BlockChain Technologies

Blockchain overview

WHAT IS A BLOCKCHAIN?

Abstract answer: a blockchain provides coordination between many parties, when there is no single trusted party

if trusted party exists ⇒ no need for a blockchain

[financial systems: often no trusted party]

SO WHAT IS THIS GOOD FOR?

(1) Basic application: a digital currency (stored value)

- Current largest: Bitcoin (2009), Ethereum (2015)
- Global: accessible to anyone with an Internet connection

Opinion

The New York Times

Bitcoin Has Saved My Family

"Borderless money" is more than a buzzword when you live in a collapsing economy and a collapsing dictatorship.

By Carlos Hernández

Mr. Hernández is a Venezuelan economist.

Feb. 23, 2019

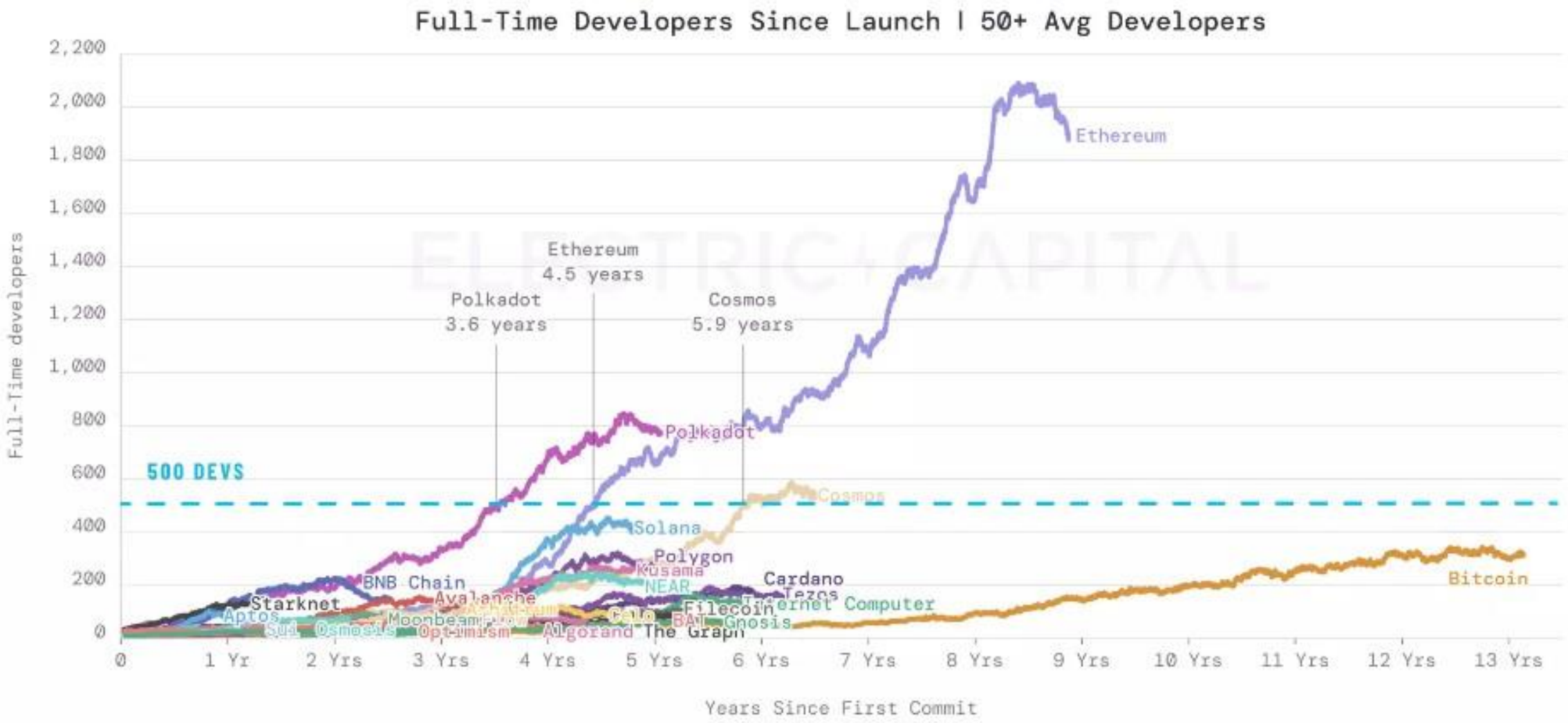
WHAT ELSE IS IT GOOD FOR?

(2) Decentralized applications (DAPPs)

- **DeFi**: financial instruments managed by public programs
  - examples: stablecoins, lending, exchanges, ….
- **Asset management** (NFTs): art, game assets, domain names, ….
- **Decentralized organizations** (DAOs): (decentralized governance)
  - DAOs for investment, for donations, for collecting art, etc.

(3) New programming model: writing decentralized programs

ELECTRIC CAPITAL



WHAT IS BLOCKCHAIN?

