JULY 7
2024

BLOCKCHAIN TECHNOLOGY

PDSC
PULCHOWK

BLOCKCHAIN
TECHNOLOGY

What is money?

Story of Money

Barter System

Commodity money

Metal coins

Paper notes

Fiat currencies

- no intrinsic value
- worthless paper used as medium of exchange
- backed by nothing

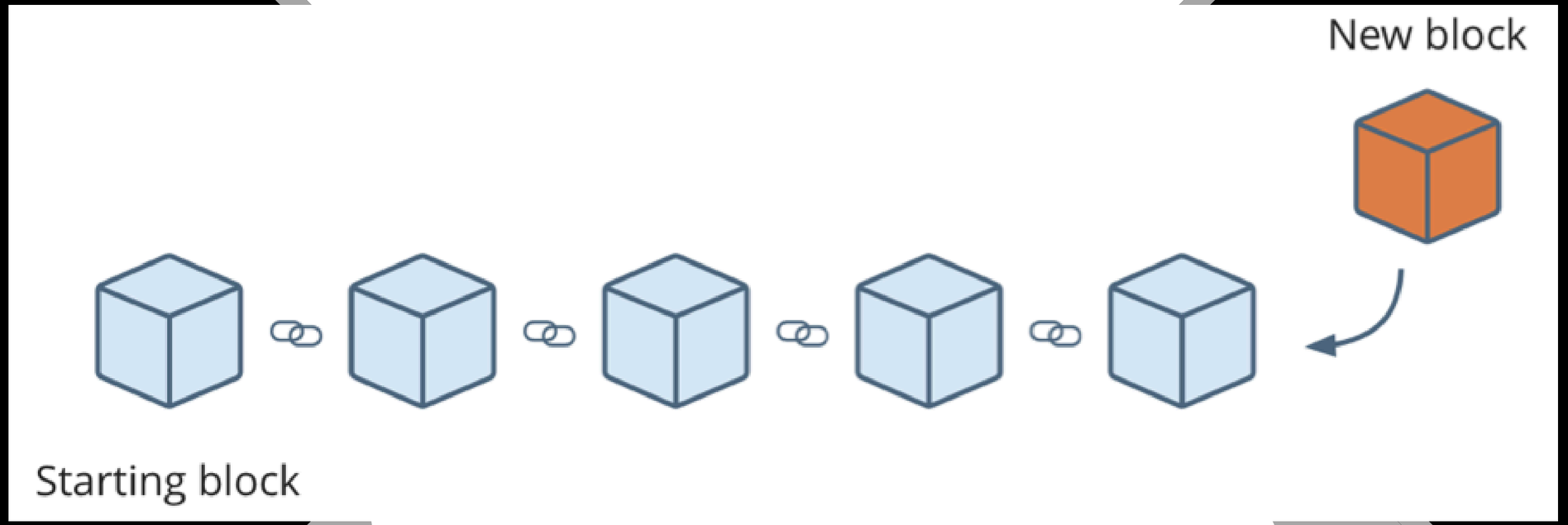
Money

- Medium of exchange
- Store of value
- Portable
- Divisible
- Unit of account
- Fungible

