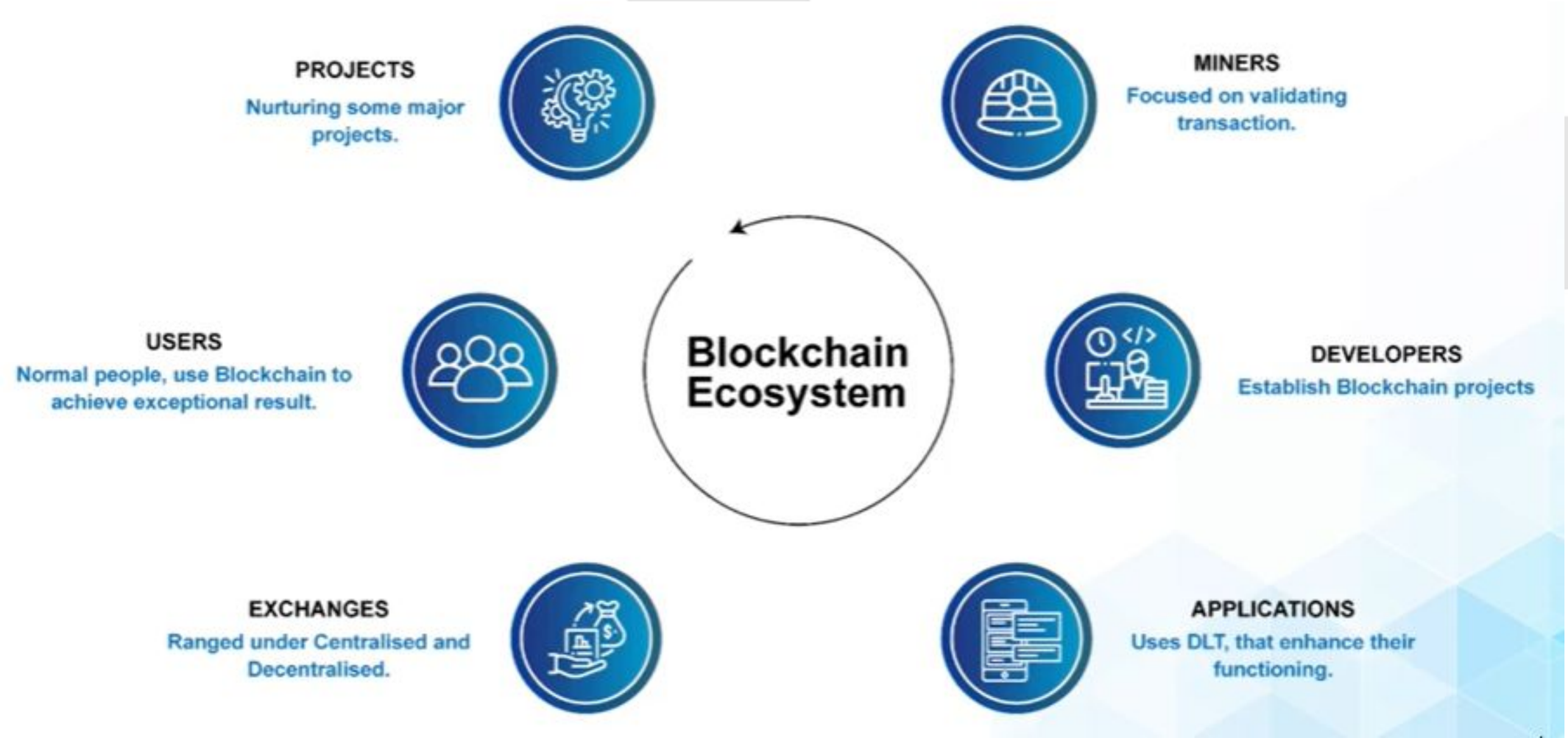
Types of blockchain

	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Access	Anyone	Single Organization	Multiple Selected Organizations
Participants	Permissionless and Anonymous	Permissioned and Known Identities	Permissioned and Known Identities
Security	• Consensus Mechanism • Proof-of-Work • Proof-of-Stake	• Pre-approved Participants • Voting-based Consensus	• Pre-approved Participants • Voting-based Consensus
Transaction Speed	Slow	Lighter and faster	Lighter and faster

