INTRODUCTION TO BLOCKCHAIN

Definition

- **Layman's definition**:

Blockchain is an ever-growing, secure, shared record keeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update.

- **Technical definition**:

Blockchain is a peer-to-peer, distributed ledger that is cryptographically-secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.

In short Blockchain → Distributed Ledger

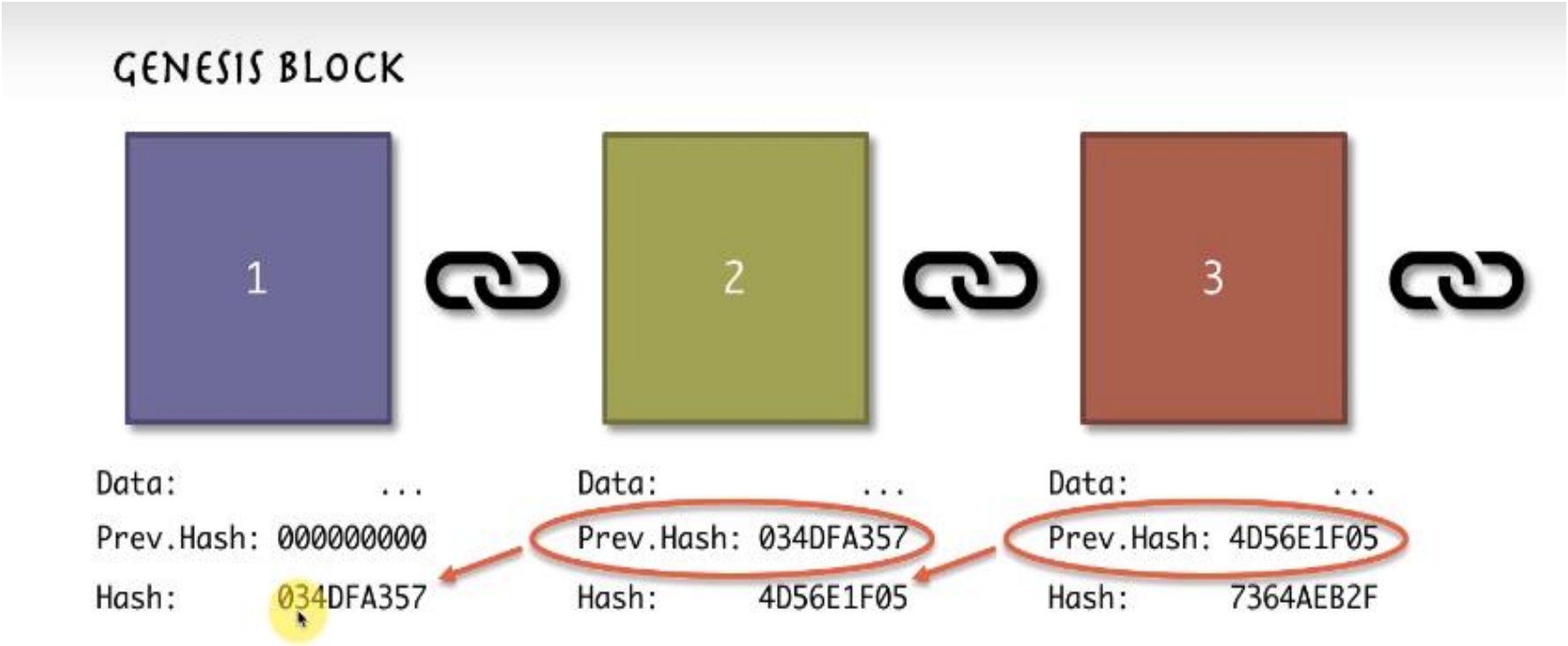
Key Terminology of Blockchain

- **Transaction**
- **Distributed Ledger**
- **Block**
- **Genesis Block**
- **Merkle root**
- **Hash Key**
- **Peer-to-peer network**
- **Node**
- **Consensus Mechanism/Protocol**
- **Smart contract**
- **Nonce**
- **Mining**
- **Wallet**