Bitcoin

- decentralized
- peer to peer electronic cash system
- trustless

Blockchain



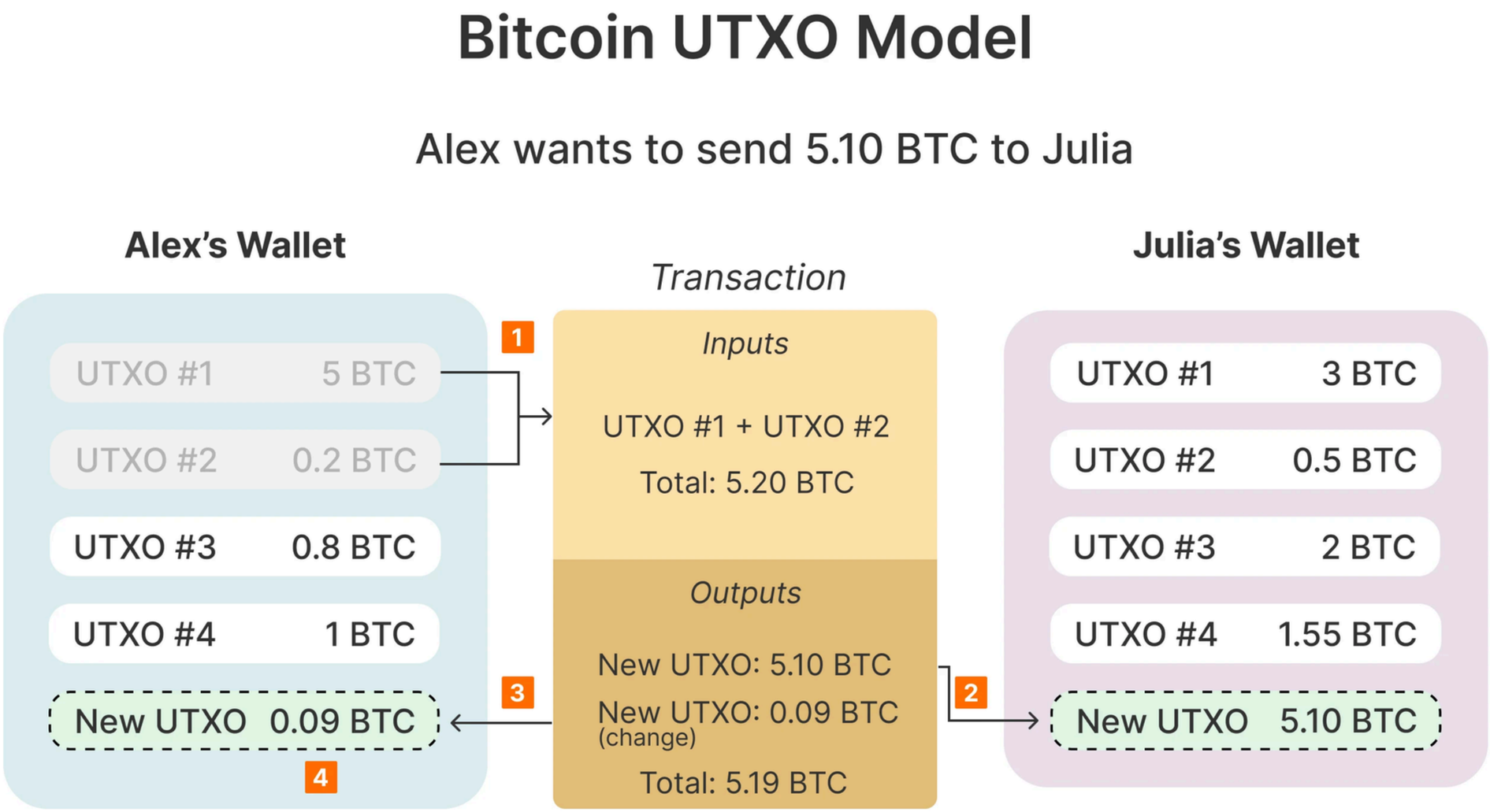

22:03
Back
Share payment request
Keep the app open until the payment is received.
Share
Copy

