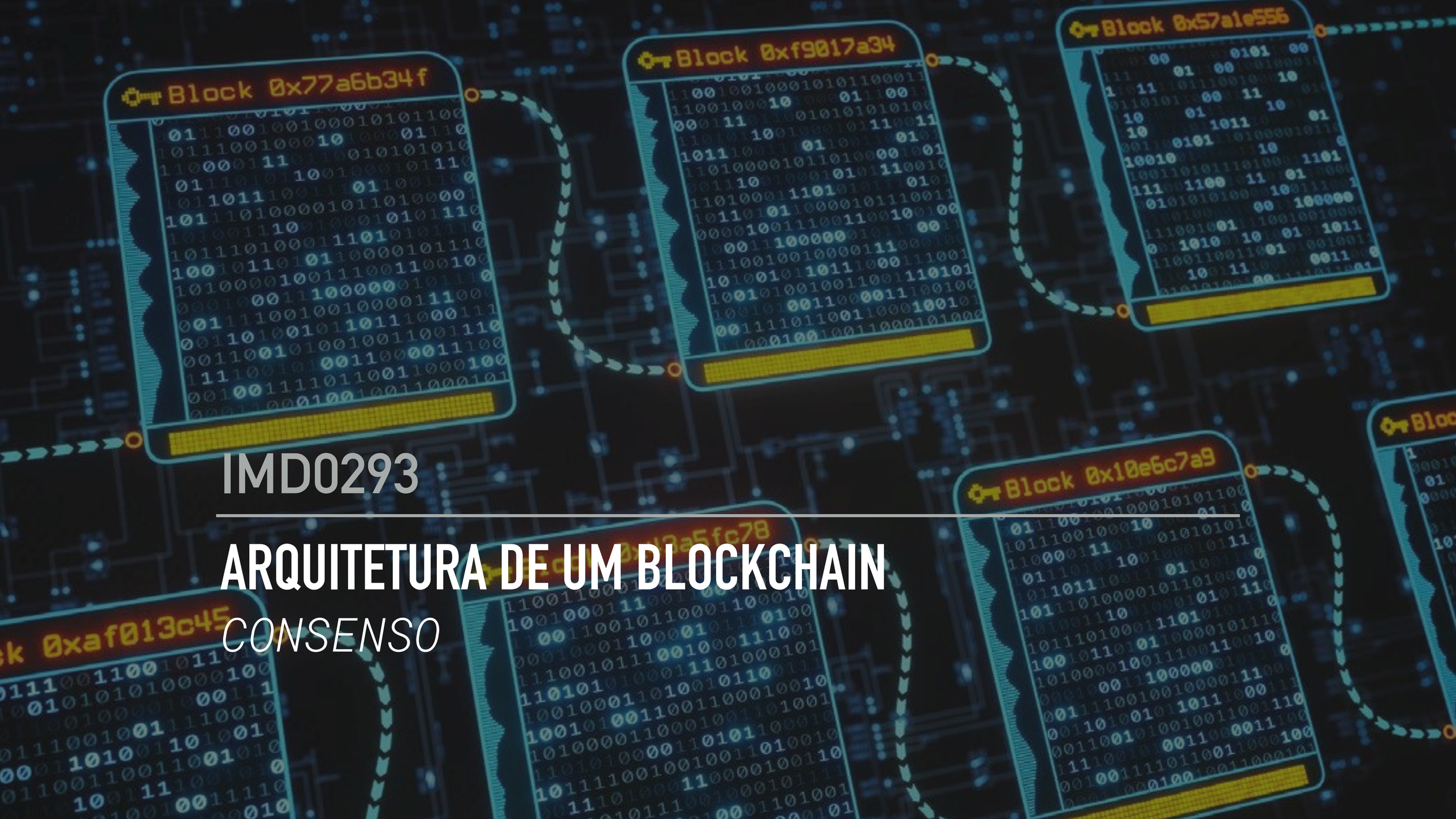
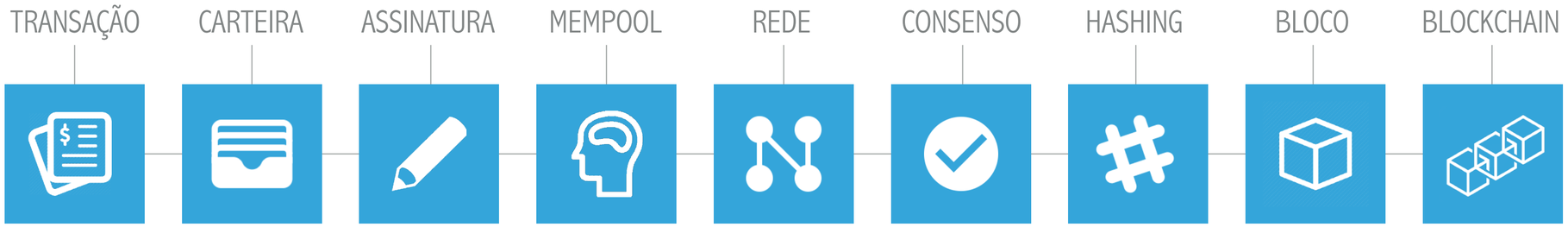