BLOCK IN BLOCKCHAIN

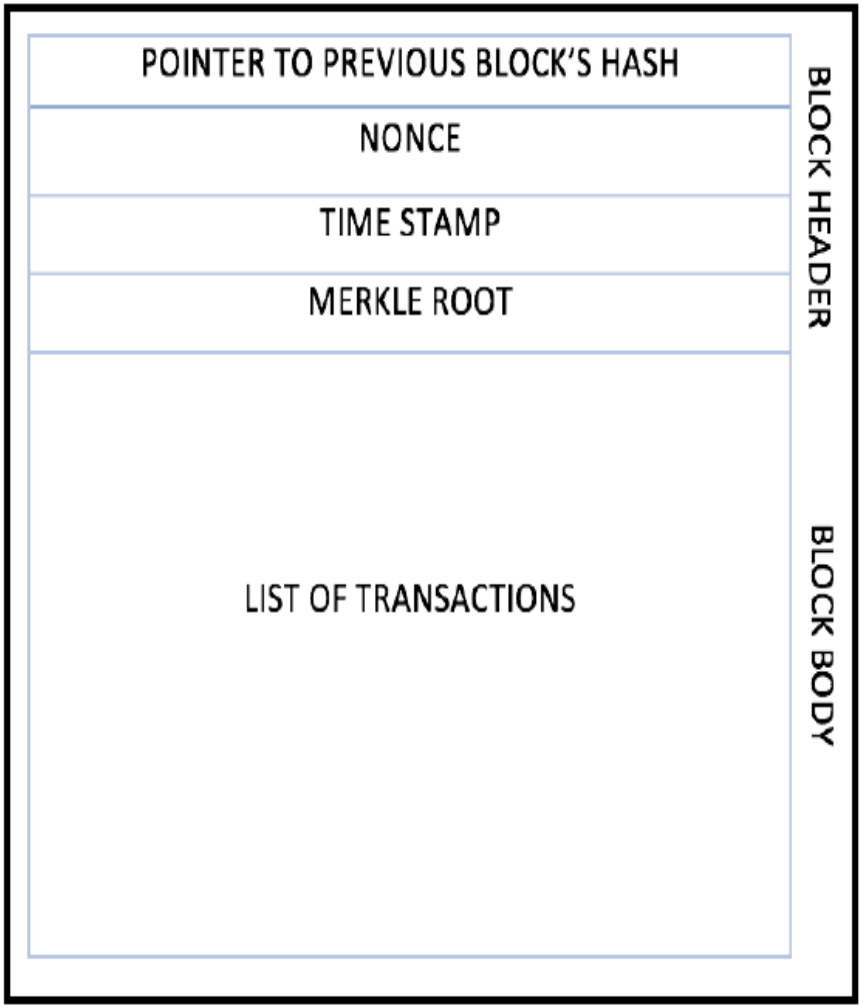
- **Transaction** - an asset transfer
- **Ledger** is the system of record for a business
- Business will have multiple ledgers for multiple business networks in which they participate.
- A shared ledger technology allowing any participant in the business network to see the system of record
- **A distributed ledger** technology allowing all participants in the business network to maintain a copy of that record/transactions
- In blockchain, a **Block** is a **container data structure** that contains a series of transactions
- **For ex. in Bitcoin:** A block may contain more than 500 transactions on average, the average size of a block is around 1 MB (an upper bound proposed by Satoshi Nakamoto in 2010)
  - May grow up to 8 MB or sometime higher (as of March 2018)
  - Larger blocks can help in processing large number of transactions in one go.