BLOCKCHAIN
TECHNOLOGY

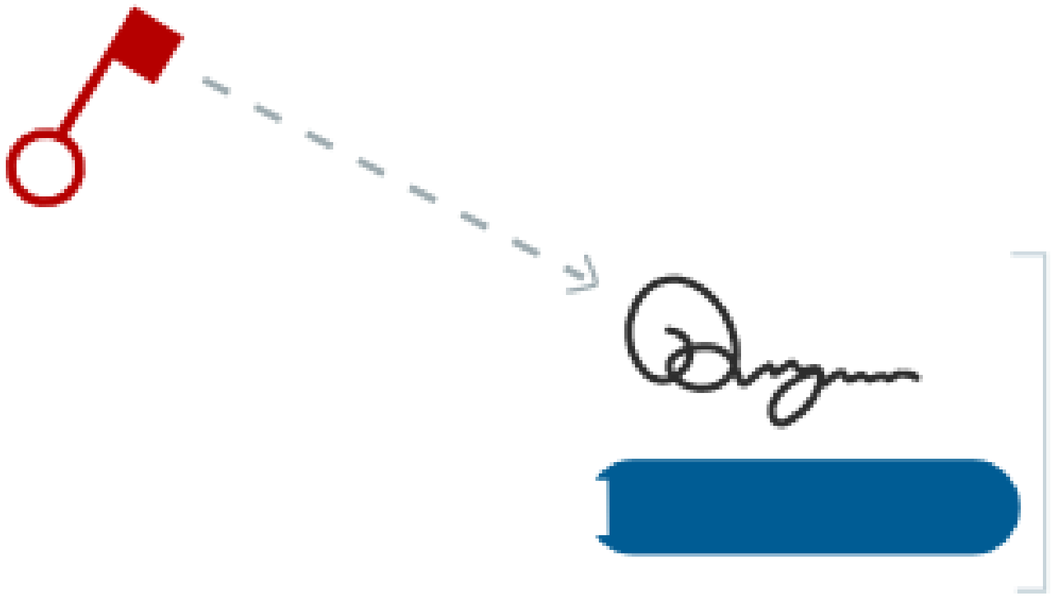
Wallet

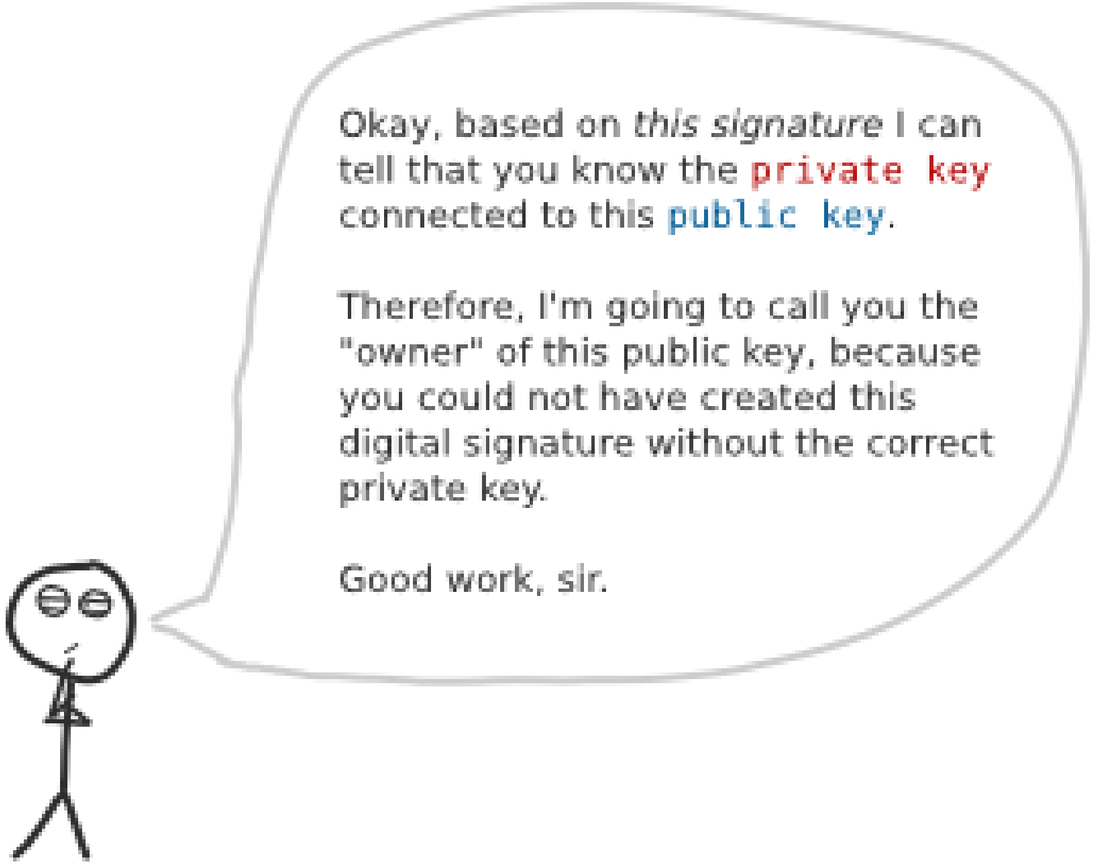
private key

Bitcoin UTXO Model

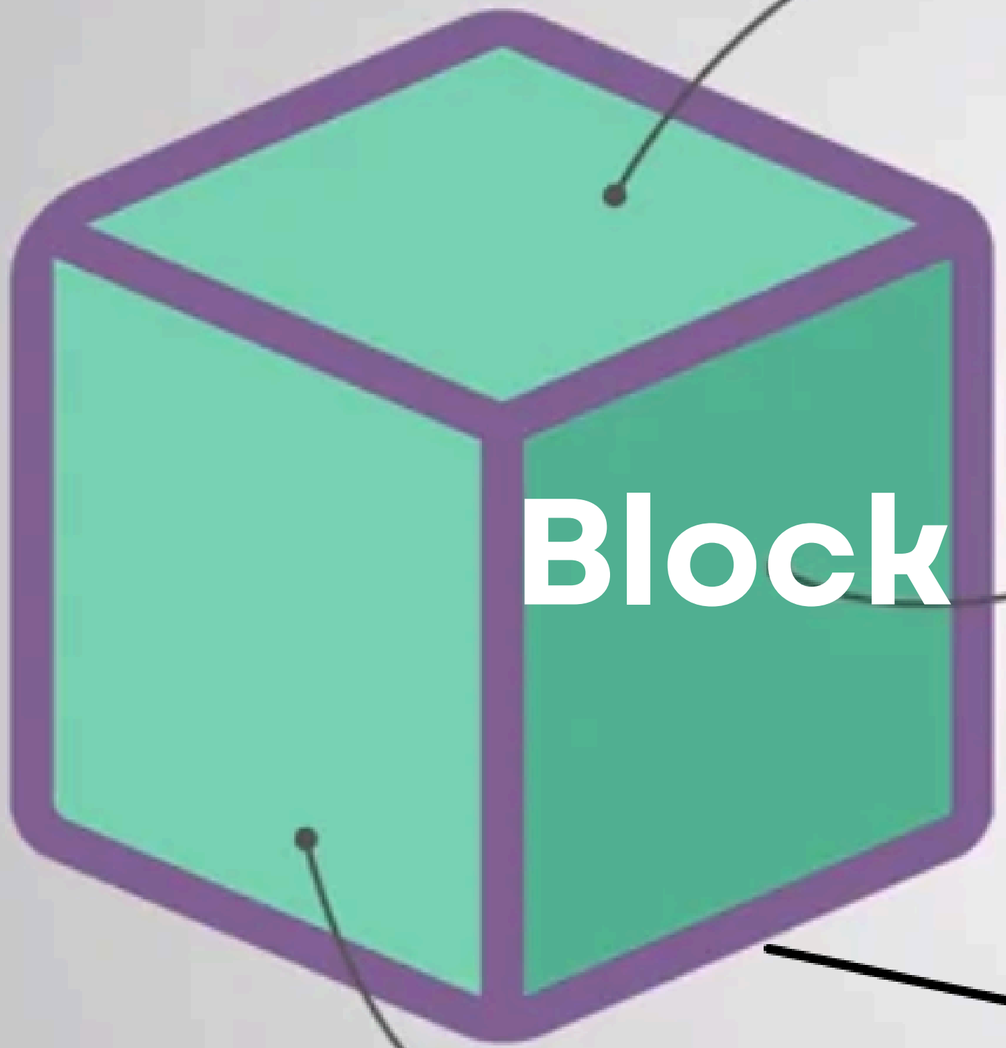


Digital Signature





BLOCKCHAIN
TECHNOLOGY



Data

Nonce

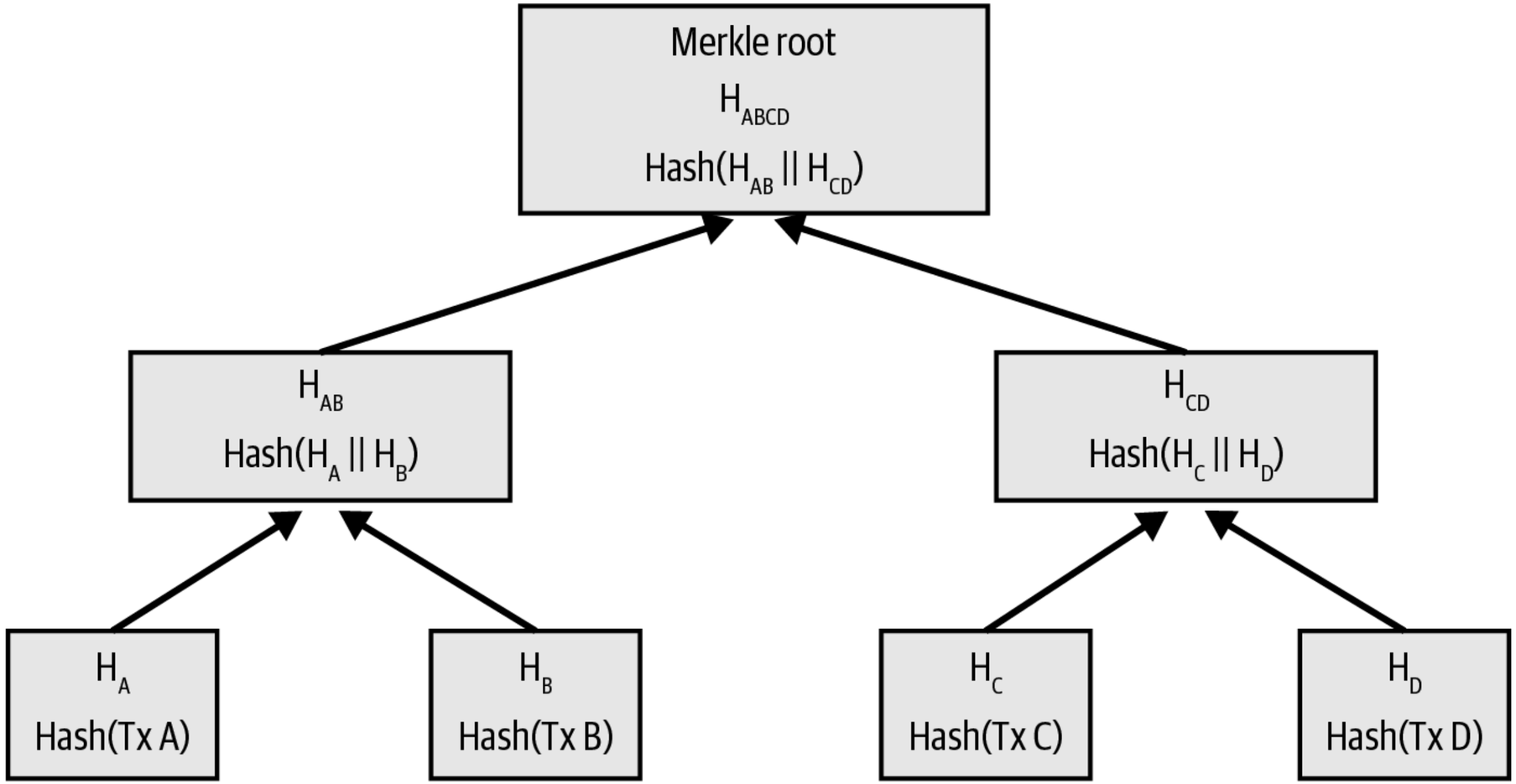
Hash of previous block

Target hash

Hashing

INPUT DATA	HASH OUTPUT (SHA-256)
My name is Toby	cacb5418163039b016be9746818a2926f68fd1e4bad1b04f6791f6aabb5e8c52
