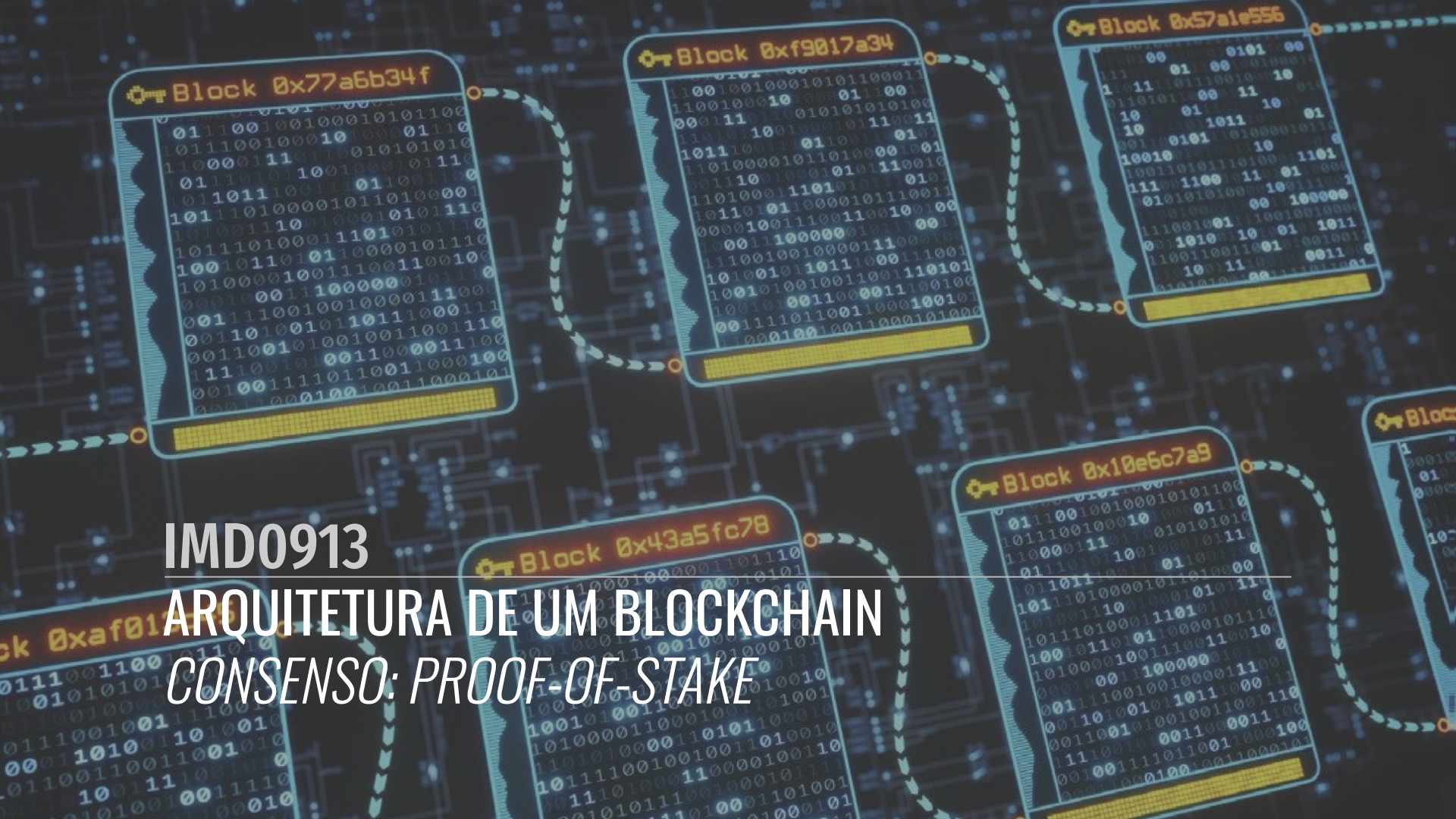
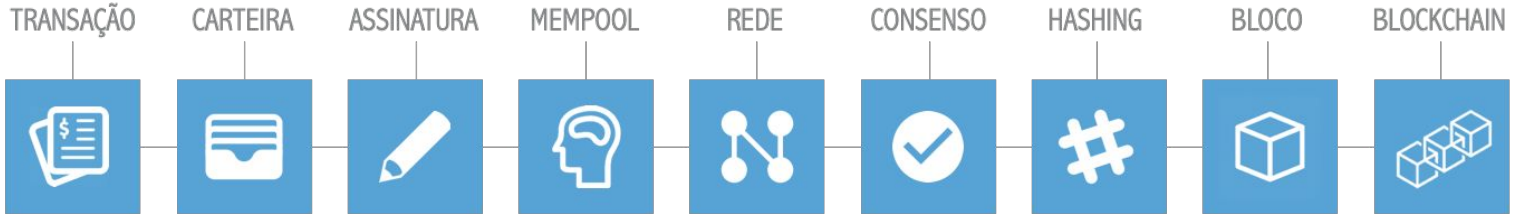