Blockchain

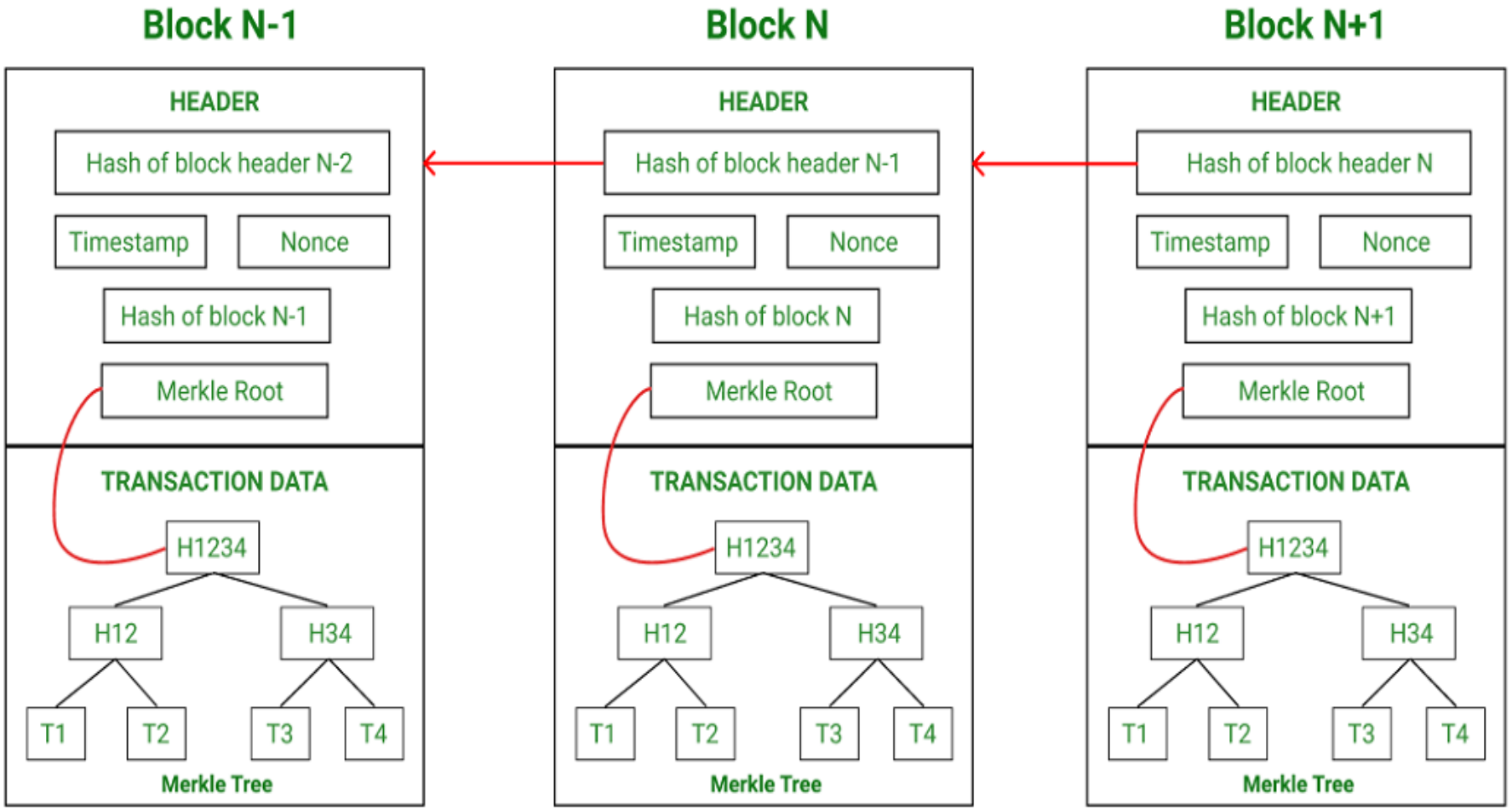

GENESIS BLOCK
1
2
3
Data: ...
Prev.Hash: 000000000
Hash: 034DFA357
Data: ...
Prev.Hash: 034DFA357
Hash: 4D56E1F05
Data: ...
Prev.Hash: 4D56E1F05
Hash: 7364AEB2F