My name is Tony	9cd2444dc56929bdb97123add1f007643effa88bf1ed061eee1eead4e15ac7f9
My name is Toby and this is my project	9abbaa0c54fcd028ac51bede2608d06e8d3a026784e34adfac14fadd143d212c

Merkle Tree

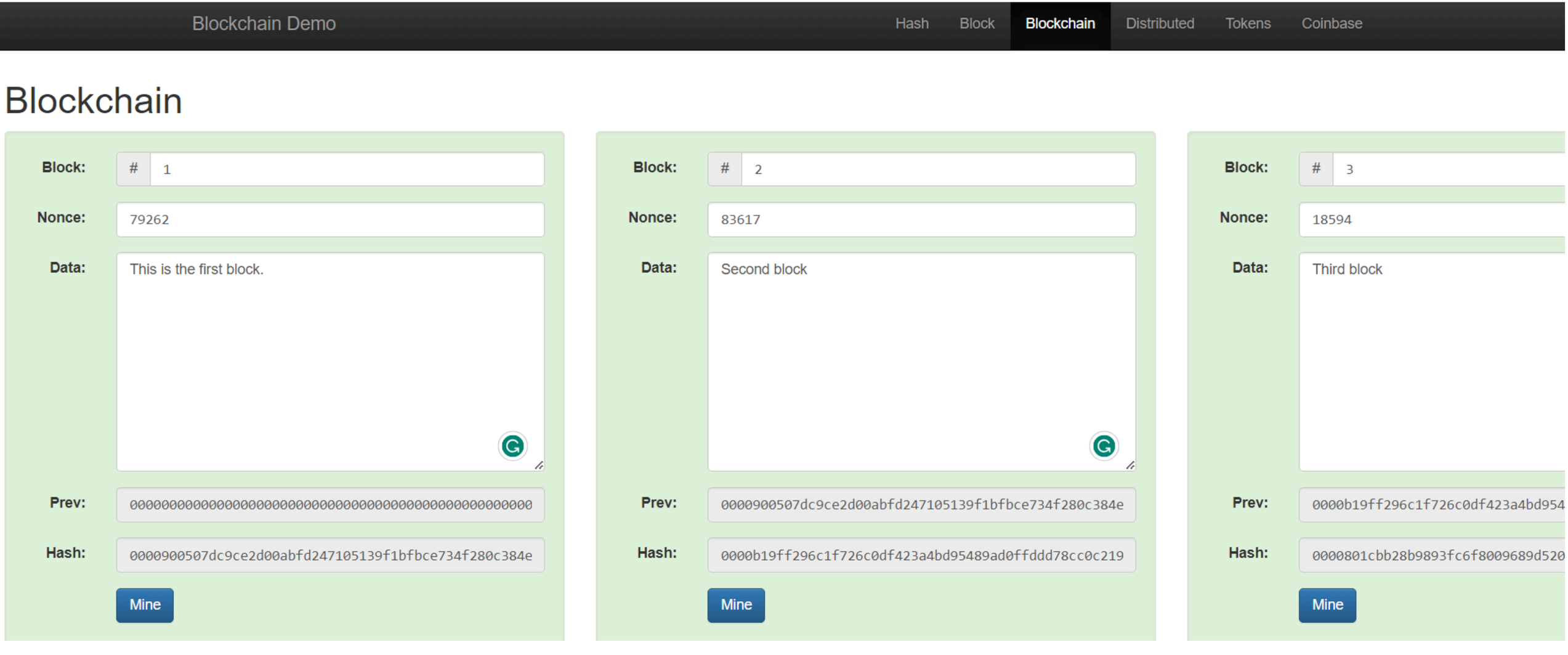

Merkle root
H_{ABCD}
$Hash(H_{AB} || H_{CD})$
H_{AB}
$Hash(H_A || H_B)$
H_{CD}
$Hash(H_C || H_D)$
H_A
Hash(Tx A)
H_B
Hash(Tx B)
H_C
Hash(Tx C)
H_D
Hash(Tx D)