IMD0913

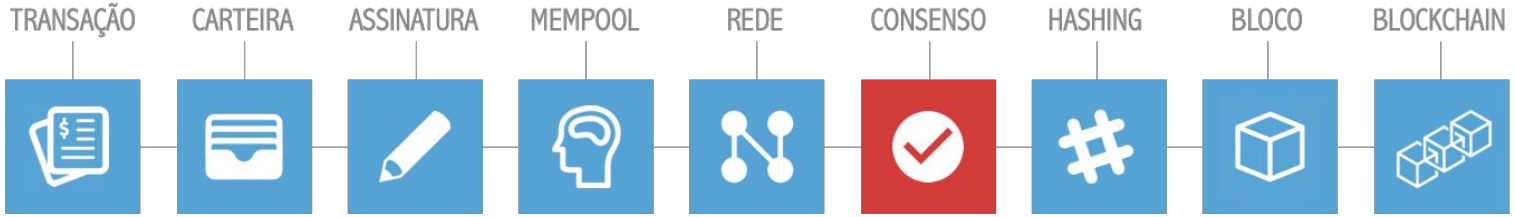
ARQUITETURA DE UM BLOCKCHAIN

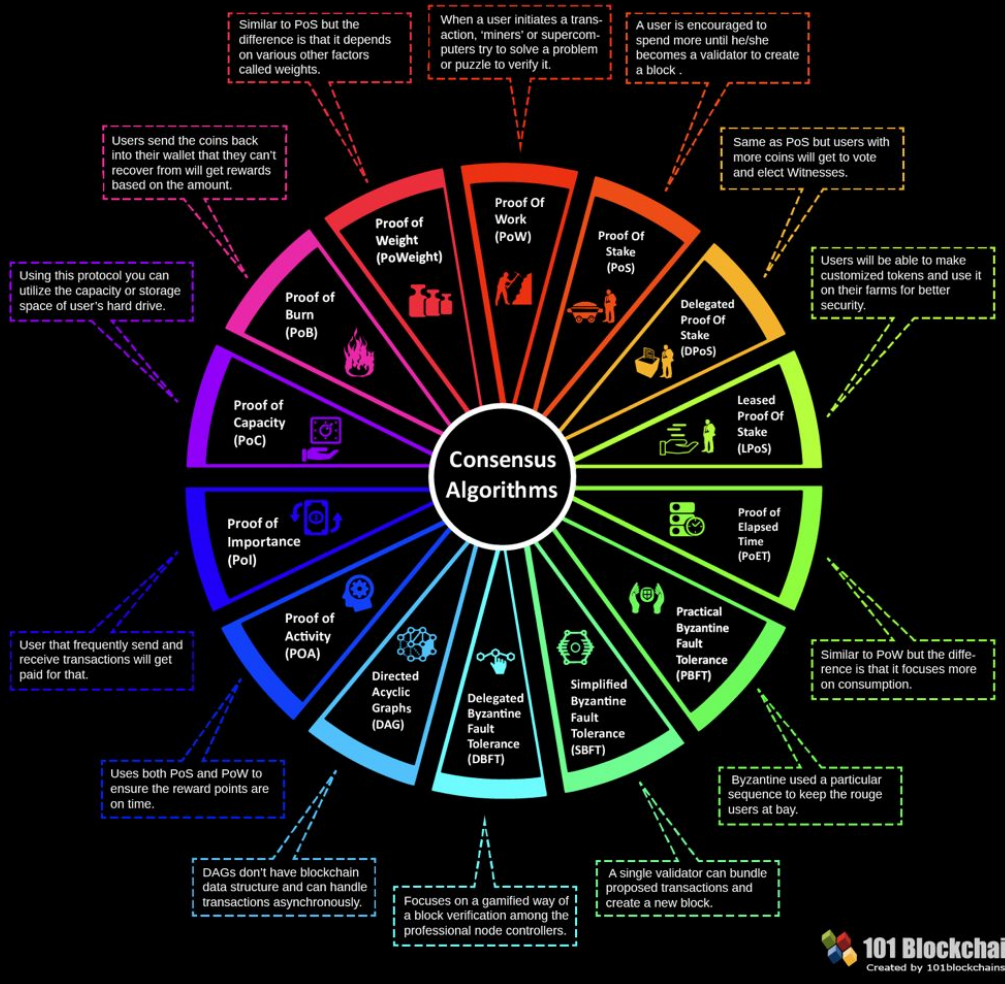
CONSENSO: PROOF-OF-STAKE

ARQUITETURA DE UM **BLOCKCHAIN**



ARQUITETURA DE UM **BLOCKCHAIN**




Consensus Algorithms
Proof of Work (PoW)
When a user initiates a transaction, 'miners' or supercomputers try to solve a problem or puzzle to verify it.
Proof Of Stake (PoS)
A user is encouraged to spend more until he/she becomes a validator to create a block .
Delegated Proof Of Stake (DPoS)
Same as PoS but users with more coins will get to vote and elect Witnesses.
Leased Proof Of Stake (LPoS)
Users will be able to make customized tokens and use it on their farms for better security.
Proof of Elapsed Time (PoET)
Proof of Weight (PoWeight)
Similar to PoS but the difference is that it depends on various other factors called weights.
Proof of Burn (PoB)
Users send the coins back into their wallet that they can't recover from will get rewards based on the amount.
Proof of Capacity (PoC)