IMD0293

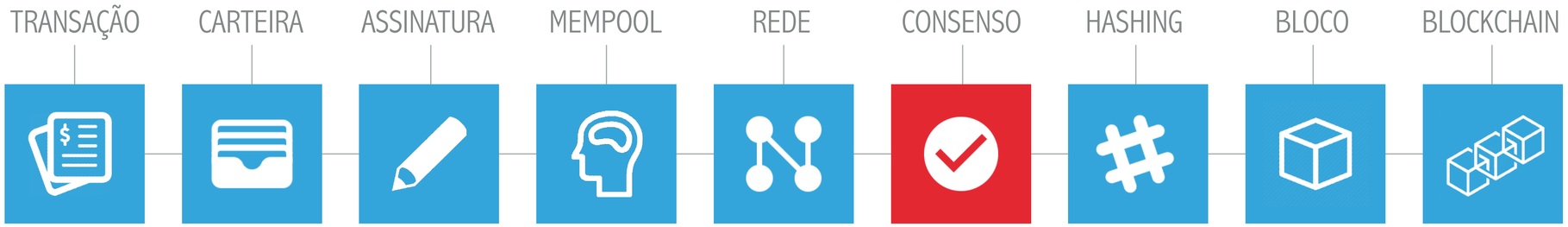
ARQUITETURA DE UM BLOCKCHAIN

CONSENSO

ARQUITETURA DE UM **BLOCKCHAIN**



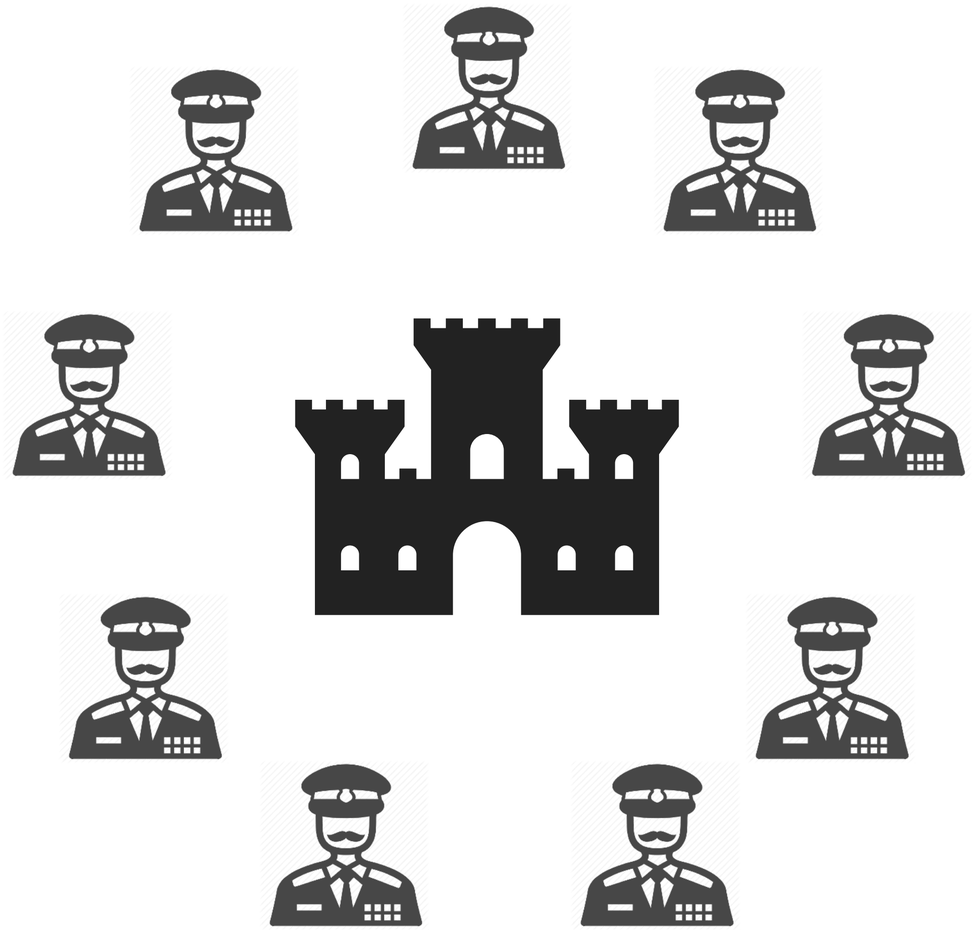
ARQUITETURA DE UM **BLOCKCHAIN**



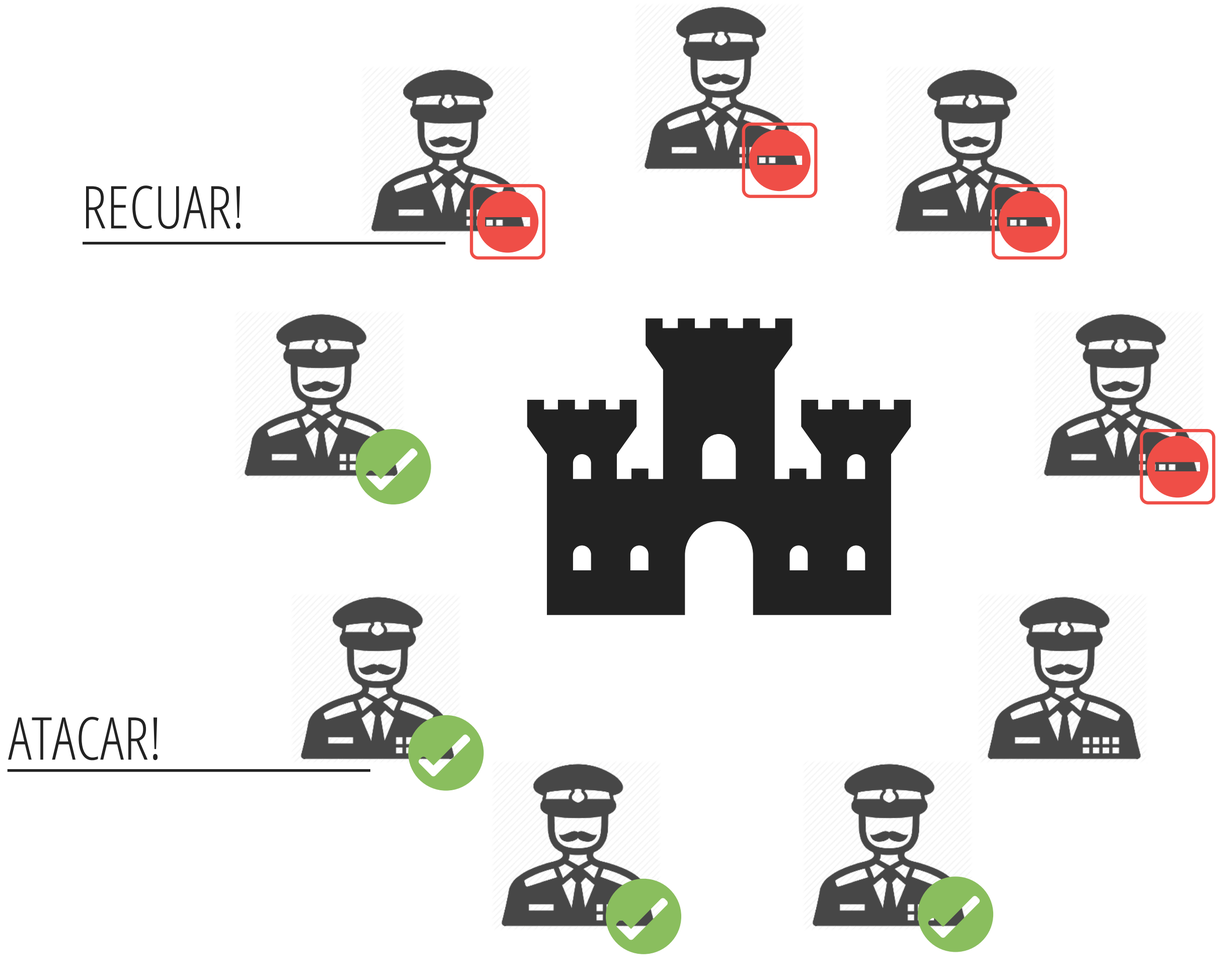
Consenso

Como a rede concorda sobre quais transações são mais confiáveis.