BLOCKCHAIN
TECHNOLOGY

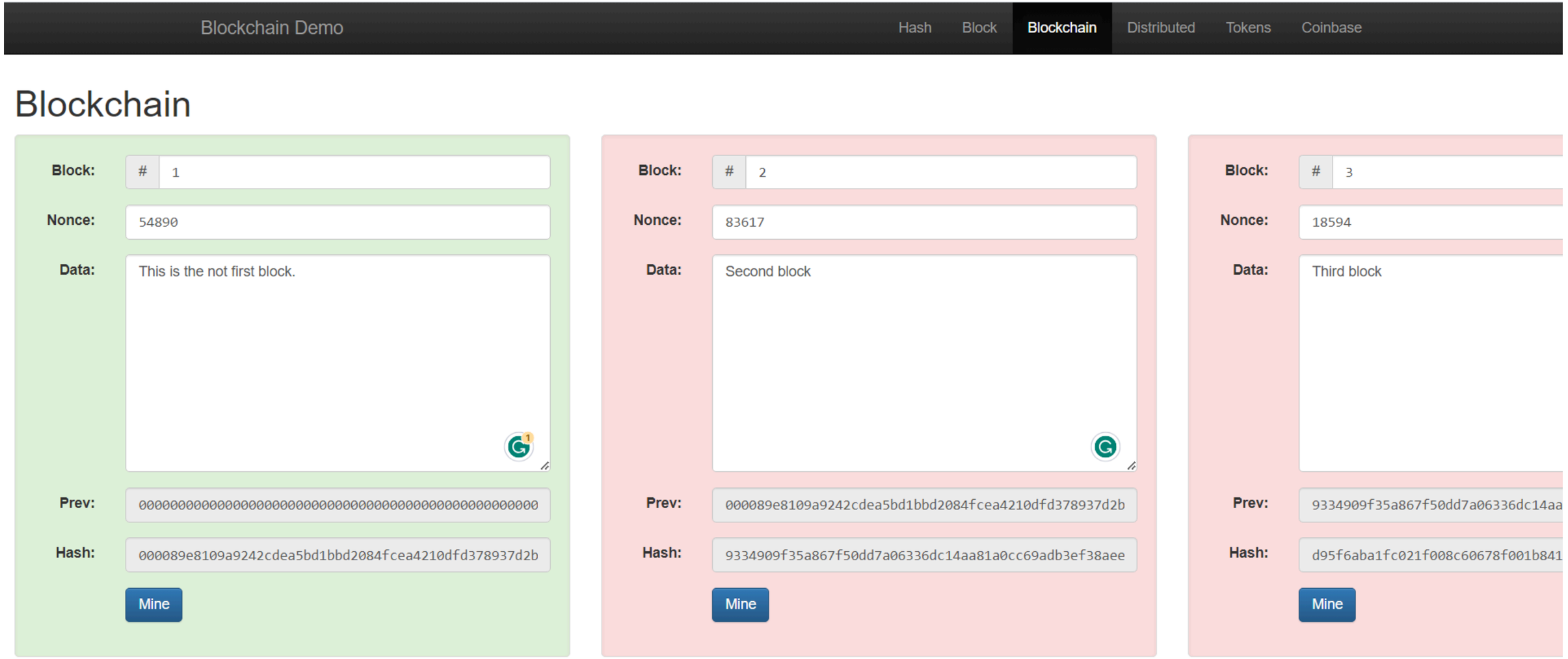
Bitcoin mining

- process of verifying transactions
- solving mathematical puzzles
- rewarded with new bitcoin

Nonce - hit and trial



Immutability



BLOCKCHAIN

TECHNOLOGY

Peer A

Block: # 1

Nonce: 11316

Data:

Prev: 0000000000000000000000000000000000000000000000000000000000000000

Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf

Mine

Block: # 2

Nonce: 35230

Data:

Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf

Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd043c19

Mine

Distributed

Peer B

Block: # 1

Nonce: 11316

Data:

Prev: 0000000000000000000000000000000000000000000000000000000000000000

Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf

Mine

Block: # 2

Nonce: 35230

Data:

Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf

Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd043c19

Mine

Network effect

- social media sites, languages, religion
- belief

BLOCKCHAIN
TECHNOLOGY

Network effect

BLOCKCHAIN
TECHNOLOGY

Ethereum

- Vitalik Buterin
- Smart Contracts
- Dapps

BLOCKCHAIN
TECHNOLOGY

Bitcoin and Ethereum

Why was Ethereum an important addition to the blockchain technology?

Proof of work....