- Distributed ledger
- Distributed shared and secured database
- Next generation internet and tool for decentralized world
- Trust is established by Protocol
- Immutable and non-stoppable transaction
- Decentralize everything
- Transparent

WHAT IS BLOCKCHAIN?

- People from anywhere in the world can transact with other in large peer-to-peer networks without centralized management
- Cryptography and computer code strengthens collaboration and cooperation between organizations and individual to form global network
- Blockchain-based applications can help remove the intermediaries from existing processes

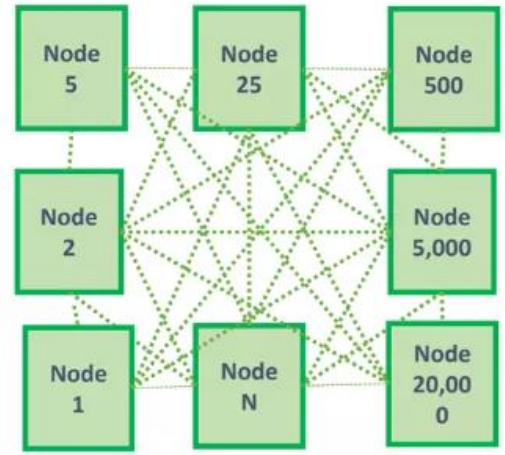
DISTRIBUTED LEDGER

- In Centralized world, most of the companies hold our data centralized and owned by the them.
- Distributed Ledger enforces storing data in Distributed nodes and which is not controlled by any organization.
- Distributed ledger is a consensus of replicated shared and synchronized digital data geographically dispersed across multiple countries or institutions without centralized administration
- Blockchain create permanent and secured distributed database.
- Blockchain records a transaction or record in distributed ledger
- This enables trust and the data cant be modified/faked

HOW BLOCKCHAIN WORKS

User requests a transaction

Transaction is broadcasted to blockchain P2P network



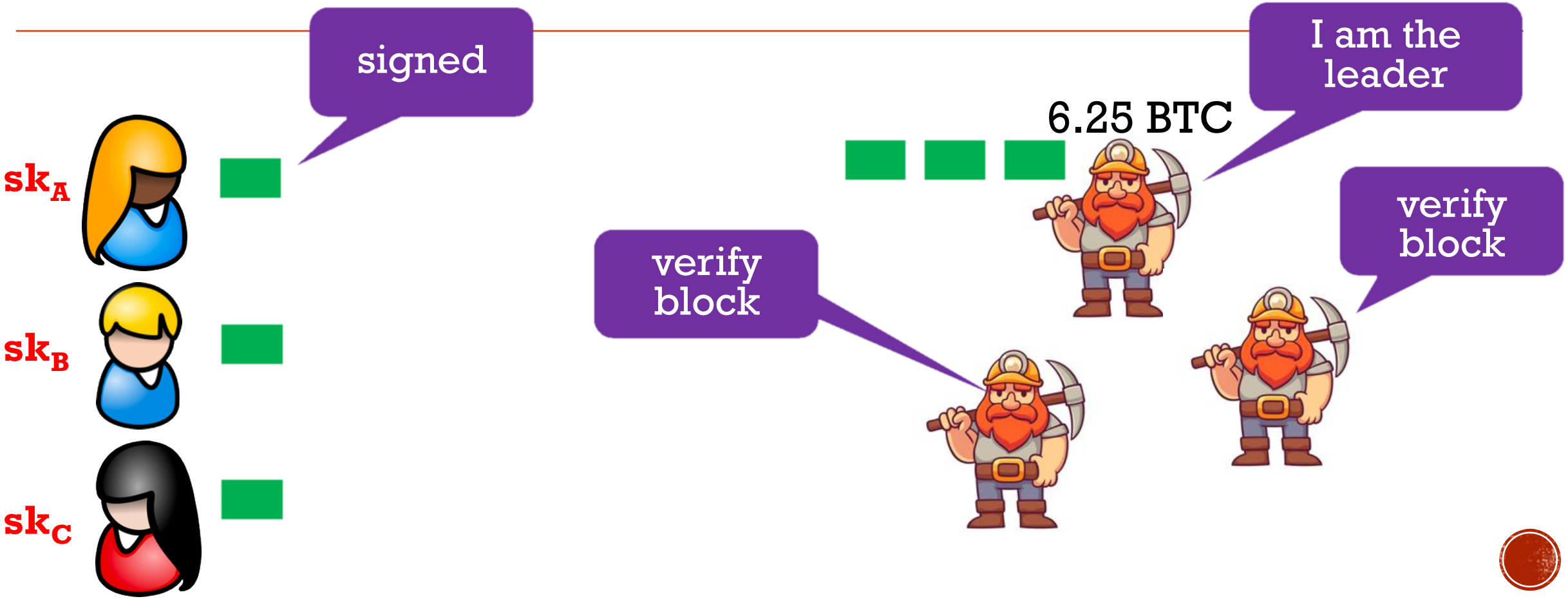
Transaction will be validated by any node in this network through some algorithms or smart contracts

once the transaction is verified by multiple nodes in the blockchain network, then new block get added to chain and replicated across all the nodes