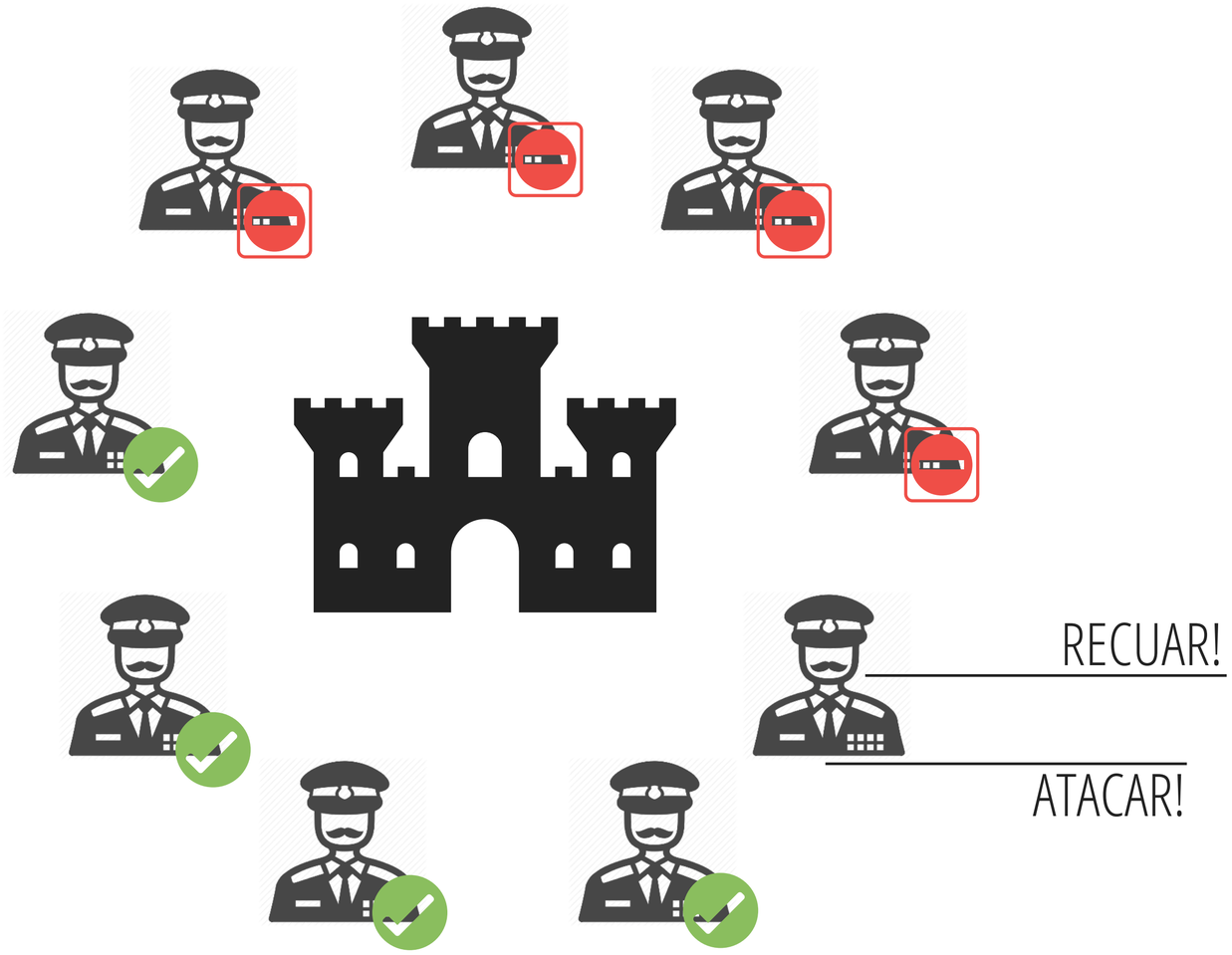
PROBLEMA DOS GENERAIS BIZANTINOS



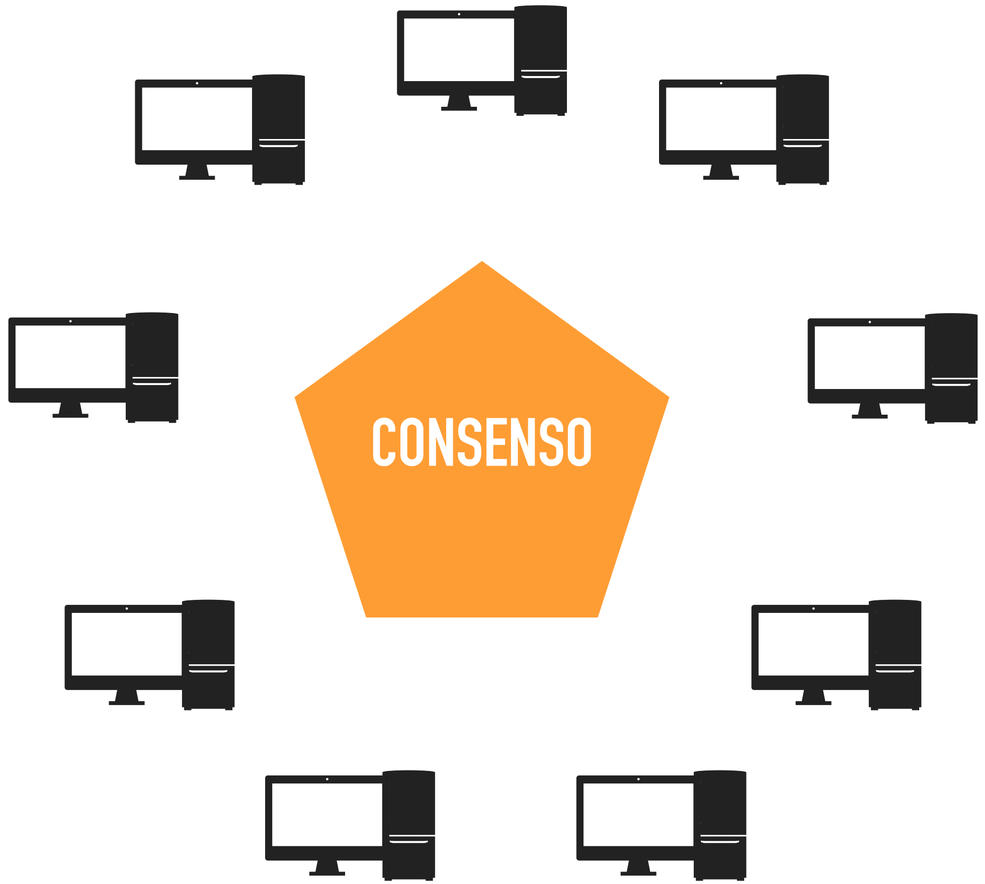
PROBLEMA DOS GENERAIS BIZANTINOS



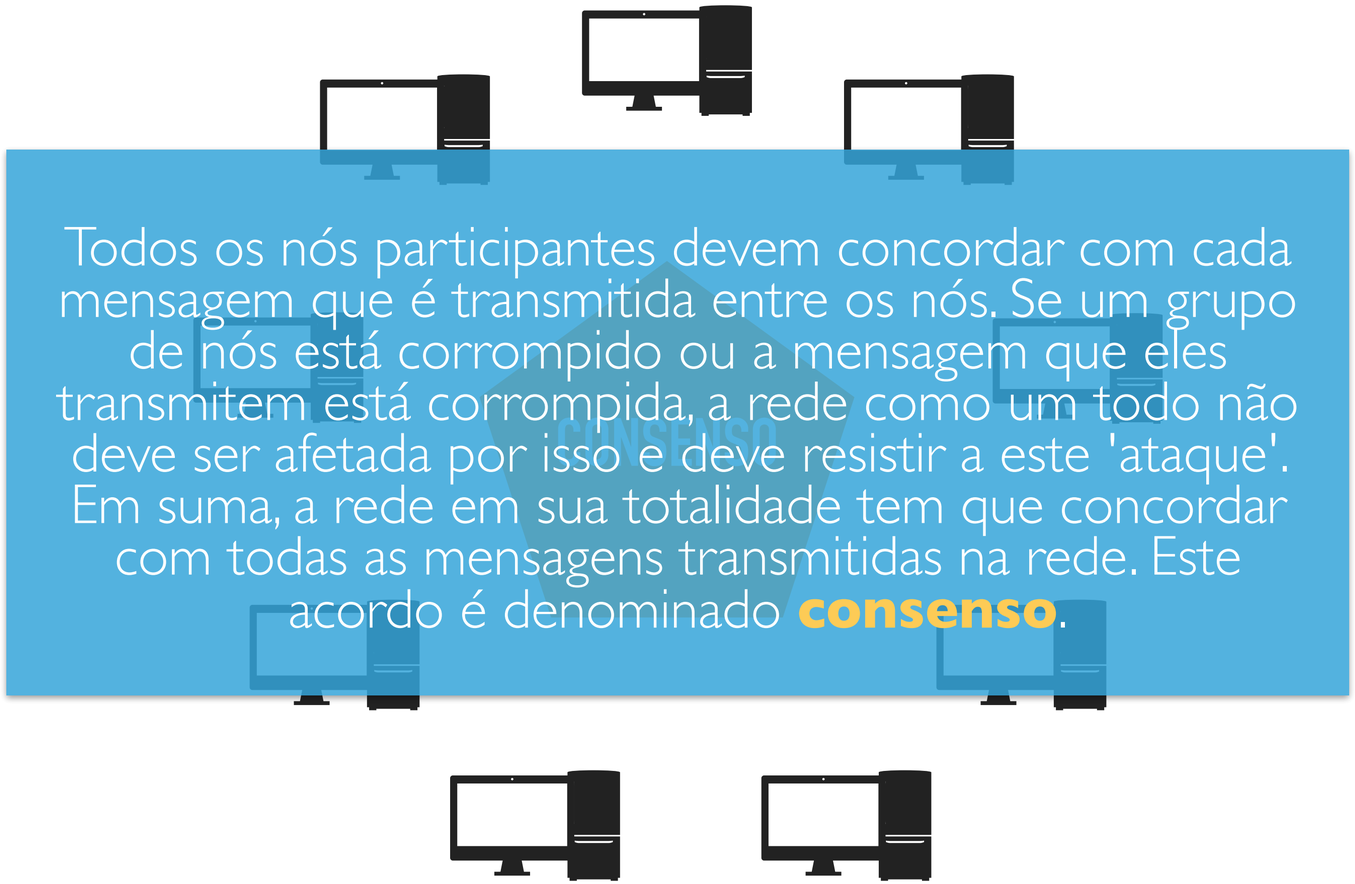
PROBLEMA DOS GENERAIS BIZANTINOS



PROBLEMA DOS GENERAIS BIZANTINOS



PROBLEMA DOS GENERAIS BIZANTINOS



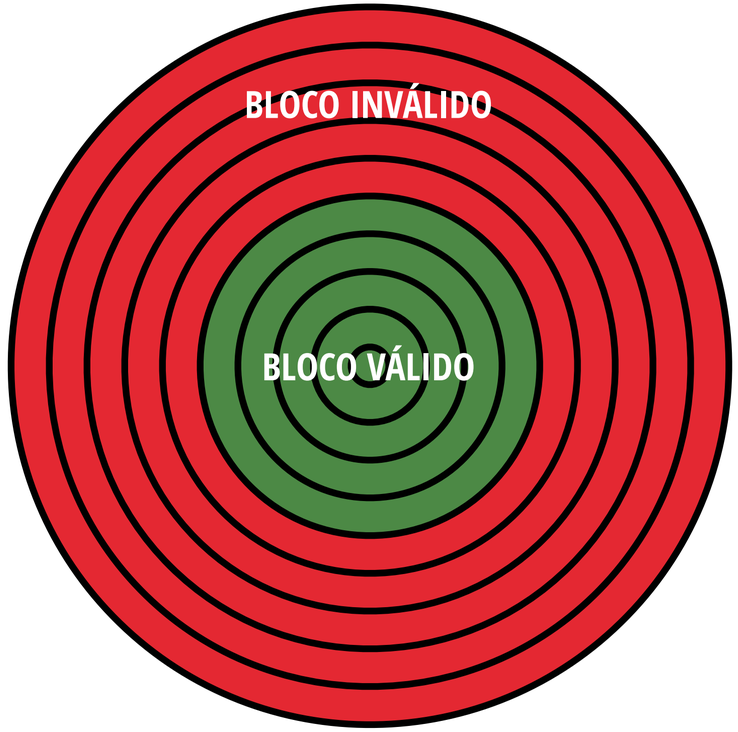
Todos os nós participantes devem concordar com cada mensagem que é transmitida entre os nós. Se um grupo de nós está corrompido ou a mensagem que eles transmitem está corrompida, a rede como um todo não deve ser afetada por isso e deve resistir a este 'ataque'. Em suma, a rede em sua totalidade tem que concordar com todas as mensagens transmitidas na rede. Este acordo é denominado **consenso**.

Proof-of-Work

Sistema em que a informação deve ser custosa para ser produzida, mas fácil de ser verificada.