Key Terminology & Block Structure

- The Block contains two parts
  - **the header** and
  - **the data (the transactions)**
- The header of a block connects the transactions – any change in any transaction will result in a change at the block header
- The headers of subsequent blocks are connected in a **chain – the entire blockchain needs to be updated if you want to make any change anywhere**

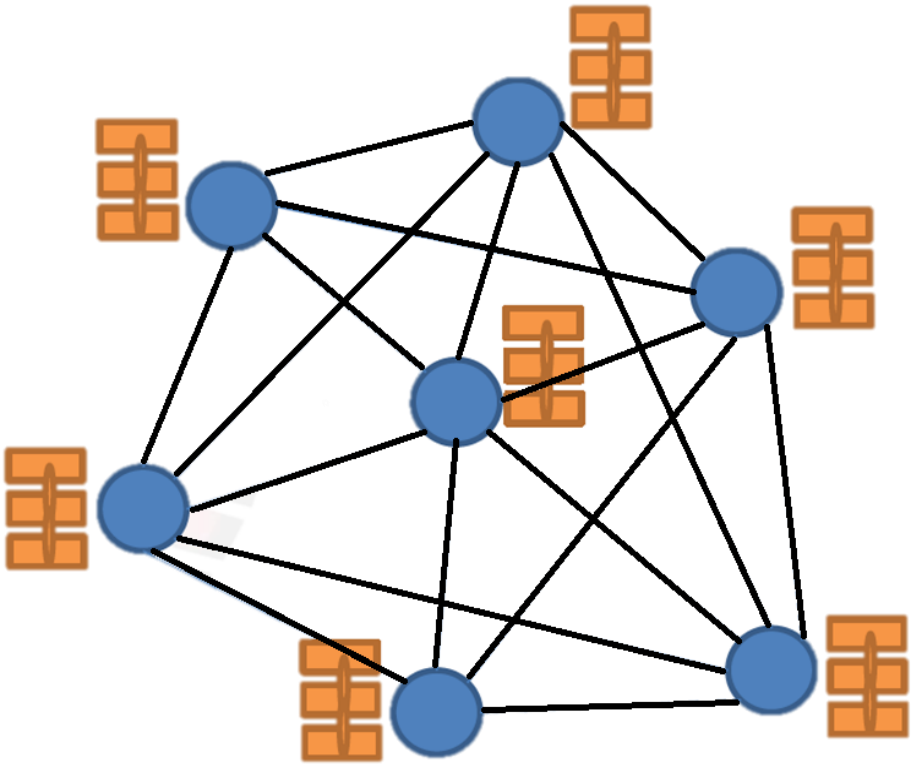


Blockchain Structure



Blockchain - The Notion of Distributed Consensus

- Every peer in a Blockchain network maintains a local copy of the Blockchain
- **Requirements**
  - All the replicas need to be **updated** with the last mined block
  - All the replicas need to be **consistent** – the copies of the Blockchain at different peers need to be **exactly similar**
- Ensure that different nodes in the network see the same data at nearly the same point of time.
- All nodes in the network need to agree or **consent** on a regular basis, that the data stored by them is the same.
- No single point of failure – the data is decentralized
- The system can provide service even in the presence of failures



51% accept

Blockchain Process

Transaction is proposed

Proposed transaction is broadcast to the network

Miners verify the transaction and bundle it into a block along with other transactions.

Miners compete to solve the complex mathematical puzzle (Mining)

The nodes verify the miner's work.

Block is added to the Blockchain.

The updated copy of the Blockchain is circulated throughout the network.

