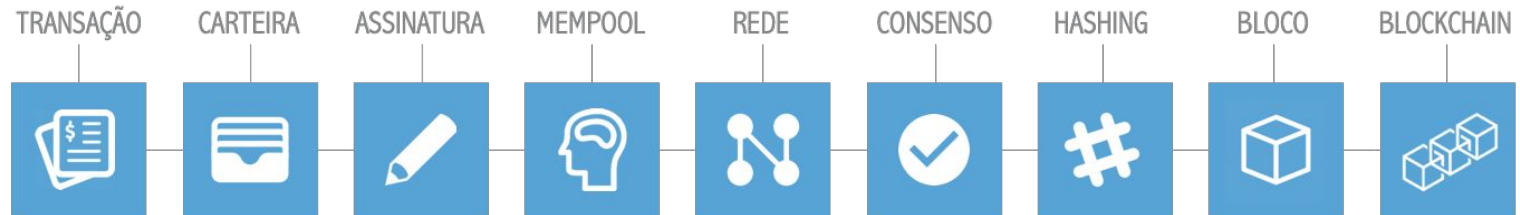


IMD0913

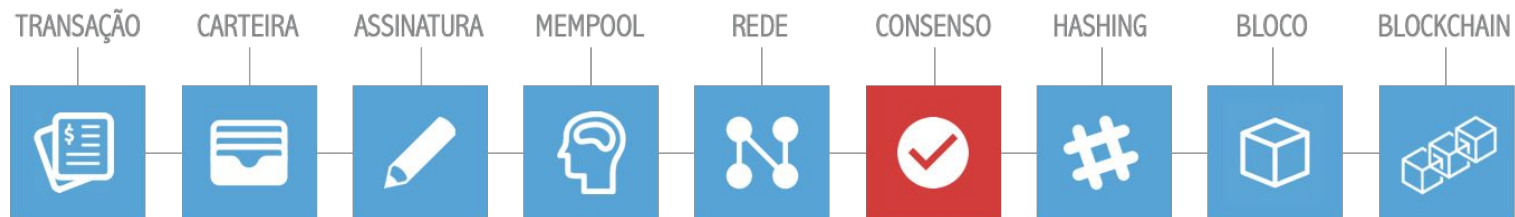
ARQUITETURA DE UM BLOCKCHAIN

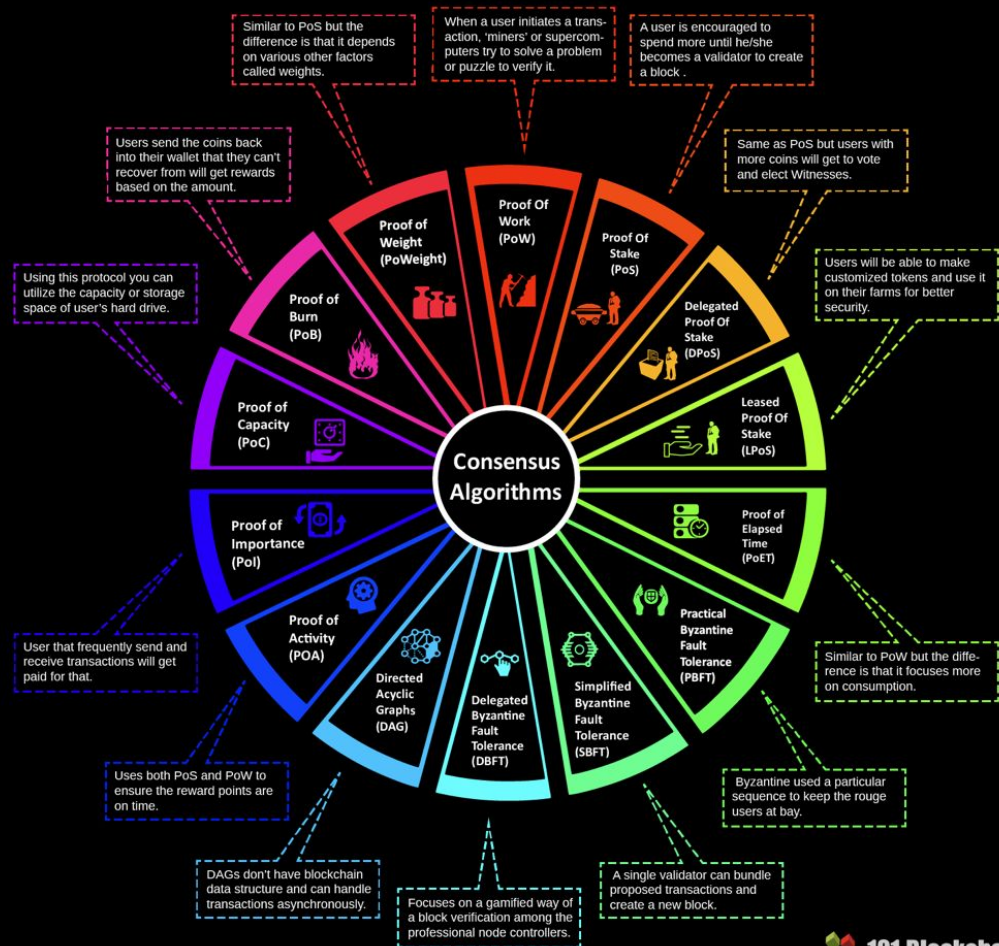
CONSENSO: PROOF-OF-STAKE

ARQUITETURA DE UM **BLOCKCHAIN**



ARQUITETURA DE UM **BLOCKCHAIN**





Proof-of-stake

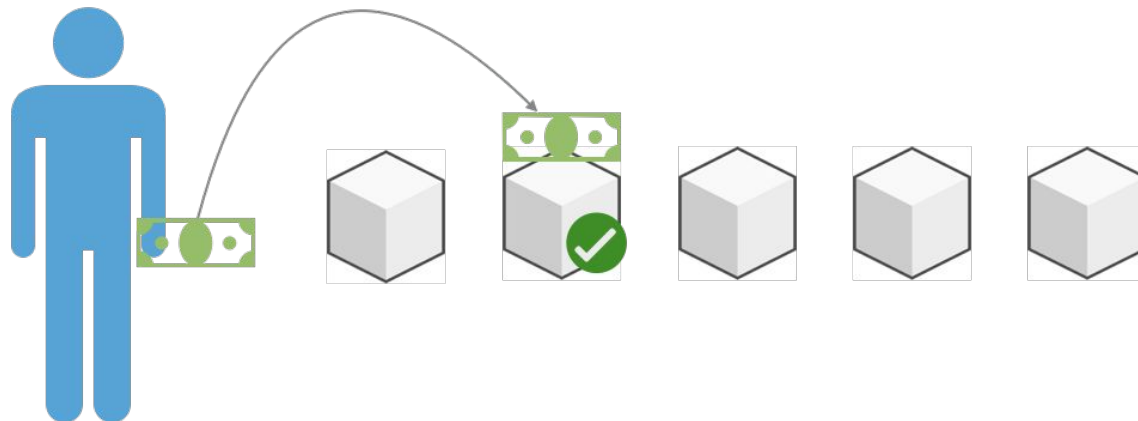