CN GROUP

Ecosystem

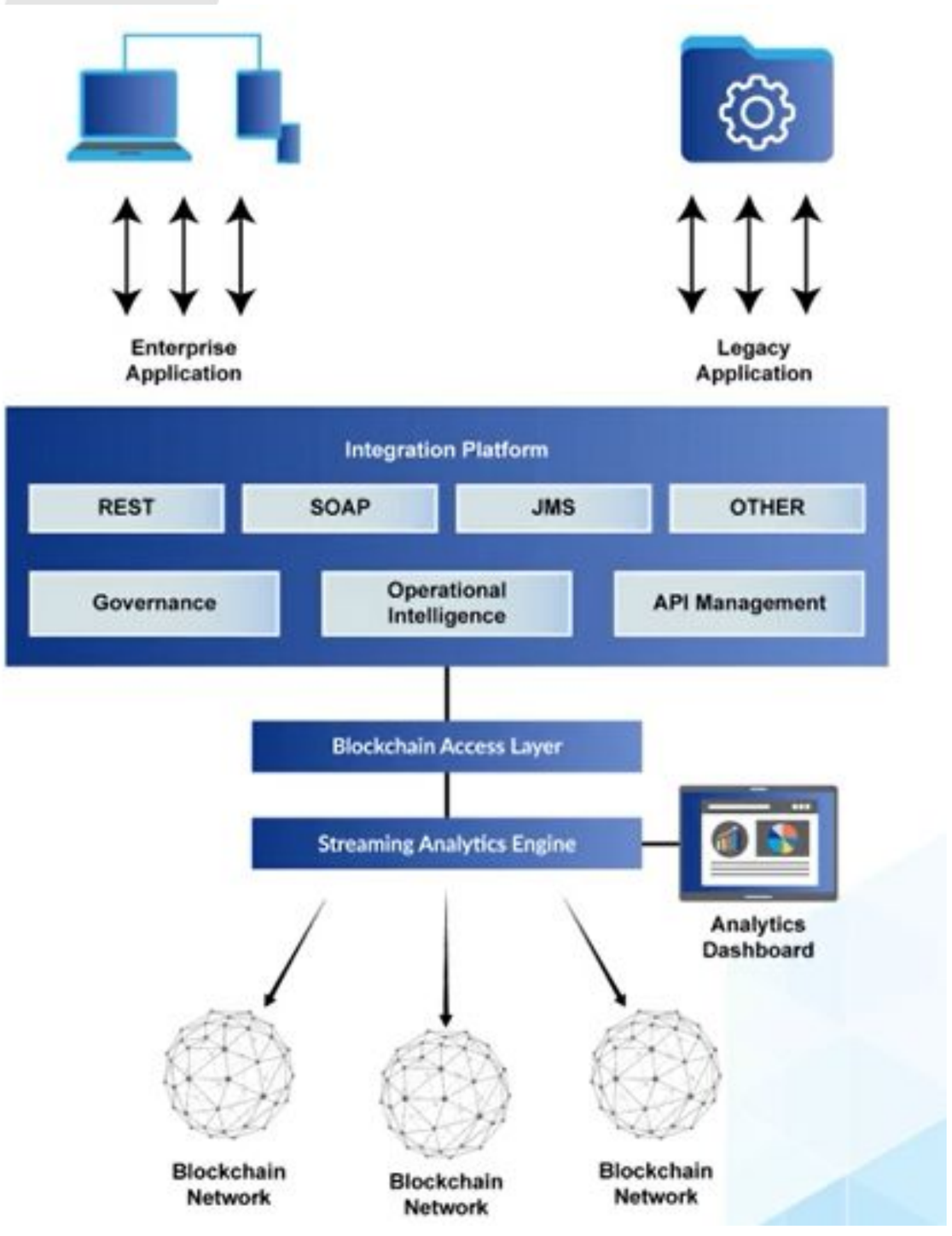
Components



CN GROUP

Ecosystem

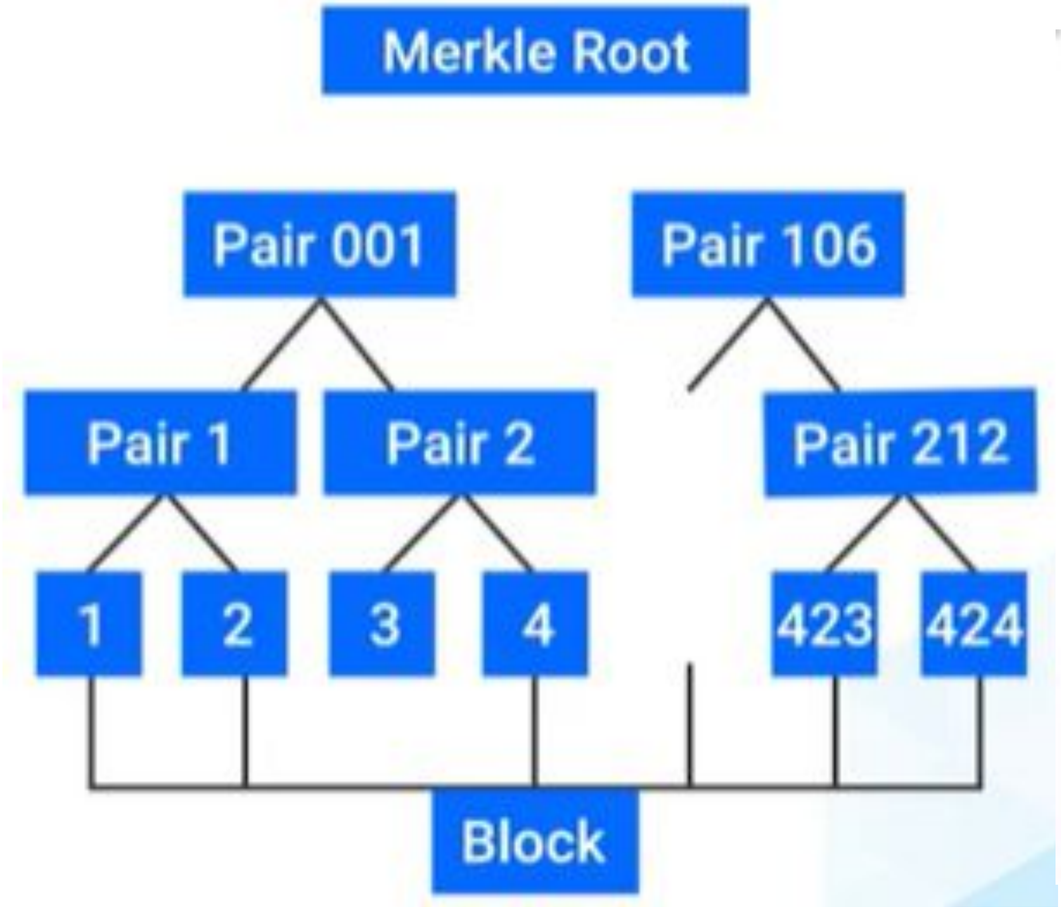