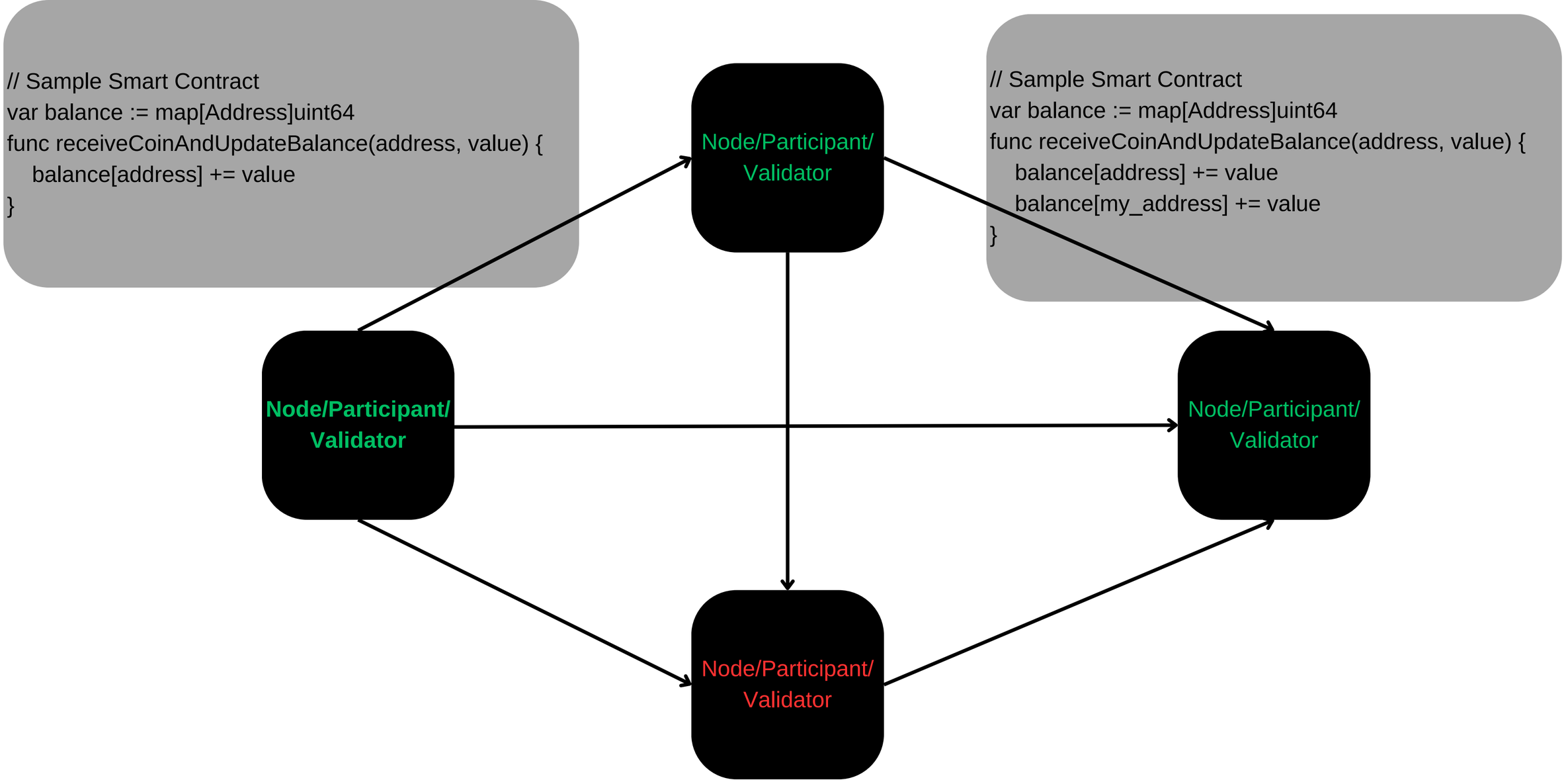
Proof of stake??