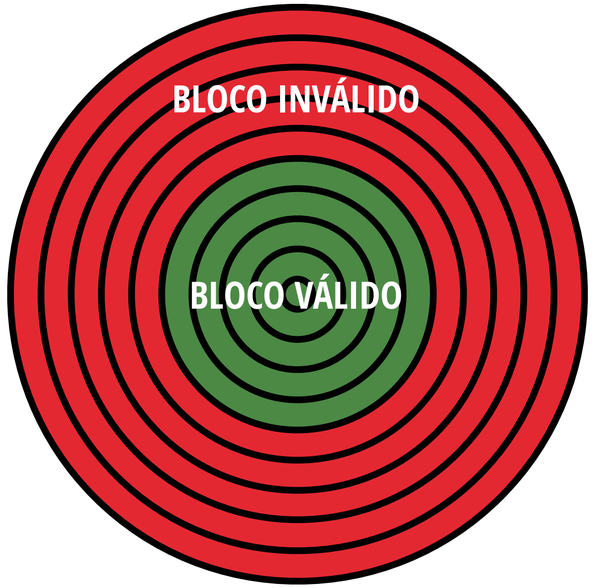
PROOF-OF-WORK

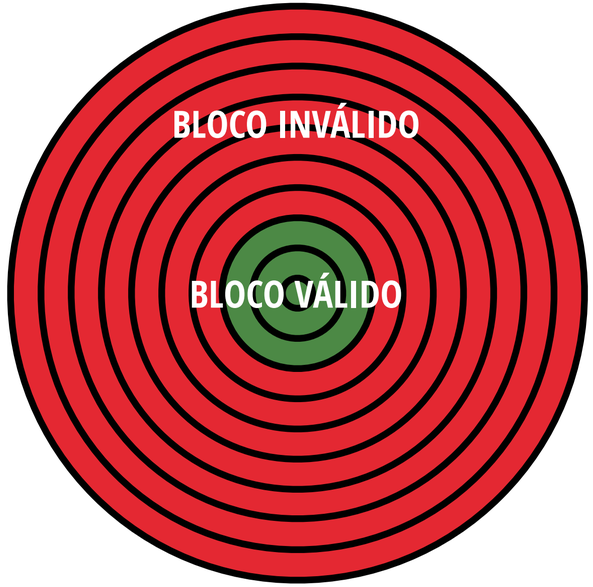
- **Minerar** é como jogar dardos em um alvo com os olhos vendados:
  - Probabilidade igual de atingir qualquer parte do alvo;
  - Lançadores velozes = mais acertos/ segundo
- Mineradores procuram por um *hash* abaixo de um alvo decidido por um algoritmo



DIFICULDADE

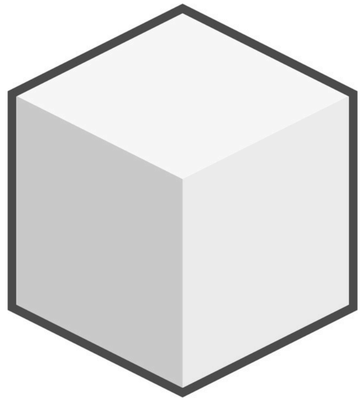
- Representação do número de computações esperados para achar um bloco válido
  - Quantidade de 0's mais significativos
  - Ajusta a cada 2016 blocos (~2 semanas)





DIFICULDADE

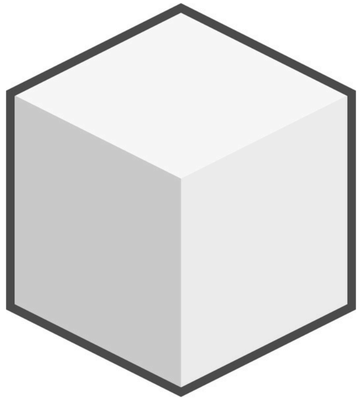
muito rápido...



0 →

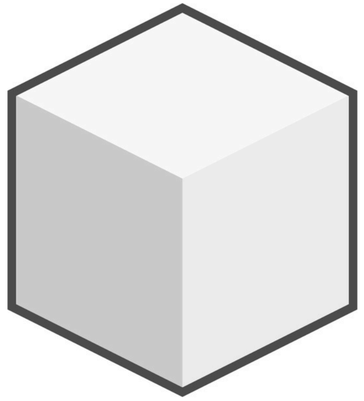
aumenta a dificuldade

10 minutos



00

muito devagar...



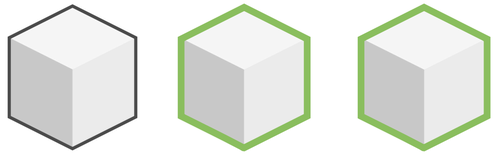
← 000

diminui a dificuldade

DIFICULDADE

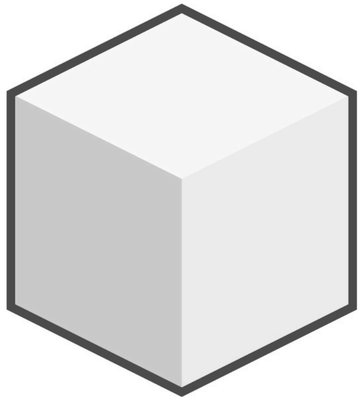
muito rápido…

modificar dados



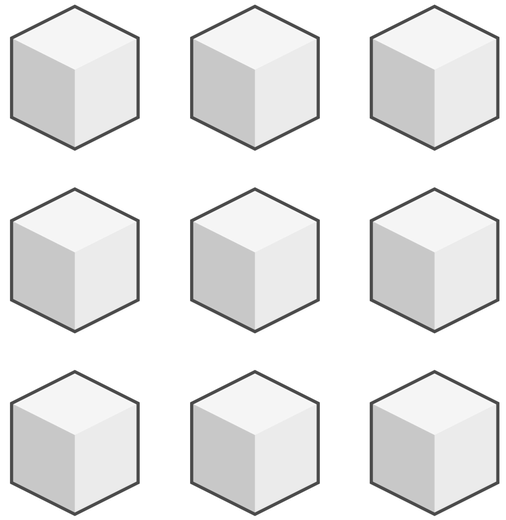
10 minutos

velocidade e segurança



muito devagar…

esperando...



DIFICULDADE

```
Difficulty: 1 (0 bits)

[...]

Difficulty: 8 (3 bits)
Starting search...
Success with nonce 9
Hash is 1c1c105e65b47142...b3c1
Elapsed Time: 0.0004 seconds
Hashing Power: 25065 hashes per second
Difficulty: 16 (4 bits)
Starting search...
Success with nonce 25
Hash is 0f7becfd3bcd1a82...e148
Elapsed Time: 0.0005 seconds
Hashing Power: 52507 hashes per second
Difficulty: 32 (5 bits)
Starting search...
Success with nonce 36
Hash is 029ae6e5004302a1...7903
Elapsed Time: 0.0006 seconds
Hashing Power: 58164 hashes per second

[...]
```

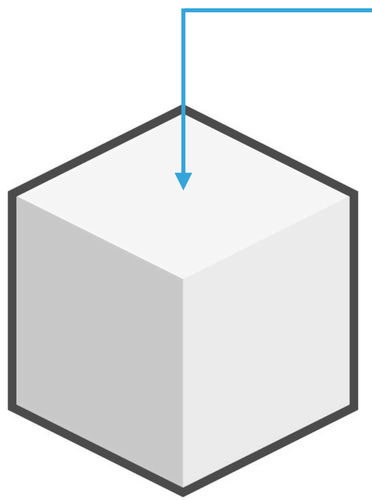
```
Difficulty: 4194304 (22 bits)
Starting search...
Success with nonce 1759164
Hash is 0000008bb8f0e731f0496...efc3
Elapsed Time: 13.3201 seconds
Hashing Power: 132068 hashes per second
Difficulty: 8388608 (23 bits)
Starting search...
Success with nonce 14214729
Hash is 000001408cf12dbd20fcb...f0a3
Elapsed Time: 110.1507 seconds
Hashing Power: 129048 hashes per second
Difficulty: 16777216 (24 bits)
Starting search...
Success with nonce 24586379
Hash is 0000002c3d6b370fccd69...8b95
Elapsed Time: 195.2991 seconds
Hashing Power: 125890 hashes per second

[...]

Difficulty: 67108864 (26 bits)
Starting search...
Success with nonce 84561291
Hash is 0000001f0ea21e676b6dd...e21a
Elapsed Time: 665.0949 seconds
Hashing Power: 127141 hashes per second
```

DIFICULDADE

target bits

0x171ba3d1

DIFICULDADE



target bits

0x171ba3d1

DIFICULDADE

0x1903a30c

$$\text{alvo} = \text{coeficiente} * 2^{(8*(\text{expoente}-3))}$$

coeficiente = 0x03a30c

expoente = 0x19

DIFICULDADE

coeficiente = 0x03a30c
expoente = 0x19

alvo = coeficiente * $2^{(8*(expoente-3))}$

alvo = 0x03a30c * $2^{(0x08*(0x19-0x03))}$

alvo = 0x03a30c * $2^{(0x08*0x16)}$

alvo = 0x03a30c * 2^{0xB0}

em decimal...

alvo = 238.348 * 2^{176}

alvo = 22829202948393929850749706076701368331072452018388575715328

de volta ao hex...

alvo = 0x00000000000003A30C000000000000000000000000000000000000000000

https://www.btc.com/0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4

DIFICULDADE

https://www.blockchain.com/charts/difficulty

MINERAÇÃO COM CPU – PSEUDOCÓDIGO

```
TARGET = (65535 << 208)/DIFFICULTY;
coinbase_nonce=0;
while (1) {
  header = makeBlockHeader(transactions, coinbase_nonce);
   for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++) {
      if (SHA256(SHA256(makeBlock(header, header_nonce))) < TARGET) {
         break; // bloco encontrado!
      }
   }
  coinbase_nonce++;
}
```