Architecture

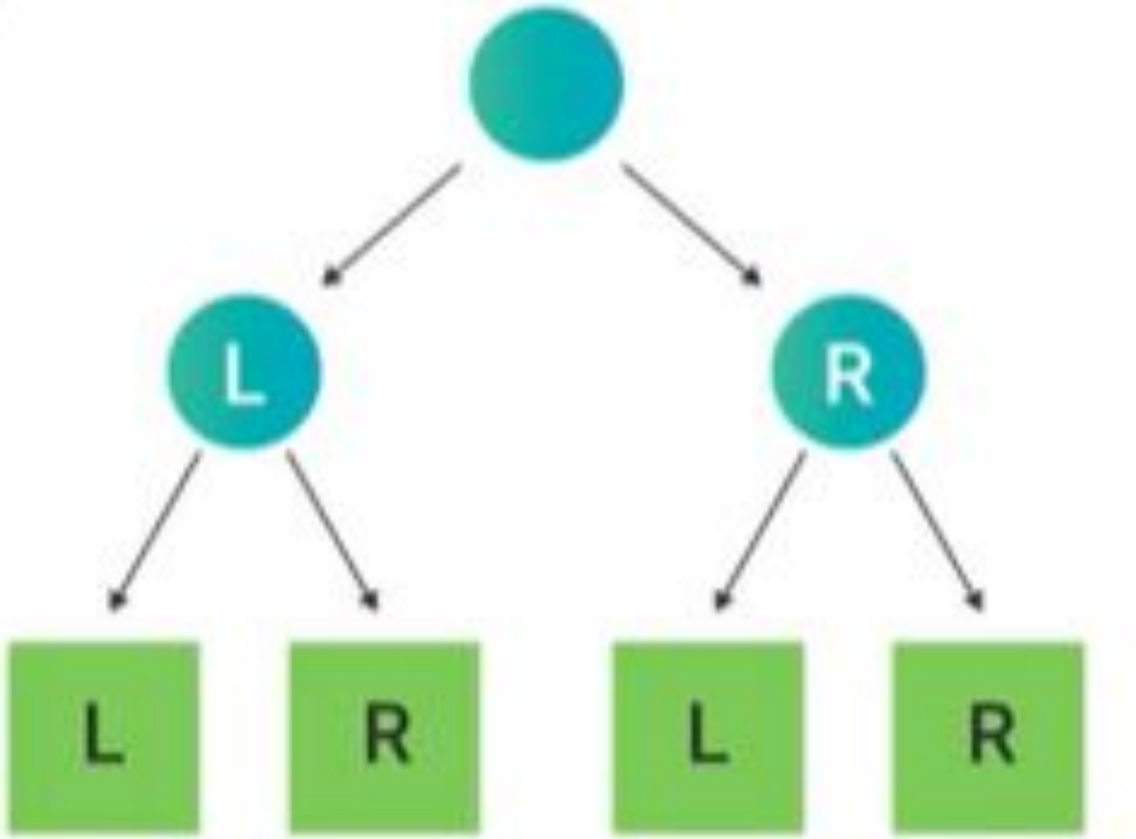


CN GROUP

Core concepts

Merkle tree



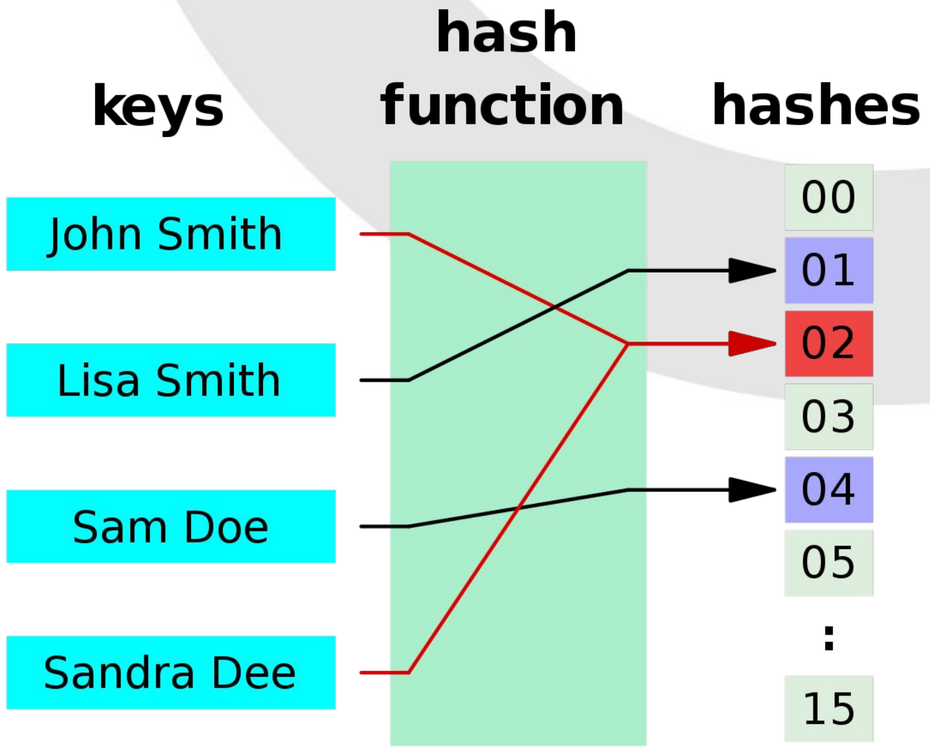


CN GROUP

Core concepts

Hashing

- Is a function that convert an input item of any length into an output item of a fixed length.