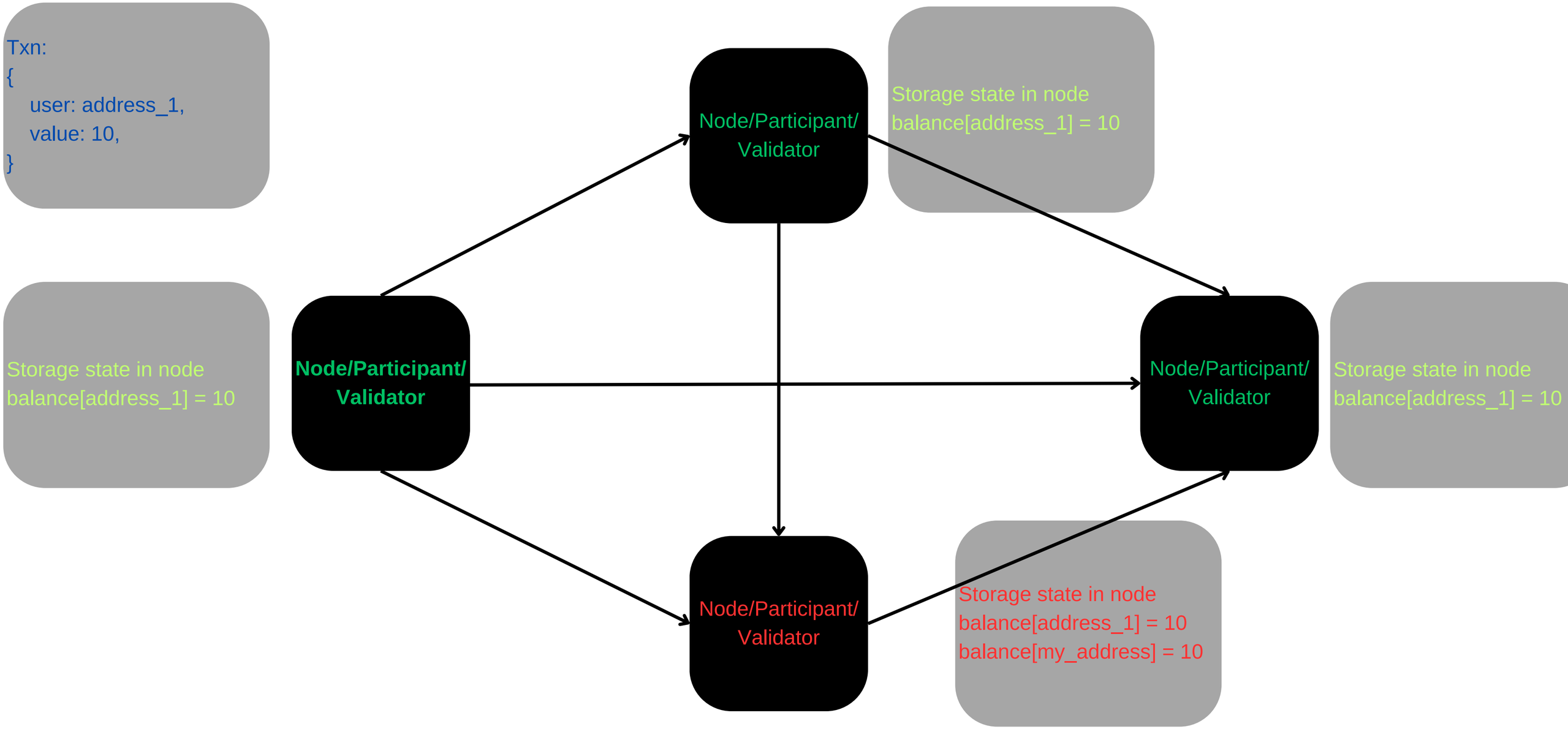
POS 101

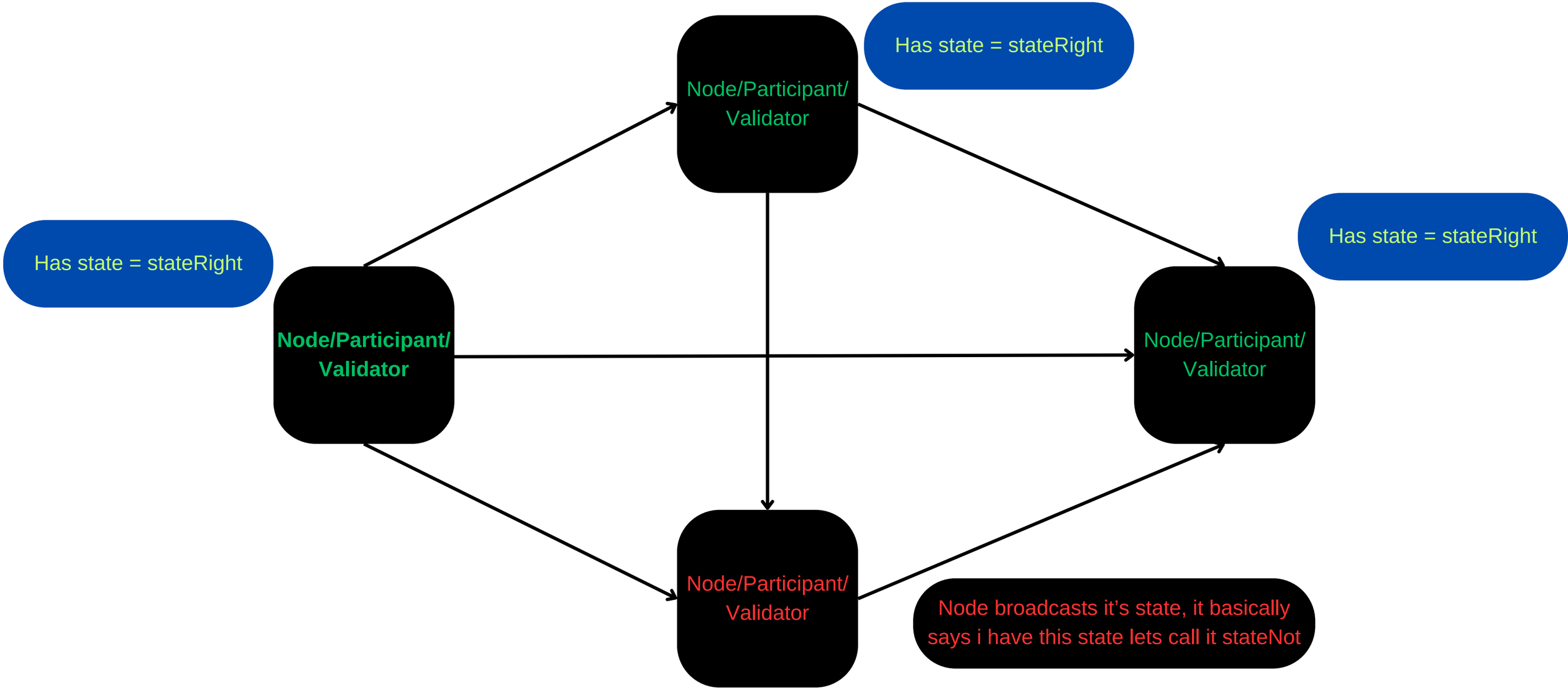
- Participants of the network stake ETH tokens in the network to ensure the security of the chain
- Network chooses a participant to be the block producer every time at random according to the stake of the participant in the network

Proof of stake Pros

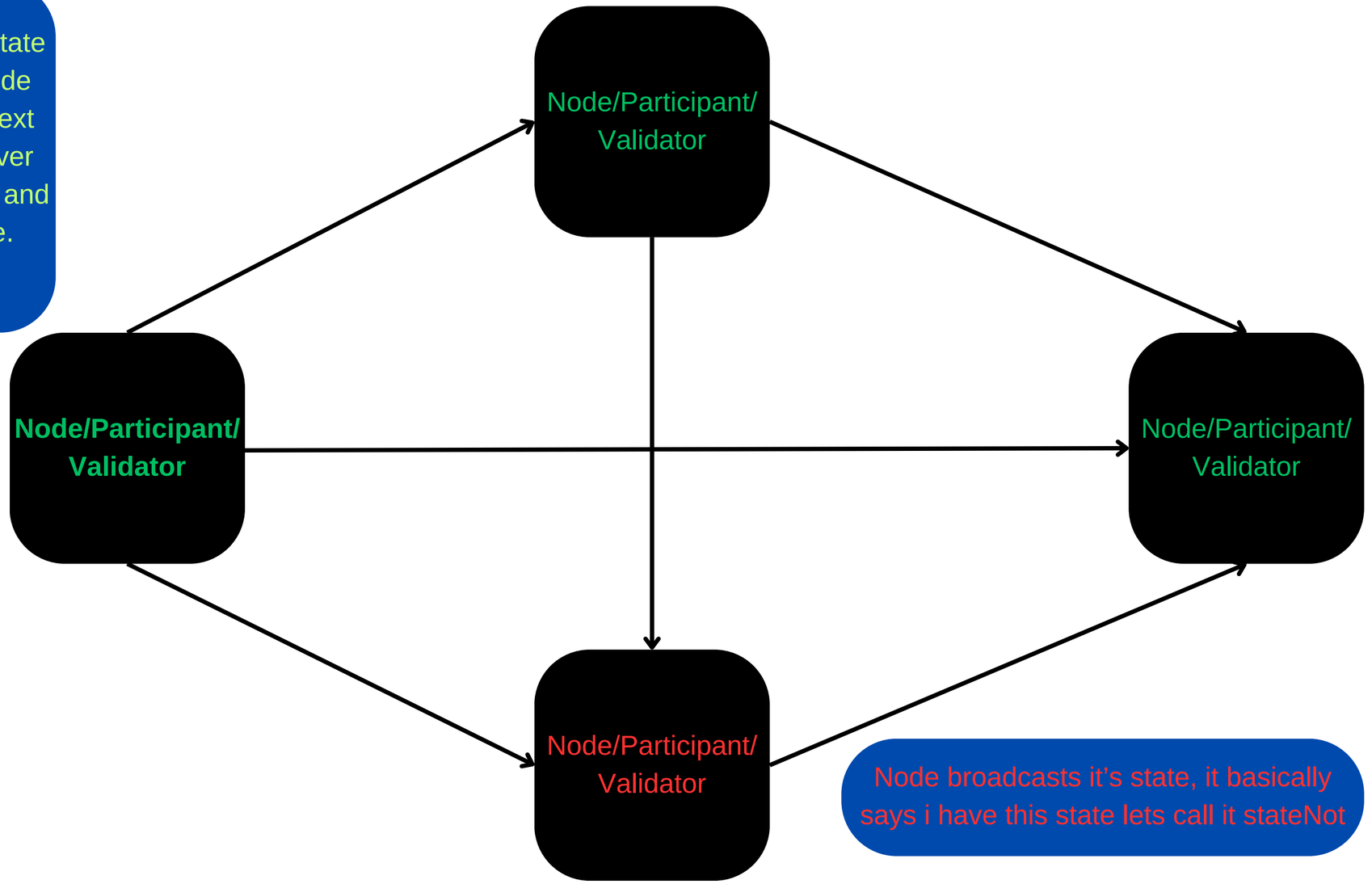
Cheap to run
No need for big hardwares
like GPUs
Environmental friendly