User requested transaction is completed

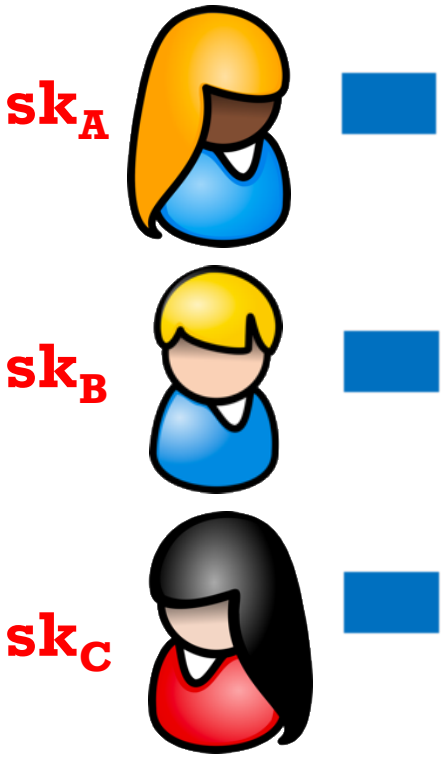
HOW ARE BLOCKS ADDED TO CHAIN?

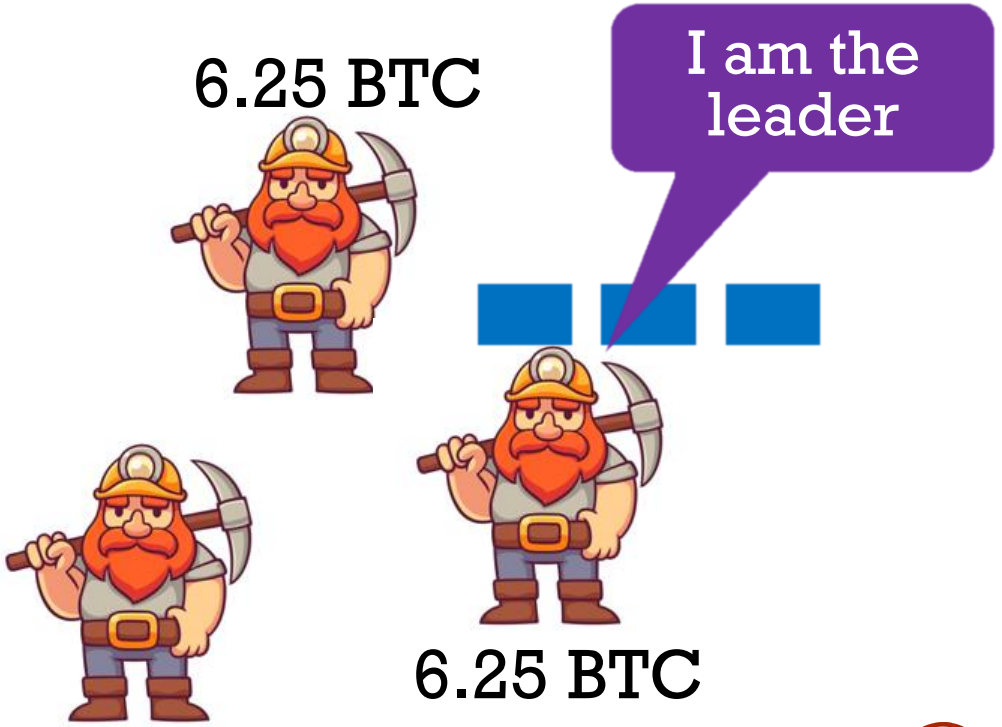
blockchain



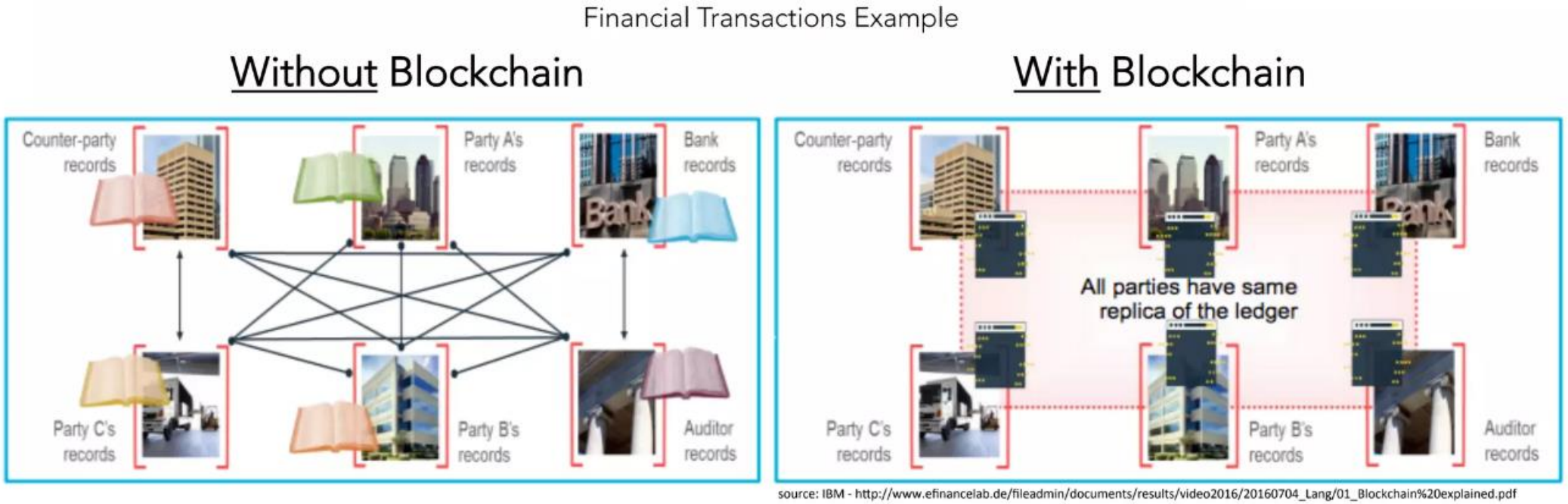
HOW ARE BLOCKS ADDED TO CHAIN?

blockchain





BEFORE AND AFTER BLOCKCHAIN

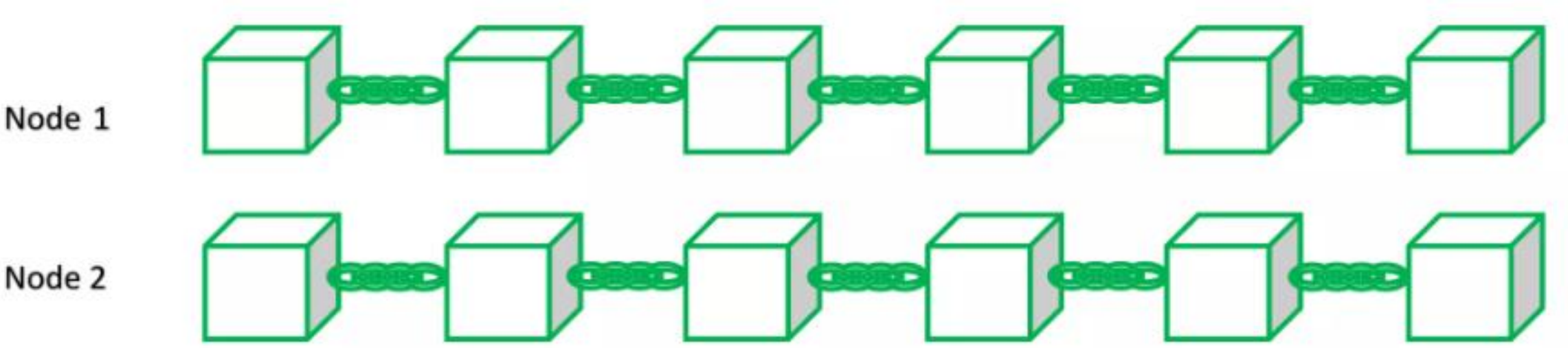


Inefficient | Expensive | Vulnerable

Consensus | Provenance | Immutability | Finality

DISTRIBUTED CHAIN OF BLOCKS

- Each node will have the copy of Blockchain