CN GROUP

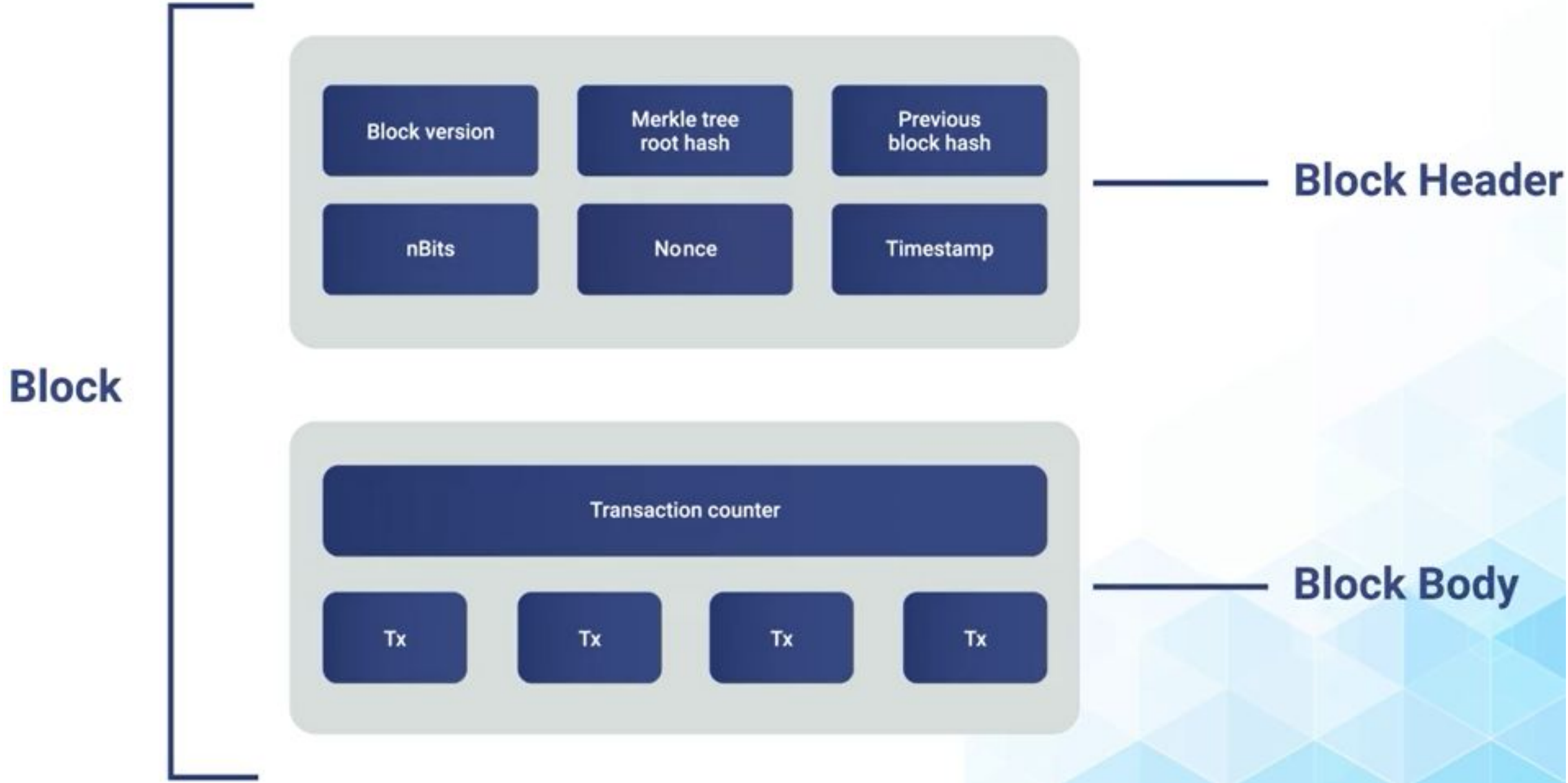
Core concepts

Nonce value

- Miners are trying to guess the hash, based on difficulty.
- The difficulty increases with the number of zeros.
- So, in this case, miners have all the transaction data, but they do not know one value, so called Nonce.