Transaction completion

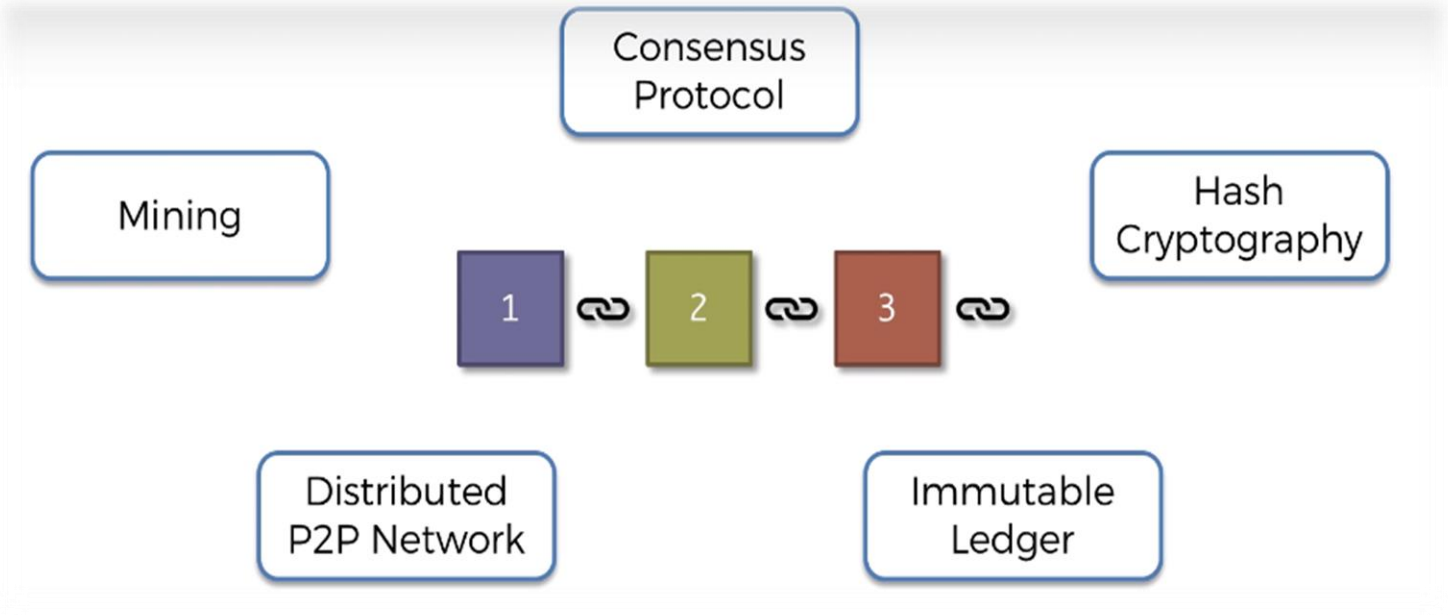
How Blockchain works?

- **Step 1:** A node starts a transaction by first creating and then digitally signing it with its private key. A transaction can represent various actions in a blockchain.
- **Step 2:** A proposed transaction is propagated (flooded) by using a flooding protocol, called Gossip protocol, to peers that validate the transaction based on preset criteria. Usually, more than one node are required to verify the transaction.
- **Step 3:** Miners verify the transaction and bundle it into a block along with other transactions, and then propagated onto the network. At this point, the transaction is considered confirmed.
- **Step 4:** Miners compete to solve the complex mathematical puzzle. The puzzle requires much computational power to solve.
- **Step 5:** The nodes verify the miner's work. The miner who finds the correct hash broadcasts the block to the network. Majority of the nodes/miners need to approve/verify the block for it to be accepted into the blockchain. Once approved, the winning miner can collect his reward(Proof of Work).
- **Step 6:** Once the block is verified, the winning miner adds his block to the existing blockchain.
- **Step 7:** The updated copy of the blockchain is circulated throughout the network.
- **Step 8:** Transaction completion.