- When new block gets added to Blockchain, all the nodes are updated with the latest block
- These nodes are spread across the world

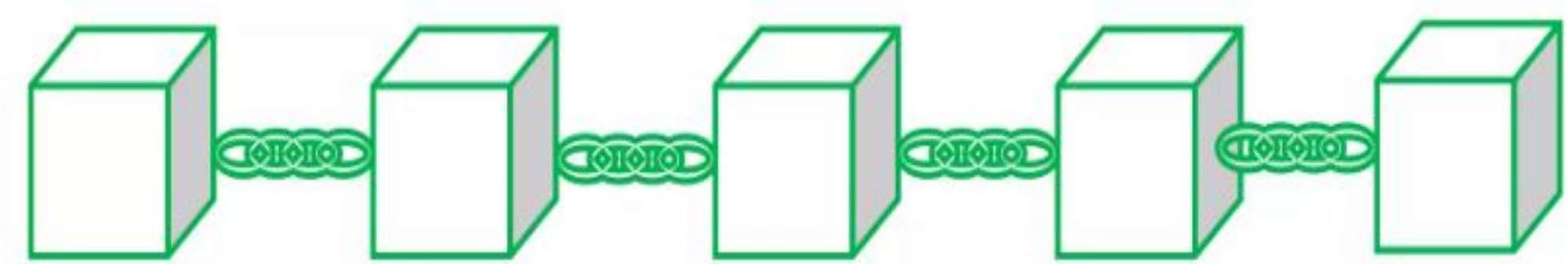


WHAT IS A BLOCK IN BLOCKCHAIN

- A Block gets added to Blockchain network for every valid transaction.
- Data is encrypted
- A Block has below details
  - Block No
  - Nonce
  - Block Hash
  - Unique identifier
  - Previous Block Hash – Unique identifier of previous block
  - Encrypted Transaction/message
  - Creation date