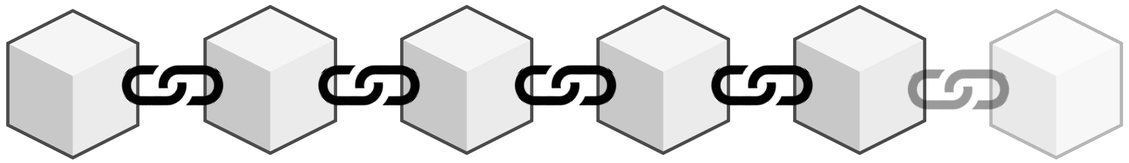
Princeton, Bitcoin and Cryptocurrency Technologies

PROOF-OF-WORK - DEMO

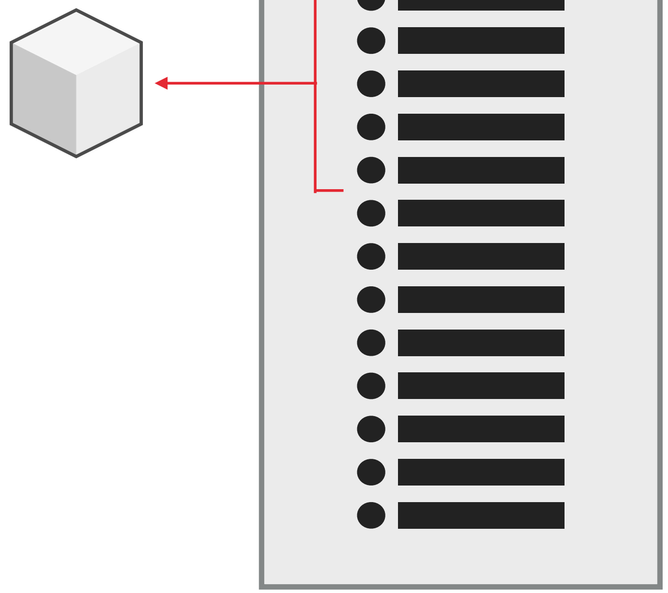
https://andersbrownworth.com/blockchain/block

PROOF-OF-WORK

Blockchain

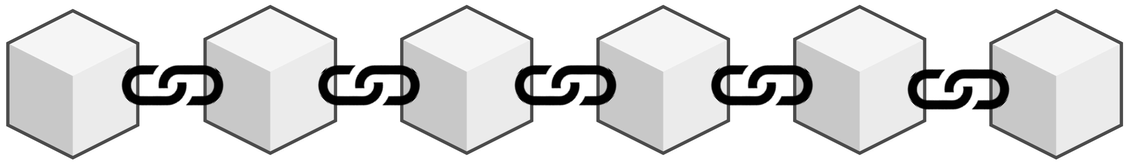


Nós da rede

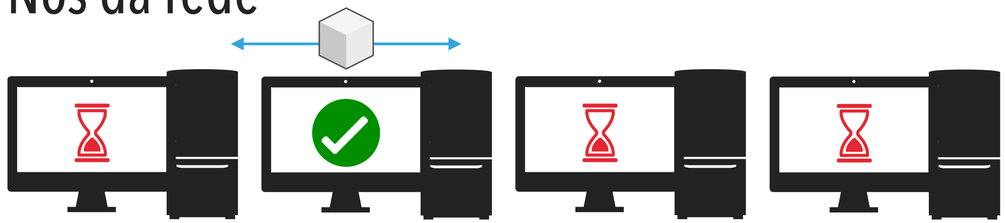


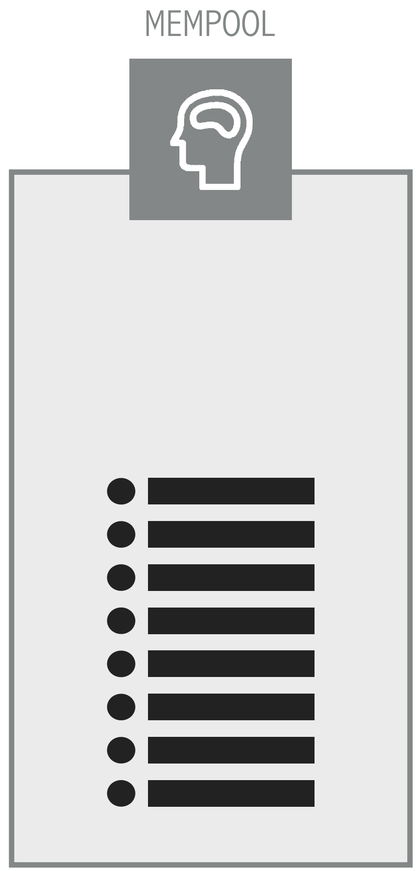
PROOF-OF-WORK

Blockchain

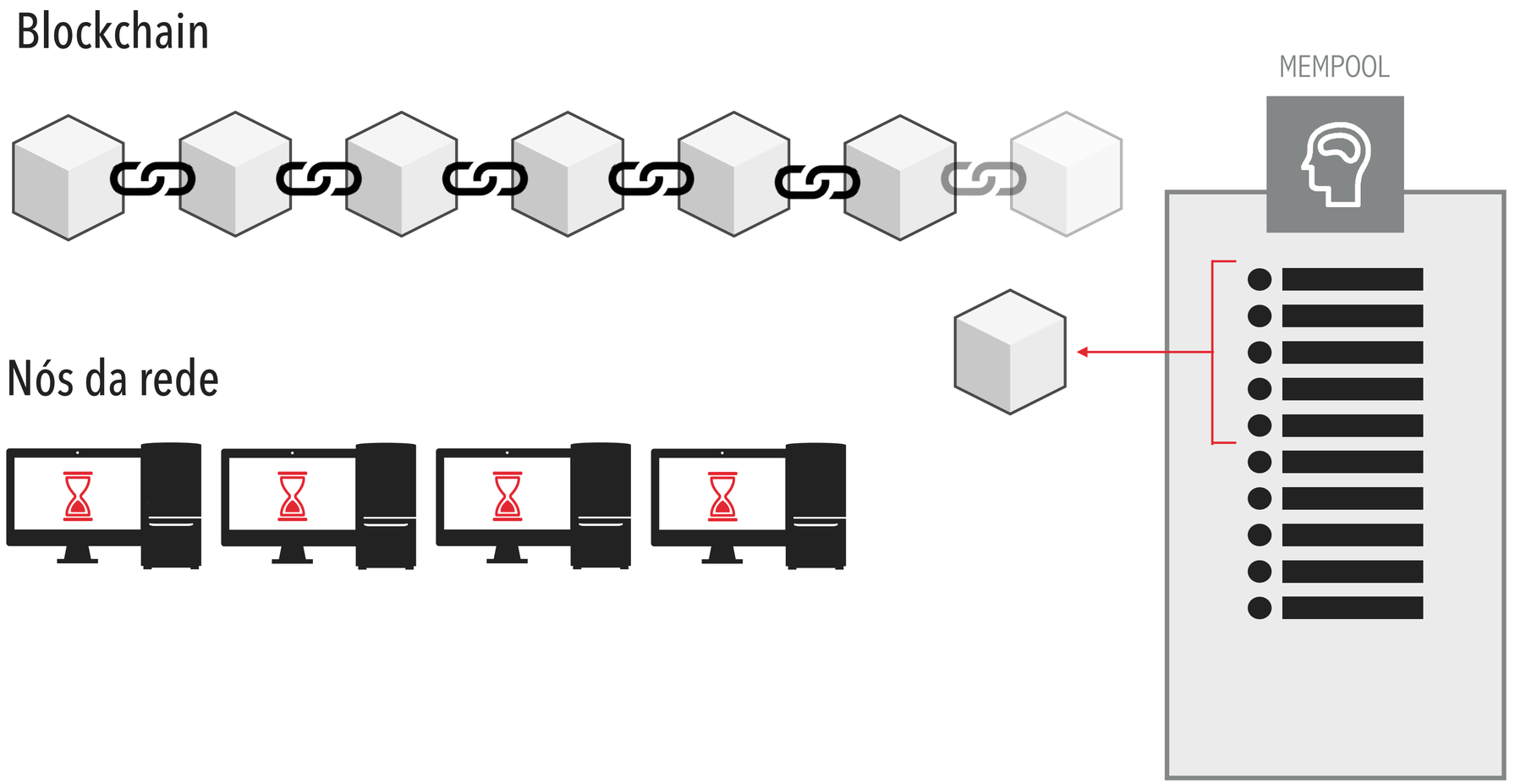


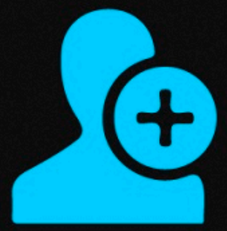
Nós da rede





PROOF-OF-WORK





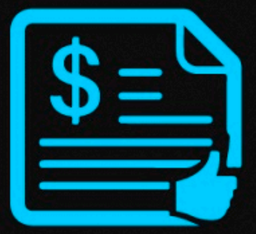
1 Um usuário cria uma transação

2 A transação é incluída em um bloco que é minerado

3 O bloco se difunde para todos os nós da rede

4 Todos os nós recebem e validam o bloco

5 O bloco é adicionado ao blockchain



6 A transação é verificada e validada

COINBASE

- Criar blocos válidos custa:
  - energia
  - tempo
  - dinheiro
- **Recompensa! $$$**
- Única maneira onde novos "bitcoins" são **criados**
  - Ou seja, UTXOs não são consumidos!