Sistema no qual os nós "apostam" suas moedas para terem chances de serem o próximo validador, propondo um novo bloco a ser inserido no *blockchain*.

Proof-of-stake

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

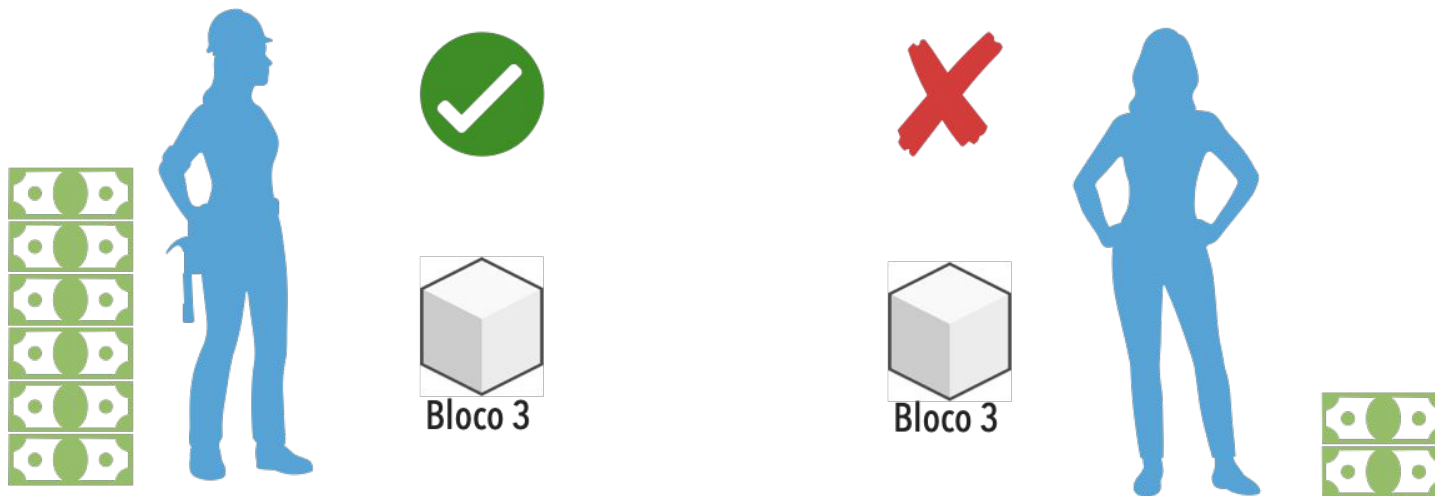
Ou seja, não é necessário investir em recursos computacionais

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/>