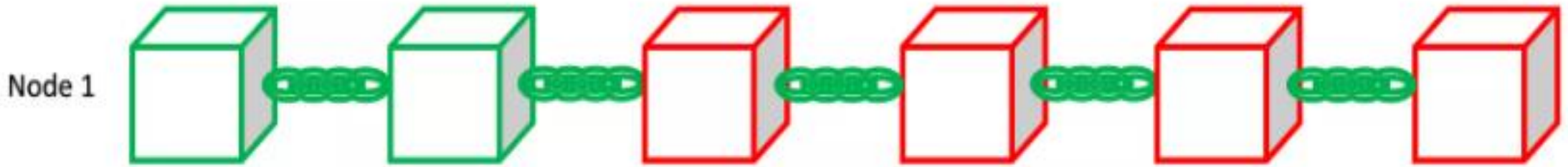
CHAIN OF BLOCKS

- A block is created for some transactions as permanent record.
- All the blocks are connected to each other by links in chain in proper linear chronological order.
- Each block has link to previous block hash value
- No block can be modified, if we trying to modify any block all the consecutive blocks will be invalidated



IMMUTABLE

- Blockchain is immutable – Blockchain data can’t be changes
- Block can’t be deleted
- As each block contains a hash value of previous dependent block.
- All the block are chained and linked
- Data tamper proof
- If any node trying to modify a block then entire Blockchain will be invalidated.
- Example: node 1 is trying to modify the 3rd block data then from 3rd block till last block are invalidated



HASHING

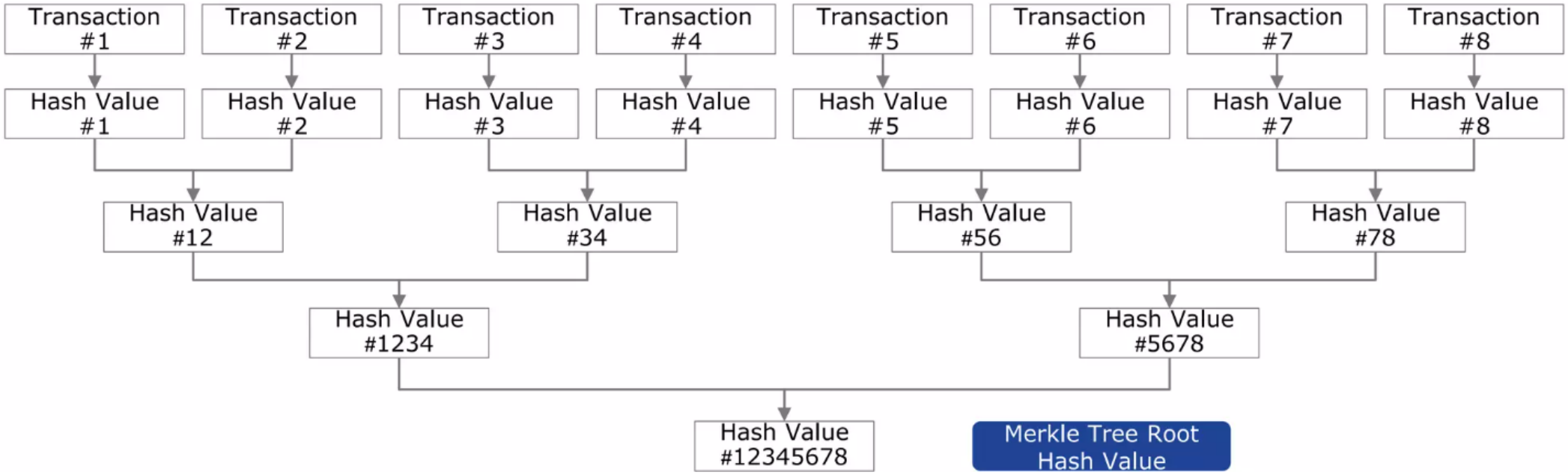
- Hashing is the process of transforming any input data into fixed length of hexadecimal number
- For each transaction, data is encrypted and given a Hash value.
- Hash Value is an unique identifier of a block
- Uses standard algorithm to compress the code and generate unique hash value

HASHING

- For any given input (smaller or bigger) the length of hash value is always same
- Easy to Compute the Hash Value
- You can’t track back the encrypted data with hash value.
- Infeasible to modify a message without changing the Hash
- Infeasible to find a message that has same hash
- No matter the size of input string data, the length of its output is always fixed

HASH TREE/MERKLE TREE

- It is a data set with a tree structure. Each leaf node is denoted by the hash value of the data node, and each non-leaf node is denoted by the hash value of its child node.
- Hash tree allows to efficiently and securely verify the contents of large data structures.