Using this protocol you can utilize the capacity or storage space of user's hard drive.
Proof of Importance (PoI)
Practical Byzantine Fault Tolerance (PBFT)
Similar to PoW but the difference is that it focuses more on consumption.
Proof of Activity (POA)
User that frequently send and receive transactions will get paid for that.
Simplified Byzantine Fault Tolerance (SBFT)
Byzantine used a particular sequence to keep the rouge users at bay.
Directed Acyclic Graphs (DAG)
Uses both PoS and PoW to ensure the reward points are on time.
Delegated Byzantine Fault Tolerance (DBFT)
DAGs don't have blockchain data structure and can handle transactions asynchronously.
Focuses on a gamified way of a block verification among the professional node controllers.
A single validator can bundle proposed transactions and create a new block.
101 Blockchains
Created by 101blockchains.com

Proof-of-stake

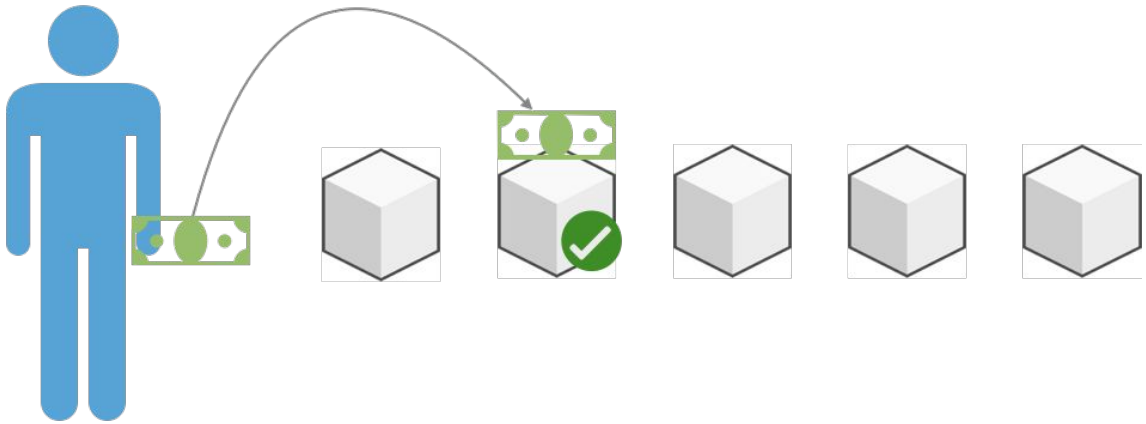
Sistema no qual os nós "apostam" suas moedas para terem chances de serem o próximo validador, propondo um novo bloco a ser inserido no *blockchain*.