Block #581096

Summary	
Number Of Transactions	2382
Output Total	10,006.88010994 BTC
Estimated Transaction Volume	475.50939515 BTC
Transaction Fees	0.65669335 BTC
Height	581096 (Main Chain)
Timestamp	2019-06-17 09:40:18
Received Time	2019-06-17 09:40:18
Relayed By	Unknown
Difficulty	7,409,399,249,090.25
Bits	388365571
Size	1219.516 kB
Weight	3992.632 kWU
Version	0x20000000
Nonce	3646959550
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000001d754d651a13718e72460393111440d20c7679dfe3603c
Previous Block	00000000000000000009950edc6c4048c352deaff9d580c9efa36796c197f2d7
Next Block(s)	00000000000000000023c91dd22524ad86a1d65ee713c3e67c44b20df5549218
Merkle Root	ce1523db5d3344d445f4c6422c9555df6747dfe4a5cd355466a5eb94bdd413cf

Transactions

1dc91c0afa4ee6291c6fce2ef212cda58031ddb69eec633eb426bdcf9c8d657c — **2019-06-17 09:40:18**

No Inputs (Newly Generated Coins)	→	1MvYASoHjqynMaMnP7SBmenyEWiLsTqoU6 Unable to decode output address
		13.15669335 BTC 0 BTC

13.15669335 BTC

6abdd1a5f6067bd30c40f0bda4c6b0d48f27a425ec2afdaf9e69e23a6ab3b6a5 — **2019-06-17 09:39:15**

36KCNoPey8WzJcUwyabCu4V7K2hMwrxYt8	→	38J8VkVaq5MUQ1UpmCxi5AixfRmRmgRwwA 38bNQE3eUXa6zkbYji4Q71erEwjkUMMk1u
		0.15 BTC 15.88415613 BTC

16.03415613 BTC

COINBASE

- Qual é essa recompensa? Começou com **50 BTC**…
- Satoshi Nakamoto definiu que a cada 210.000 blocos minerados, a recompensa seria diminuída pela metade (chamado de ***halving***)
  - Novembro/2012: 25 BTC
  - Julho/2016: 12,5 BTC
  - Maio/2020: 6,25 BTC
  - ~Março/2024: 3,125 BTC

TAXAS DE TRANSAÇÃO

- A maioria das transações incluem ***transactions fees*** para recompensar mineradores
- Incentivo para que mineradores incluam sua transação no próximo bloco
- Taxas de transação são recolhidas pelo minerador

fees = sum(inputs) - sum(outputs)

TAXAS DE TRANSAÇÃO

Transaction View information about a bitcoin transaction

6abdd1a5f6067bd30c40f0bda4c6b0d48f27a425ec2afdaf9e69e23a6ab3b6a5

36KCNoPey8WzJcUwyabCu4V7K2hMwrxYt8	38J8VkVaq5MUQ1UpmCxi5AixfRmRmgRwwA	0.15 BTC
	38bNQE3eUXa6zkbYji4Q71erEwjkUMMk1u	15.88415613 BTC

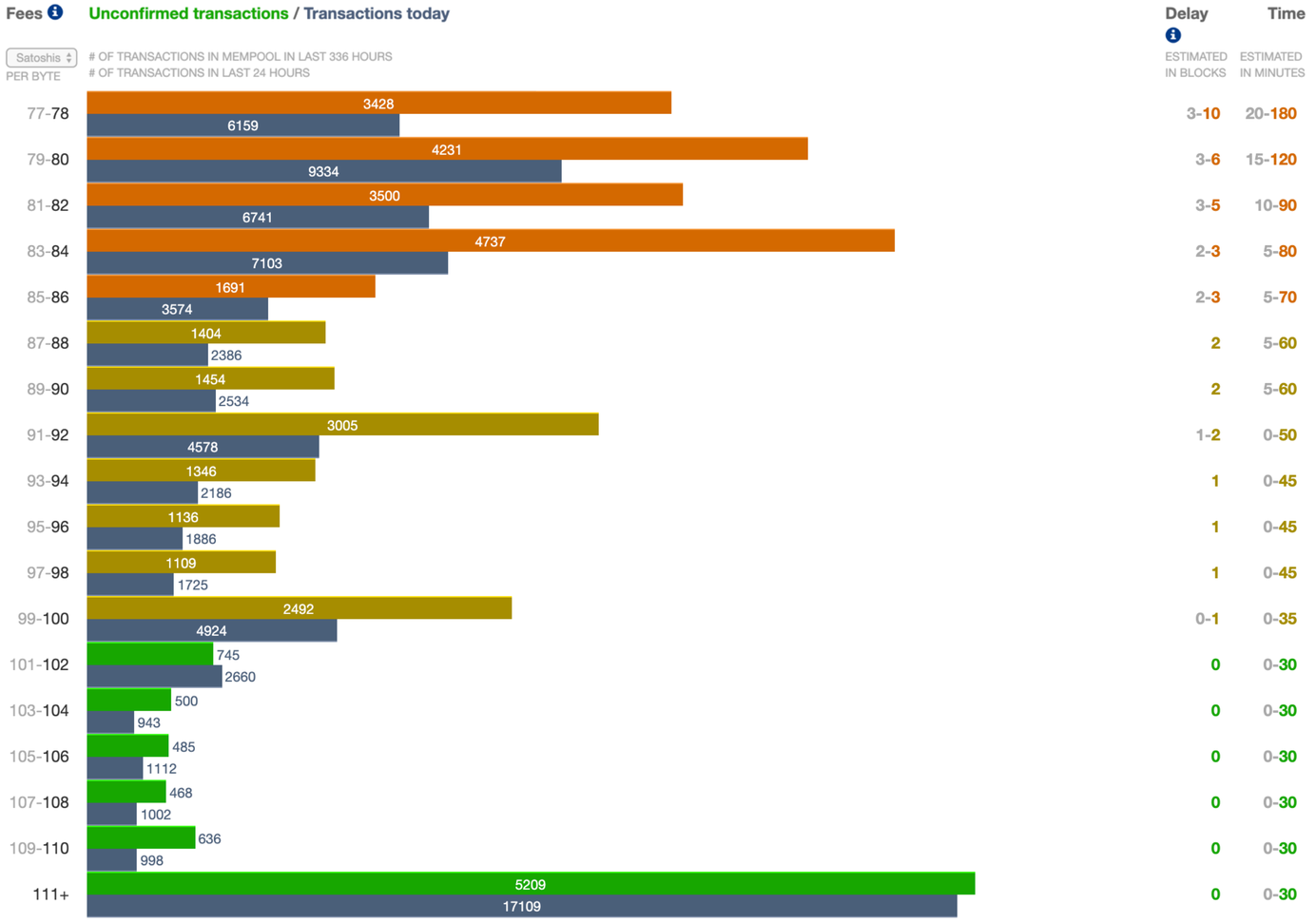
21 Confirmations | 16.03415613 BTC

Summary	
Size	247 (bytes)
Weight	661
Received Time	2019-06-17 09:39:15
Included In Blocks	581096 (2019-06-17 09:40:18 + 1 minutes)
Confirmations	21
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	16.03476902 BTC
Total Output	16.03415613 BTC
Fees	0.00061289 BTC
Fee per byte	248.134 sat/B
Fee per weight unit	92.722 sat/WU
Estimated BTC Transacted	0.15 BTC
Scripts	Show scripts & coinbase

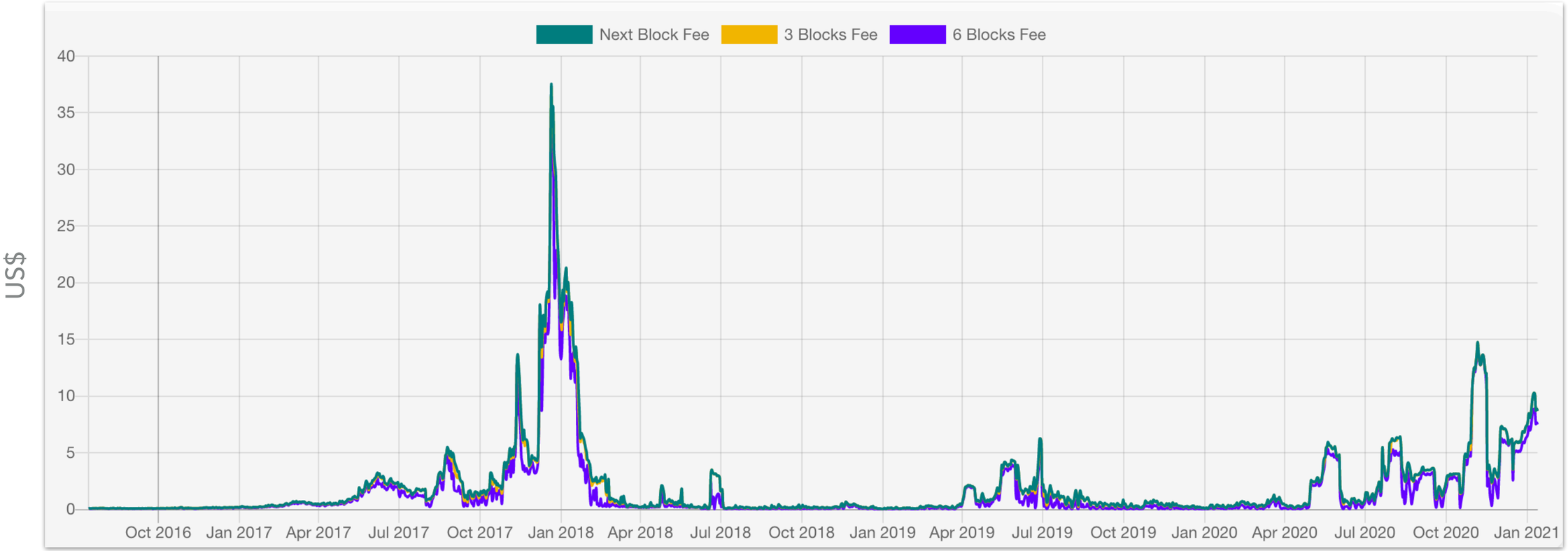
https://www.blockchain.com/btc/tx/6abdd1a5f6067bd30c40f0bda4c6b0d48f27a425ec2afdaf9e69e23a6ab3b6a5