PUBLIC KEY CRYPTOGRAPHY

- Public key is the address on the Blockchain
- This is a generated random number.
- Any transaction happens through Blockchain happens through Public Key to identify the sender and receiver
- Private key is like password to access the data
- Public key is associated with Private key
- Only the person with the Private key can decrypt the data
- Digital Signature is the combination of Authentication and Non-repudiation

CONSENSUS

- Consensus is the agreement between the nodes in Blockchain network which operates without trust between parties.
- Consensus are not owned and controlled any central authority rather it's the nodes across the world.
- State or value of block is agreed by multiple nodes in Blockchain network.
- The choice of Consensus algorithm depends on Blockchain type you choose
- Consensus Mechanism is the steps taken to agree upon block state.
- Consensus will run even when some node are down

CONSENSUS MECHANISM ALGORITHMS

- Some Consensus Mechanism algorithms
  - Proof of Work
  - Proof of Stake
  - Leased Proof of Stake
  - Delegated Proof of Stake
  - Proof of Importance
  - Proof of Elapsed Time
  - Proof of Deposit
  - Federated Consensus

TRANSACTIONS IN THE BLOCKCHAIN

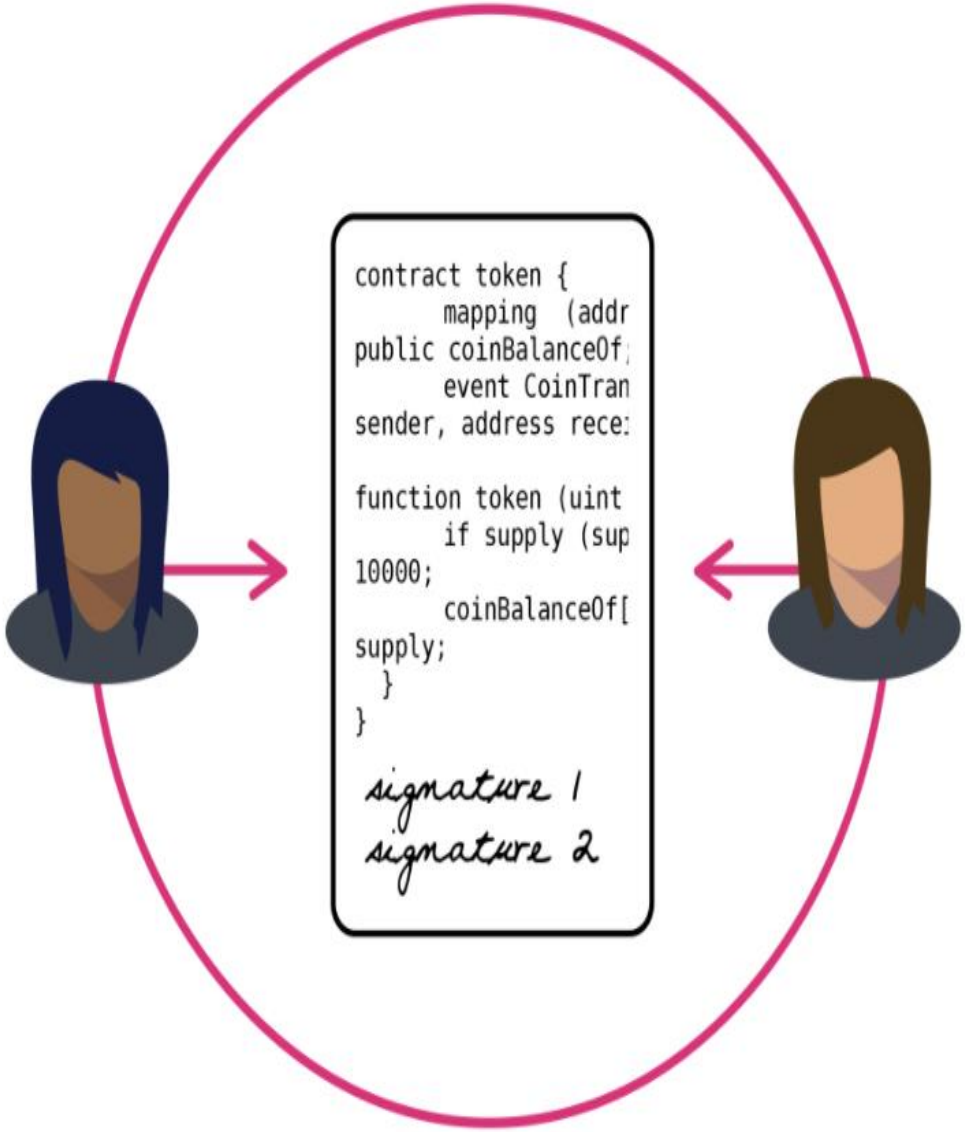
- Each transaction is digitally signed with cryptography
- Atomic, full operation run or not at all
- Run independently
- Inspect able
- Immortal
- Each transaction has cost associated Each transaction creates block into Blockchain