Key Elements of Blockchain

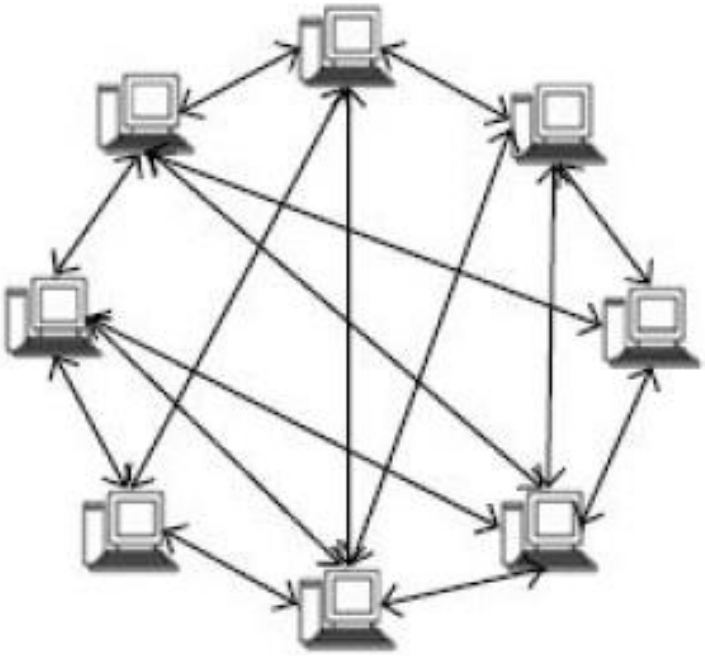
Definition:

Blockchain is a peer-to-peer, distributed ledger that is cryptographically-secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.



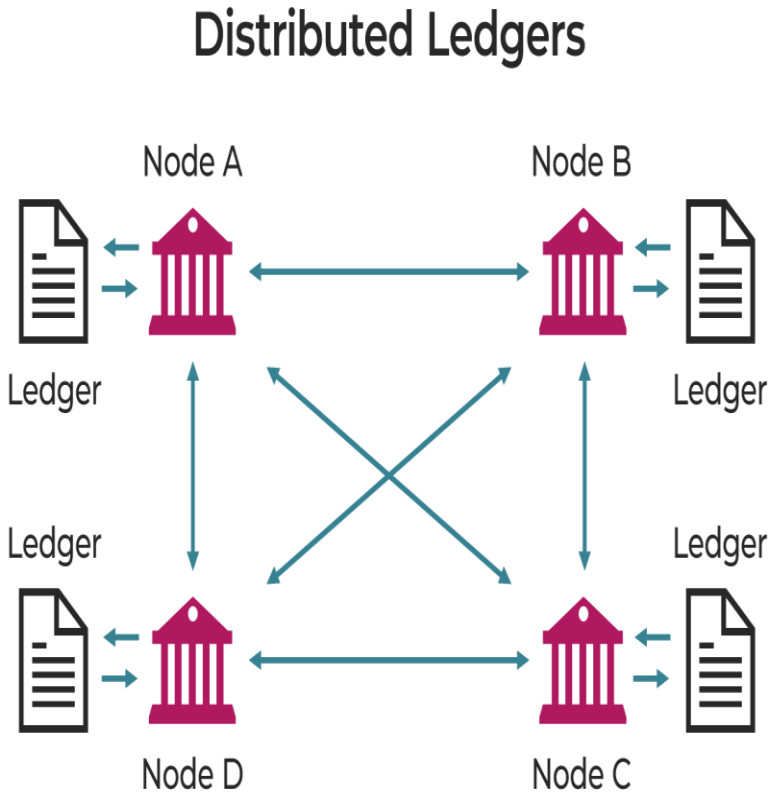
- Distributed Peer-to-Peer Network: There is no central controller in the network, and all participants talk to each other directly. This property allows for cash transactions to be exchanged directly among the peers without a third-party involvement, such as by a bank.