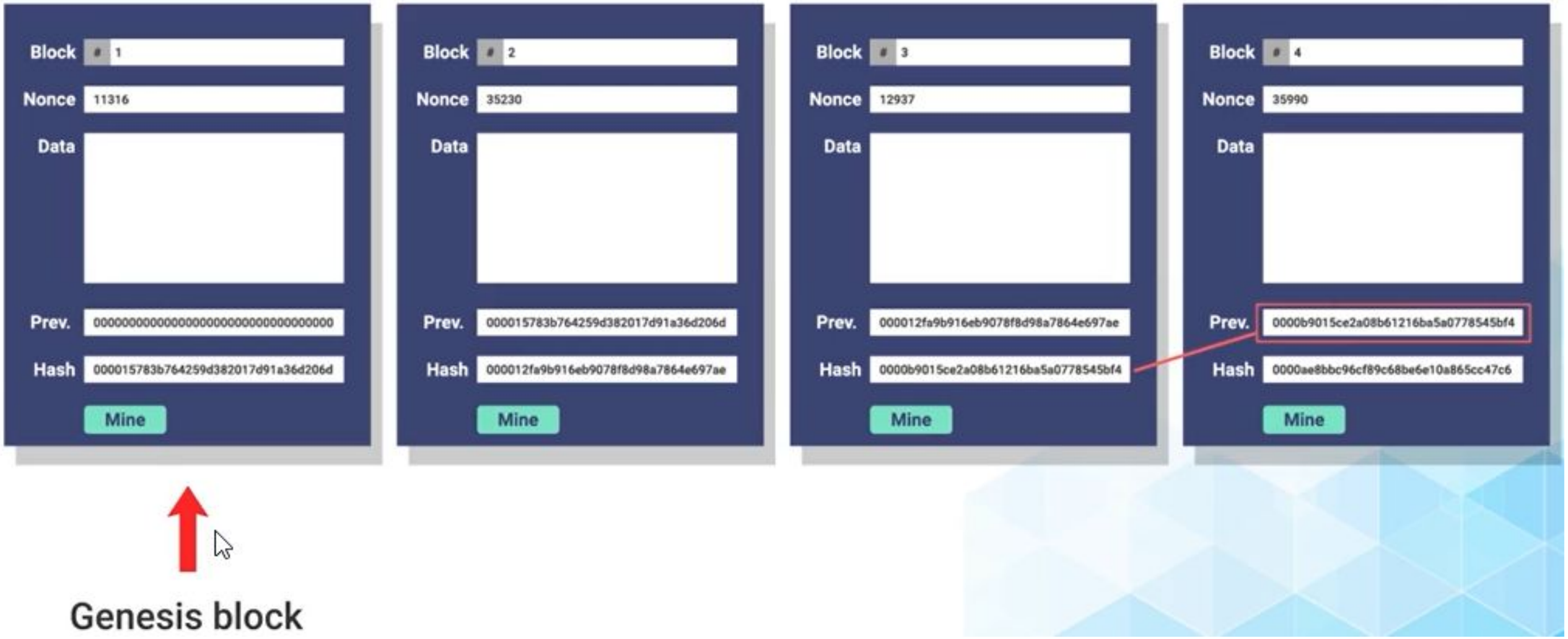
Core concepts

Block



Core concepts

Chain of Blocks



Core concepts

Transaction execution

- Initiation of transaction proposal.
- Transaction is broadcasted.
- Transaction is verified.
- Transaction is committed.

Core concepts

Mining

- It is a process of recording new transactions on