MINING

- Mining is the process of validating the transactions and adding new block to the Blockchain network.
- Broadcast to other nodes in the network who has the copy of database
- All the nodes should agree about its state to add transaction to nodes.
- Miner who solves the puzzle, gets the reward as crypto currency or fee
- In Bitcoin world it uses PoW algorithm

SMART CONTRACT

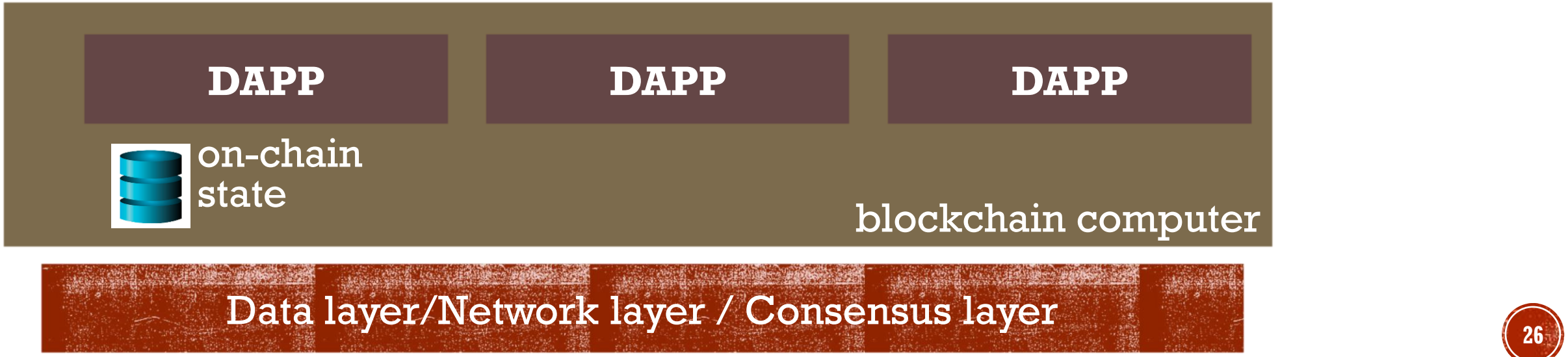
- Agreements are written as Smart Contracts.
- Smart Contracts are business logic
- Transactions are validated against Smart Contract
- Digitized and codified rules of transaction between accounts
- In Ethereum world smart contracts are writt in language called Solidity and deployed int Ethereum network
- You can write your smart contract online through Remix



APPLICATION LAYER

Decentralized applications (DAPPs):

- Run on blockchain: code and state are written on chain
- Accept Tx from users ⇒ state transitions are recorded on chain



STRUCTURE OF THE BLOCKCHAIN ARCHITECTURE

Application and presentation layer

Smart contracts · Chaincode · DApps · UI

Consensus layer

PoW · PoS · DPoS · PoET · PBFT

Network layer

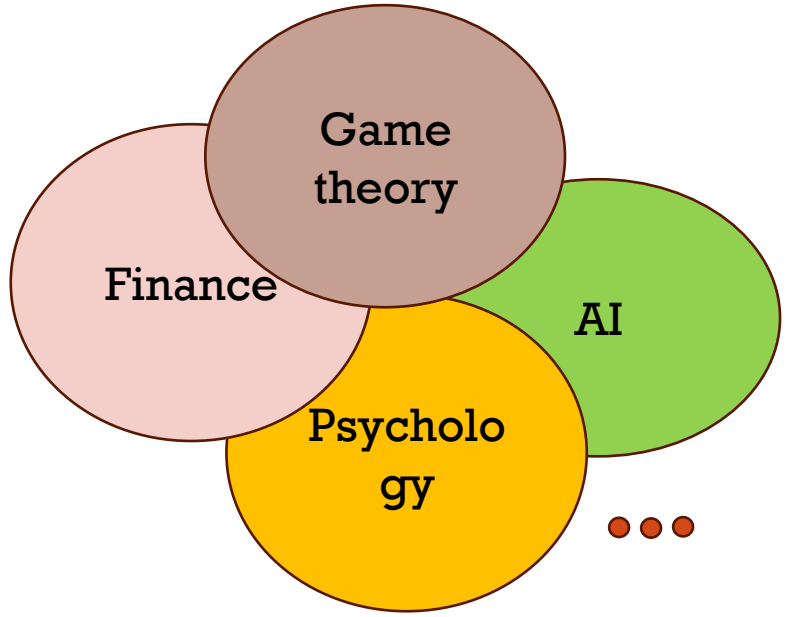
Peer-to-Peer (p2p)