Proof-of-stake

No **PoS** não existem mineradores, e sim **validadores**

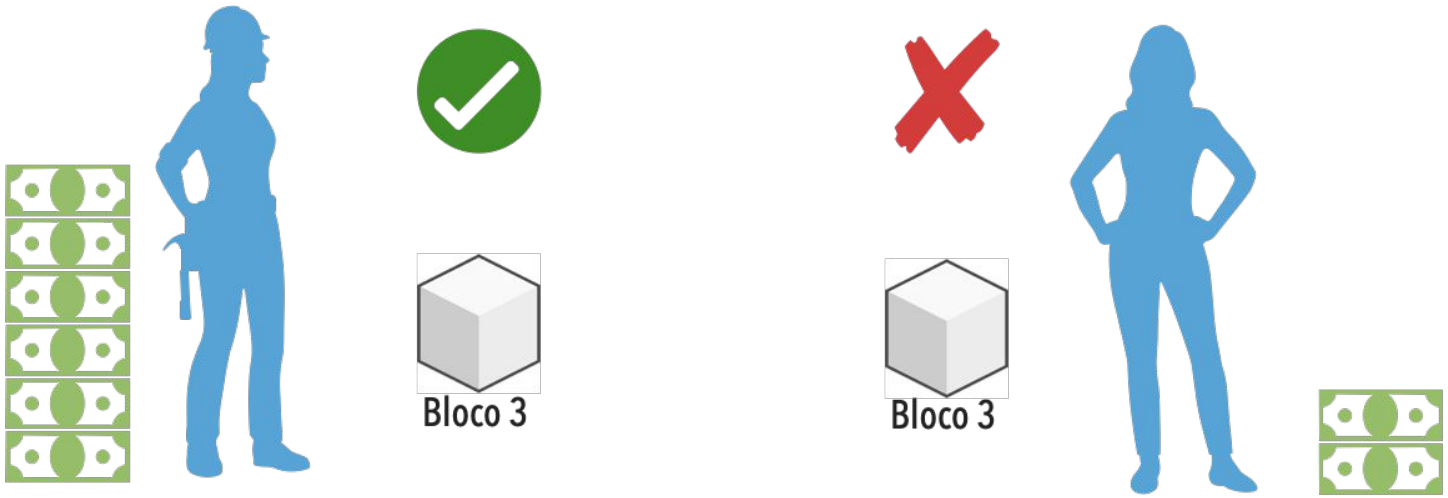
Ou seja, não é necessário investir em recursos computacionais

O validador "aposta" seu dinheiro, e se sorteado pode propor um bloco



Proof-of-stake

Maior o *stake*, maiores as chances de propor um próximo bloco!



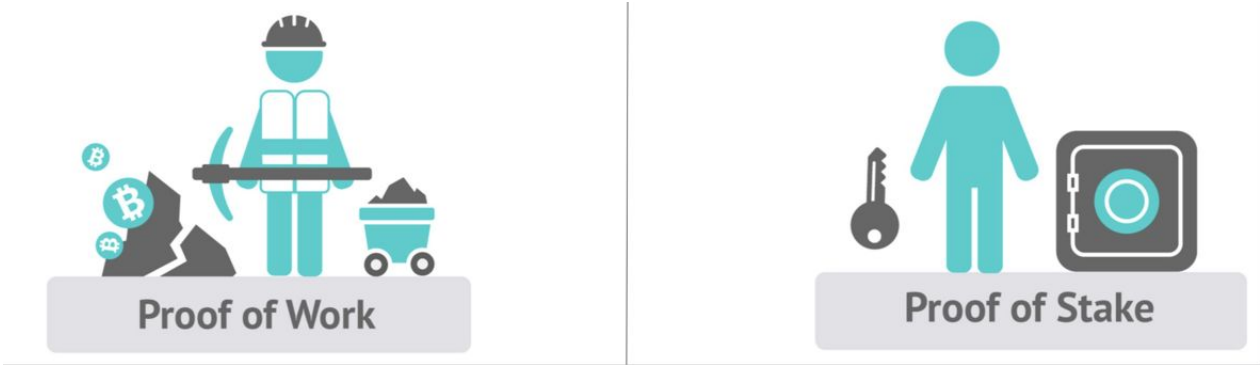
Proof-of-stake

Nós realizam um *staking* para participar do processo de consenso

- Moedas apostadas não podem ser gastas
- Poder de voto proporcional a quanto eles apostam
- ***Slashing***: moedas destruídas por comportamento indevido

Ideia: Alguém que investe na rede se comportará para seu melhor interesse

PoW vs PoS



Mineradores tem poder de voto proporcional ao seu poder computacional

Validadores tem poder de voto proporcional ao seu stake apostado

Proof-of-stake: Ethereum

https://ethereum.org/pt/staking/

Outros mecanismos de consenso...

Delegated Proof of Stake (DPoS): Lisk (LSK), EOS.IO (EOS), Steem (STEEM), BitShares (BTS), Ark (ARK)

Proof of Activity (PoA): Decred (DCR), Espers (ESP)

Proof of Authority (PoA): JPMorgan (JPMCoin), VeChain (VET)

Proof of Burn (PoB): Slimcoin (SLM), Counterparty (XCP), Factom (FCT)

Proof of Capacity/Proof of Space (PoC/PoSpace): Signum (SIGNA), Storj (STORJ), Chia (XCH).

Proof of Elapsed Time (PoET): Hyperledger Sawtooth

Proof of Importance (PoI): NEM Network (XEM)