the blockchain ledger. When 2 users make a transaction, nobody can see it until a miner puts it in a block. It is only after confirming the nonce value by the miner, which matches a valid hash (under target encoded in nbits).

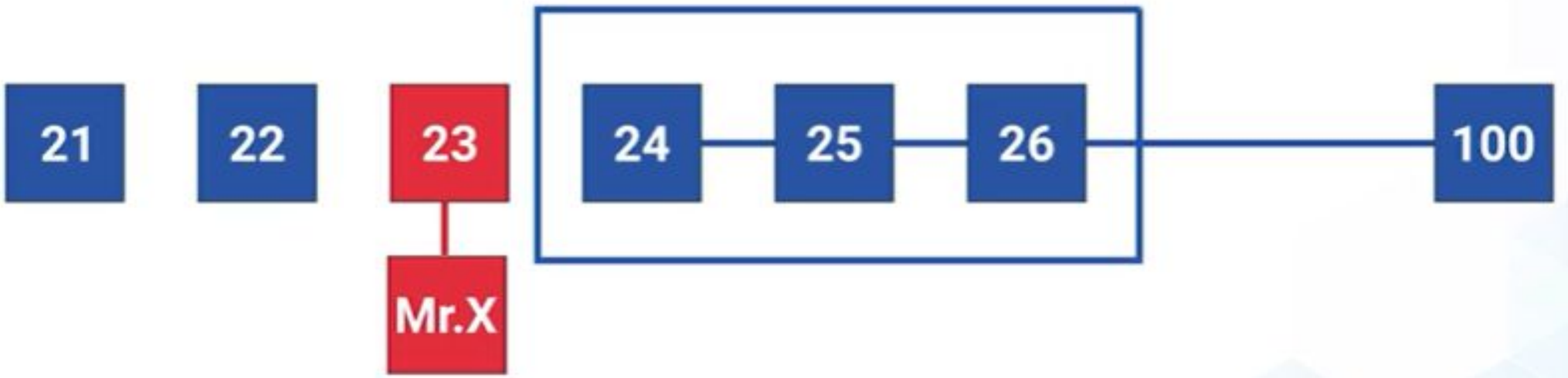
- The mining process is not mandatory for a blockchain to exist.