// Sample Smart Contract
var balance := map[Address]uint64
func receiveCoinAndUpdateBalance(address, value) {
balance[address] += value
}
Node/Participant/
Validator
// Sample Smart Contract
var balance := map[Address]uint64
func receiveCoinAndUpdateBalance(address, value) {
balance[address] += value
balance[my_address] += value
}
Node/Participant/
Validator
Node/Participant/
Validator
Node/Participant/
Validator


Txn:
{
user: address_1,
value: 10,
}
Node/Participant/
Validator
Storage state in node
balance[address_1] = 10
Storage state in node
balance[address_1] = 10
Node/Participant/
Validator
Node/Participant/
Validator
Storage state in node
balance[address_1] = 10
Node/Participant/
Validator
Storage state in node
balance[address_1] = 10
balance[my_address] = 10


Has state = stateRight
Node/Participant/
Validator
Has state = stateRight
Has state = stateRight
Node/Participant/
Validator
Node/Participant/
Validator
Node/Participant/
Validator
Node broadcasts it’s state, it basically
says i have this state lets call it stateNot

Quickly dismisses the state update of the faulty node and moves on to the next block. So the block never gets added to the chain and the network is secure. YAY!!



Node broadcasts it's state, it basically says i have this state lets call it stateNot

BLOCKCHAIN
TECHNOLOGY

Ethereum

Smart Contracts

Programmability in blockchain

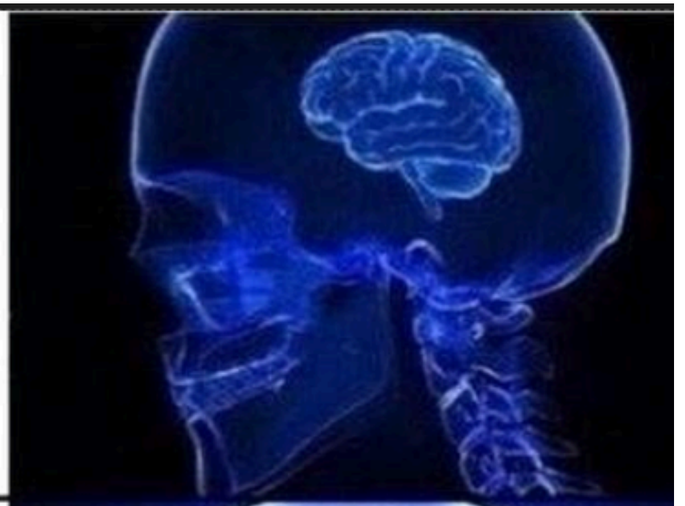
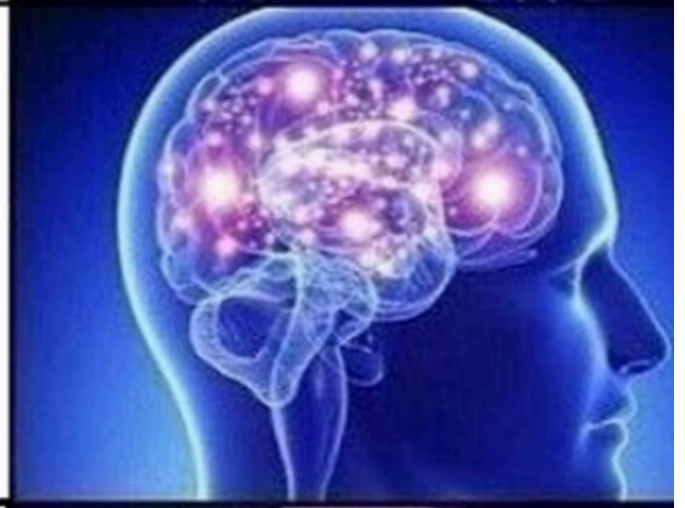
BLOCKCHAIN
TECHNOLOGY

Applications

- Transparency
- Verification
- Intermediary

Applications

- DeFi
- Decentralized Identity
- Gaming and NFTs
- Insurance
- Voting

Work for money	
Have money work for you	
Create money