Types of Ledgers
Types of Nodes
Types of Blockchain
Layered Architecture
CAP Theorem



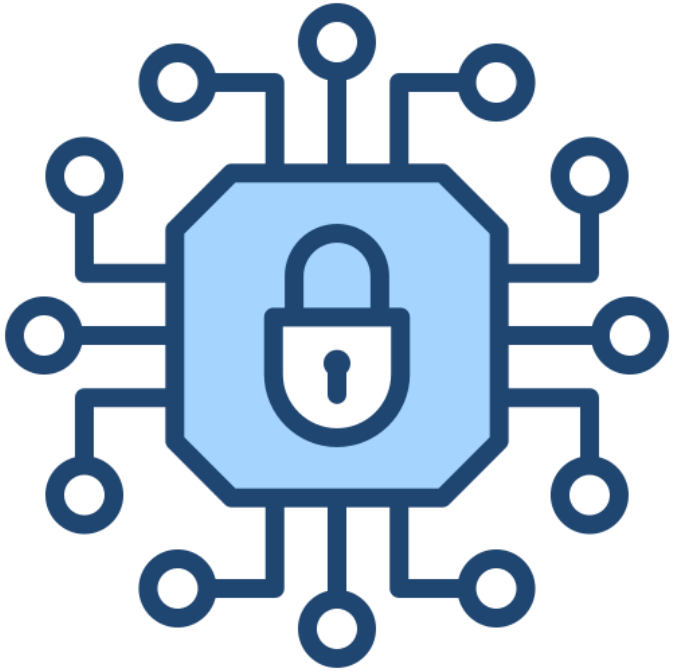
- Immutable Ledger: Which simply means that a ledger is spread across the network among all peers in the network, and each peer holds a copy of the complete ledger.

Decentralization
Distributed Ledger Technology(DLT)



- Cryptographically-Secure: Which means that cryptography has been used to provide security services which make this ledger secure against tampering and misuse. These services include non-repudiation, data integrity, and data origin authentication.

Cryptography
Hash Mechanisms
NONCE



- Append-only: Which means that data can only be added to the blockchain in *time-ordered sequential order*. This property implies that once data is added to the blockchain, it is almost impossible to change that data and can be considered practically immutable.
- Updateable Only Via Consensus: This is what gives it the power of decentralization. In this scenario, no central authority is in control of updating the ledger. Instead, any update made to the blockchain is validated against strict criteria defined by the blockchain protocol and added to the blockchain only after a consensus has been reached among all participating peers/nodes on the network.