Core concepts

Longest chain rule

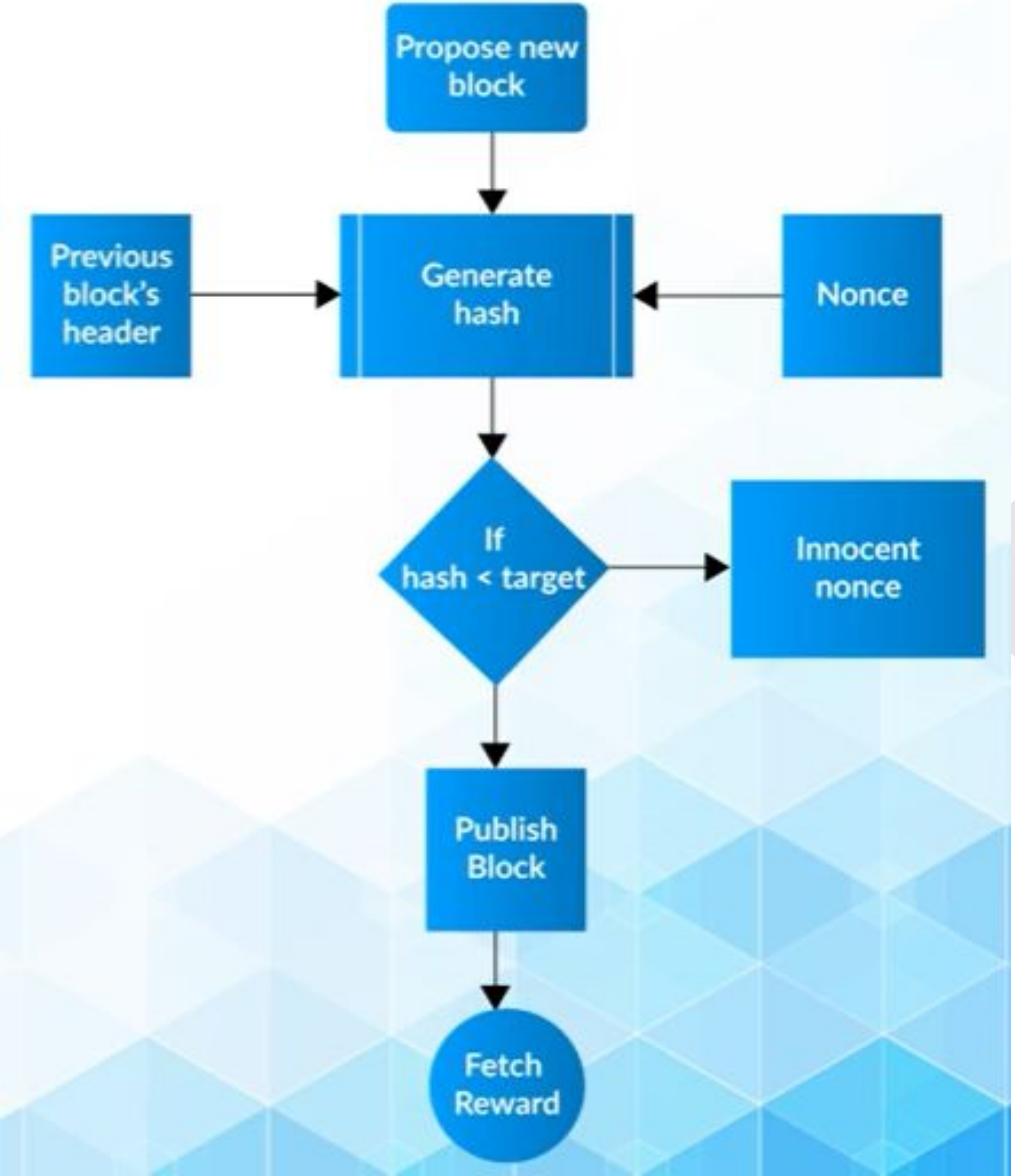
- For adding a new block to the block chain, we need to use a lot of effort to generate the blocks. As a rule, nodes will always select the longer chain over the shorter one.

- However, sometimes longest chain rule does not mean necessary the blockchain that required the most energy to be created. => most cumulative chainwork



Core concepts

Mining algorithm



CN GROUP

Core concepts

Consensus mechanisms

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Delegated Proof of Stake (DPoS)
- Proof of Importance (PoI)

CN GROUP

Thank you for your attention.

Mail:

gruia@cngroup.dk

Lucian Gruia

medium.com/@luciancgruia/blockchain-72a02a12784b

CN GROUP