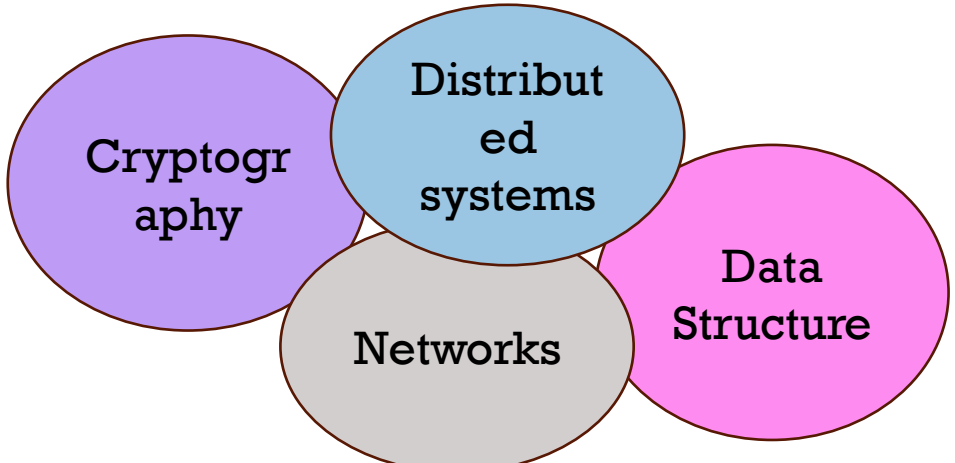
Data layer

Digital signature · Hash · Merkel tree · Transaction

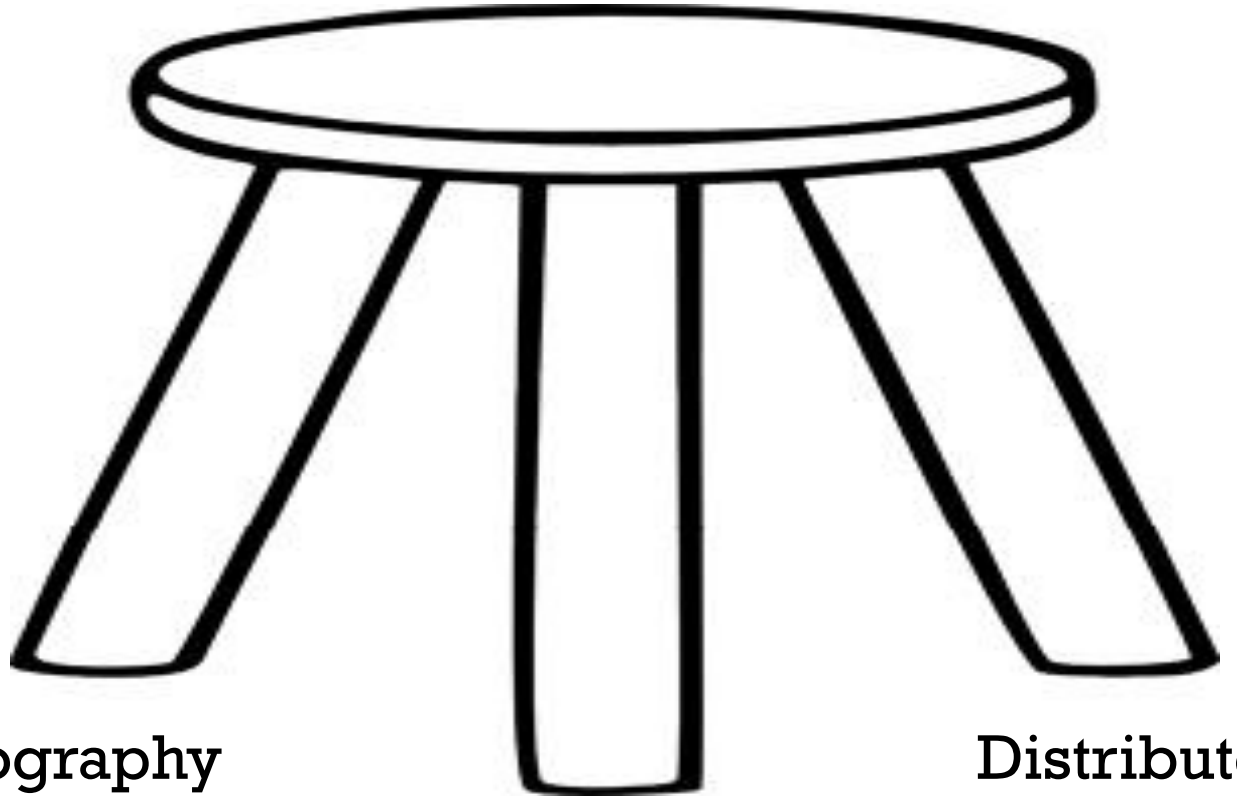
Hardware / Infrastructure layer

Virtual machine · Containers · Services · Messaging





THIS COURSE



Cryptography

Distributed systems

Application and presentation