TAXAS DE TRANSAÇÃO



https://bitcoinfees.earn.com

TAXAS DE TRANSAÇÃO



https://bitcoinfees.info

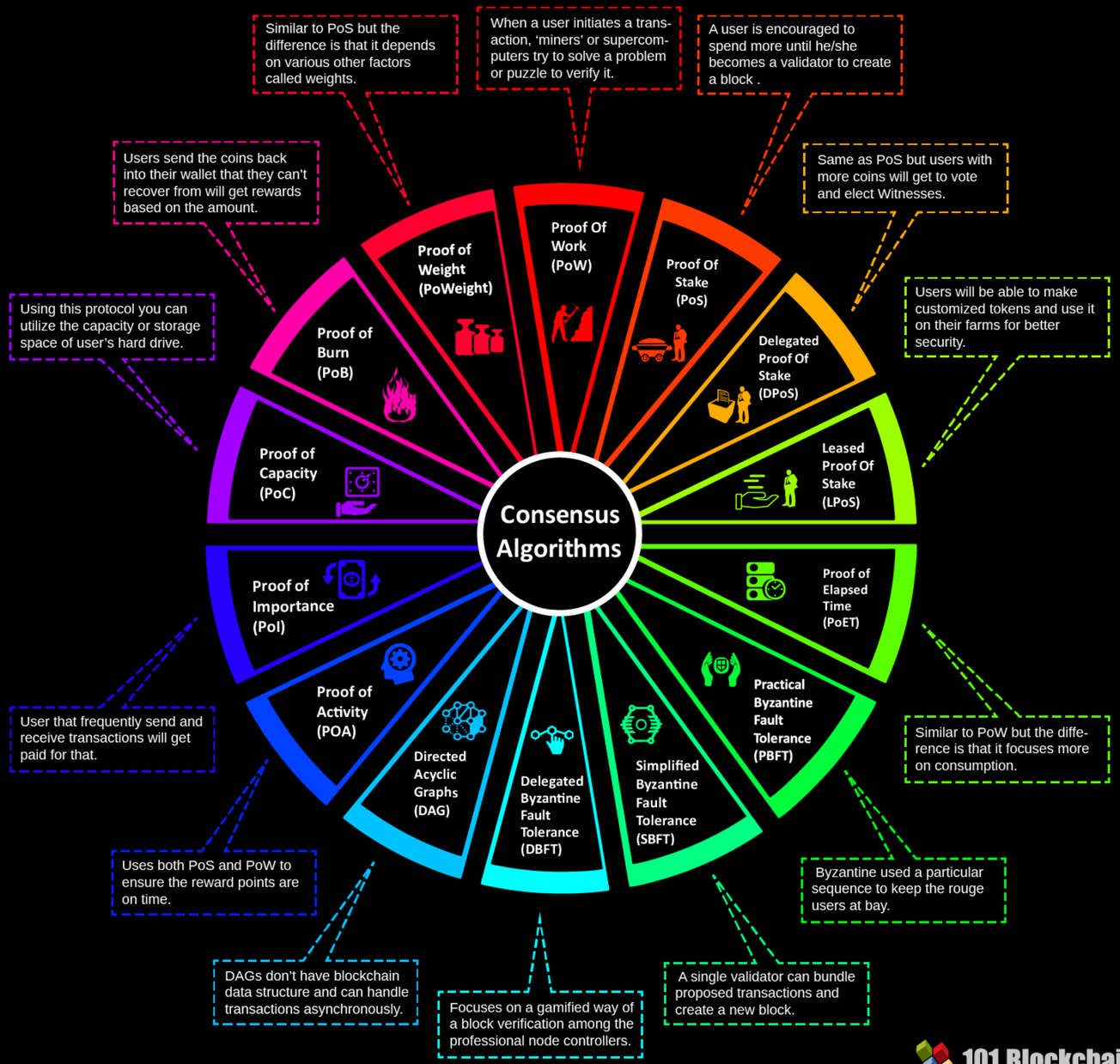
TAXAS DE TRANSAÇÃO – CASOS NOTÁVEIS

https://btc.com/cc455ae816e6cdafdb58d54e35d4f46d860047458eacf1c7405dc634631c570d

https://btc.com/7e8fce9686572d8308d8c40fa3cb96fdbf96c0787c147d3159c893fd560aabc7

https://btc.com/1a3a7e334d5d894c66830dadd2f94f22f64b0c3aa5fb4cc956ef6734f1bb98ab

DIFERENTES TIPOS DE ALGORITMOS DE CONSENSO

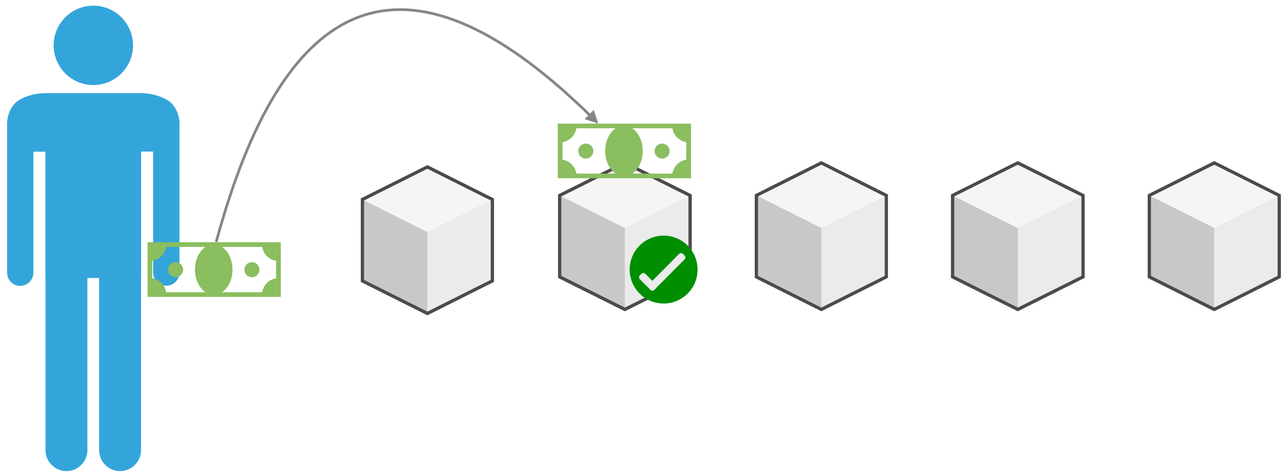


Proof-of-Stake

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.