Etherium

DApp

Smart Contracts

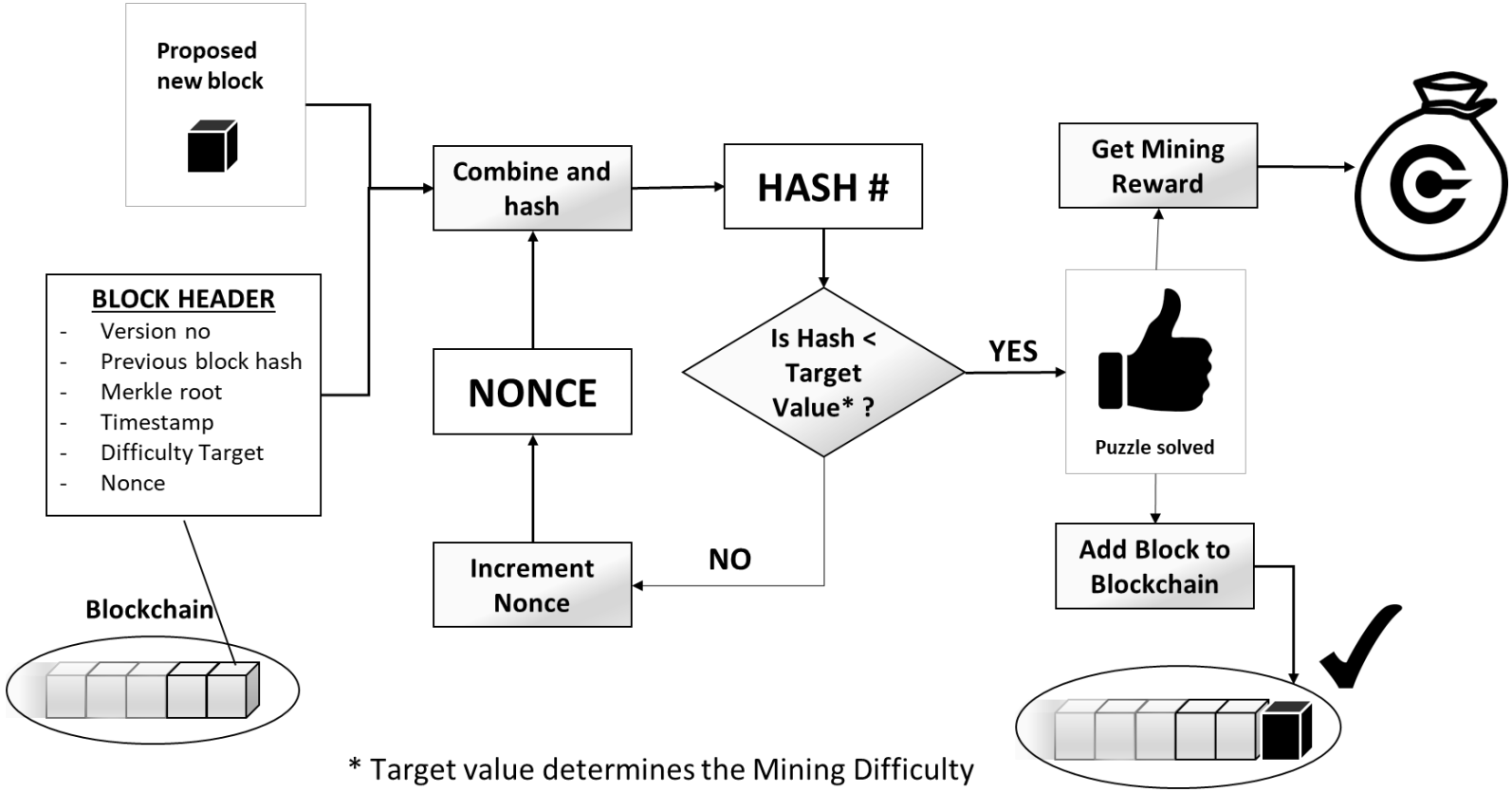
HyperLedger

• Mining Process

Mining – the mechanism to generate the hash

- The mechanism needs to be complicated enough, to make the blockchain **tamper proof**
- **Bitcoin Mining:** $H_k = Hash(H_{k-1} \,||\, T \,||\, Nonce)$
- Find the nonce such that H_k has certain predefined **complexity** (number of zeros at the prefix)

The header contains mining statistics – timestamp, nonce and difficulty



* Target value determines the Mining Difficulty

Applications of Blockchain

- Currency – Bitcoin
- IoT
- Health
- Finanace
- Media
- Aviation
- Voting
- Identity Management
- Stock trading
- Agriculture

Benefits of Blockchain

- Decentralization → copy is maintained by all
- Transparency and trust → better communication between nodes
- Immutability → all transactions are made auditable
- High availability → removes Single Point of failure
- Highly secure → consensus mechanism & complex security algorithms
- Cost saving → no intermediaries

Limitations of Blockchain

- Scalability - Significant computing power is expended by miners leading to substantial energy consumption and wastage. Hence, it is not suitable for organizations that require instant transaction results within milliseconds.
- Adaptability – If a time-tested and fully functional database and the operational network are already in place, the benefits of replacing or introducing blockchain may not produce the required return on investment.
- Not every node has the capacity to maintain and run a full copy of the blockchain. This can potentially affect consensus and immutability.
- Privacy– Stronger players (nodes with higher computing power or with pooling) can take control of the network, impacting decentralization. In smaller blockchains, there is a risk of a 51% attack.
- Regulation standard

Fundamental Concepts of Blockchain Terminology