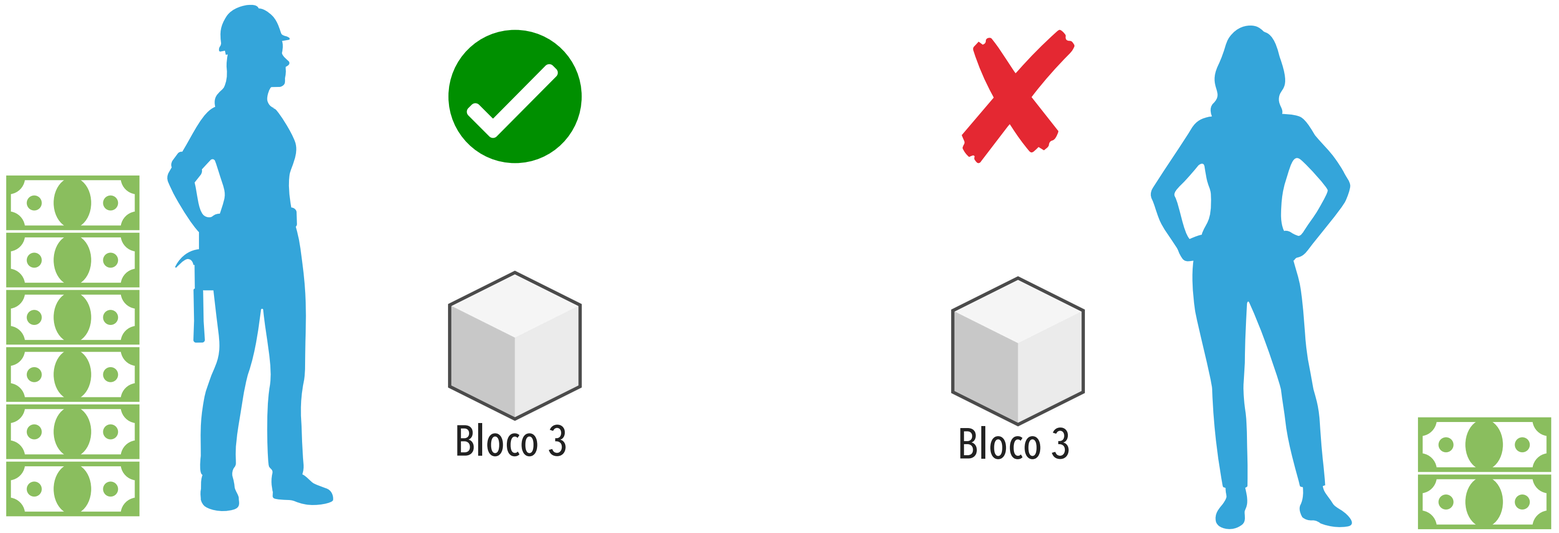
PROOF-OF-STAKE

- 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



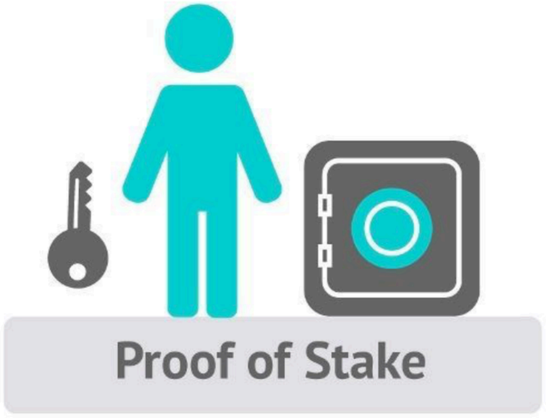
PROOF-OF-STAKE

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



PROOF-OF-STAKE

- Nós **apostam** moeda 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

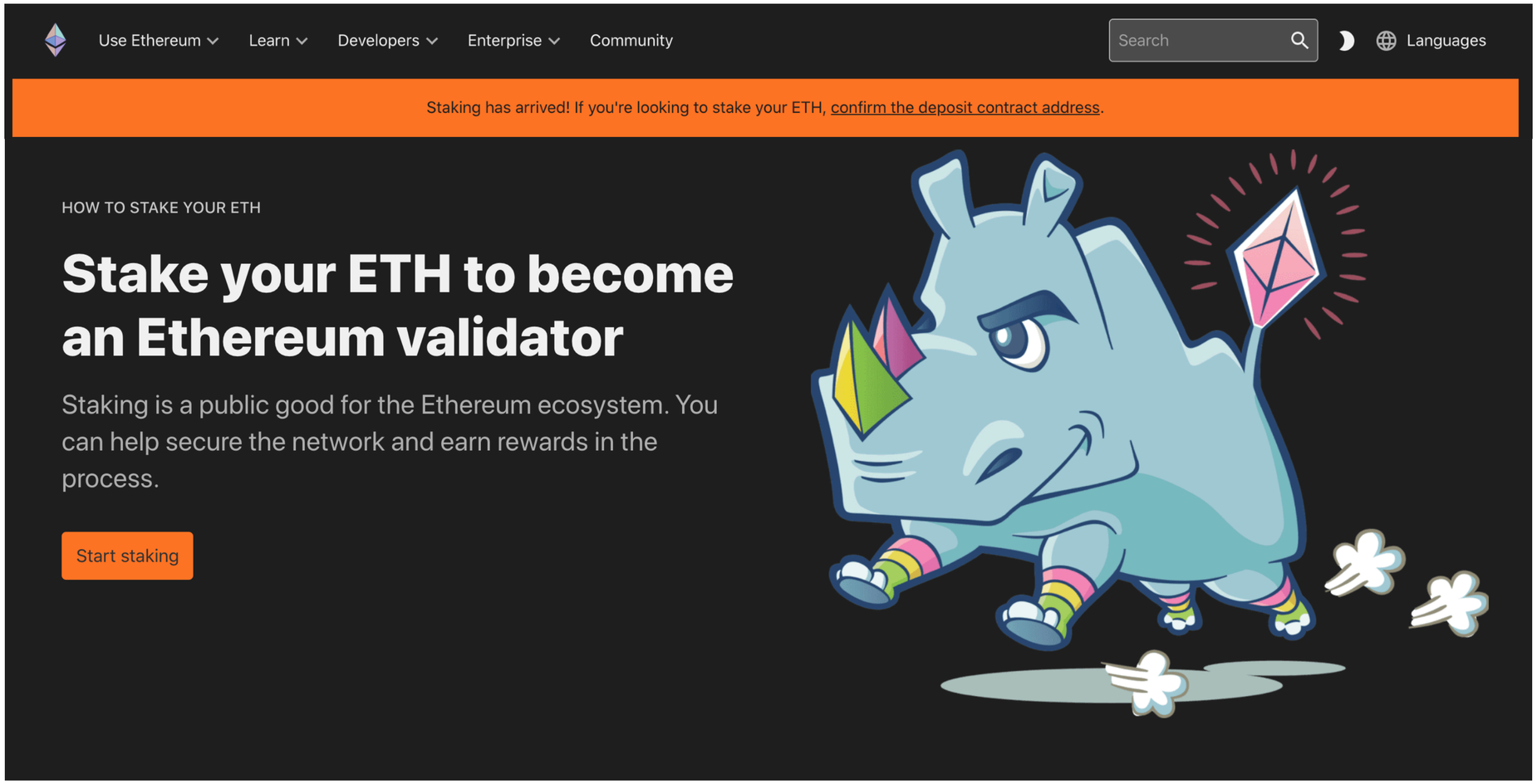


POW VS POS

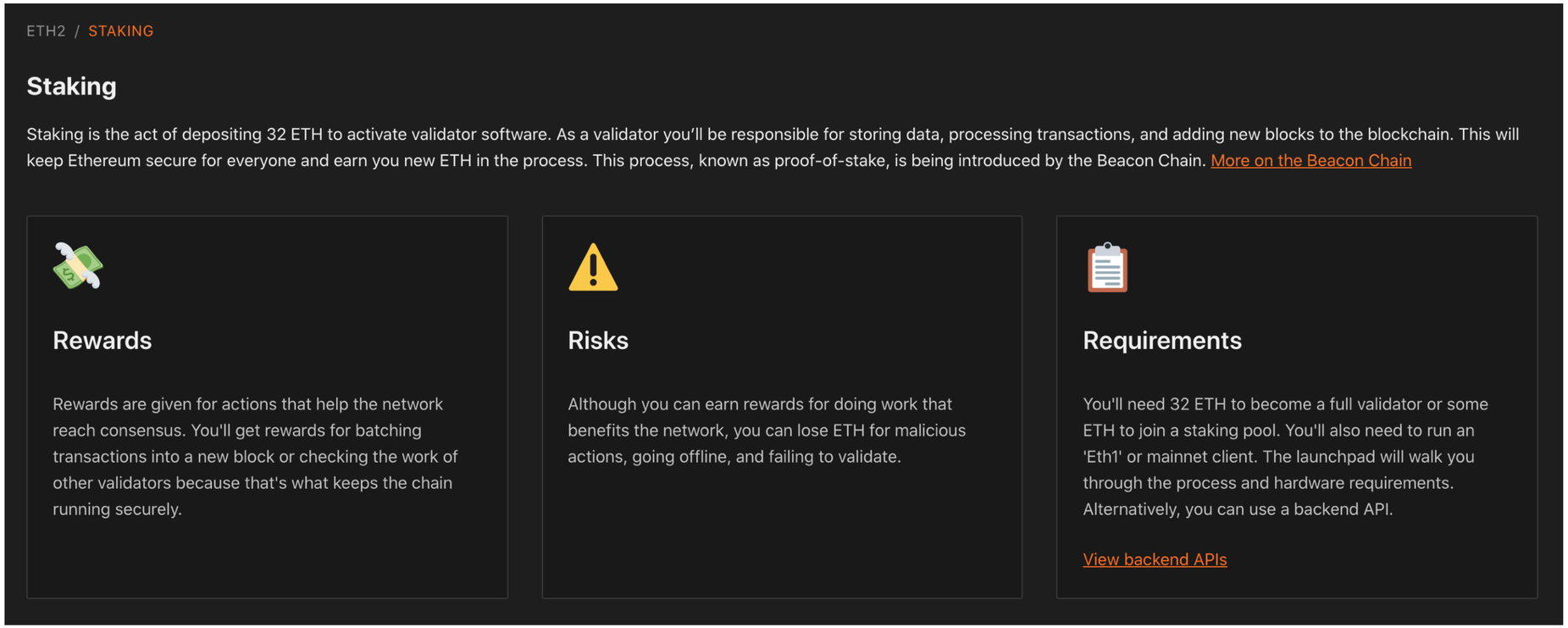
Mineradores tem poder de voto proporcional ao seu poder computacional

Validadores tem poder de voto proporcional ao seu stake apostado

PROOF-OF-STAKE: ETH2.0



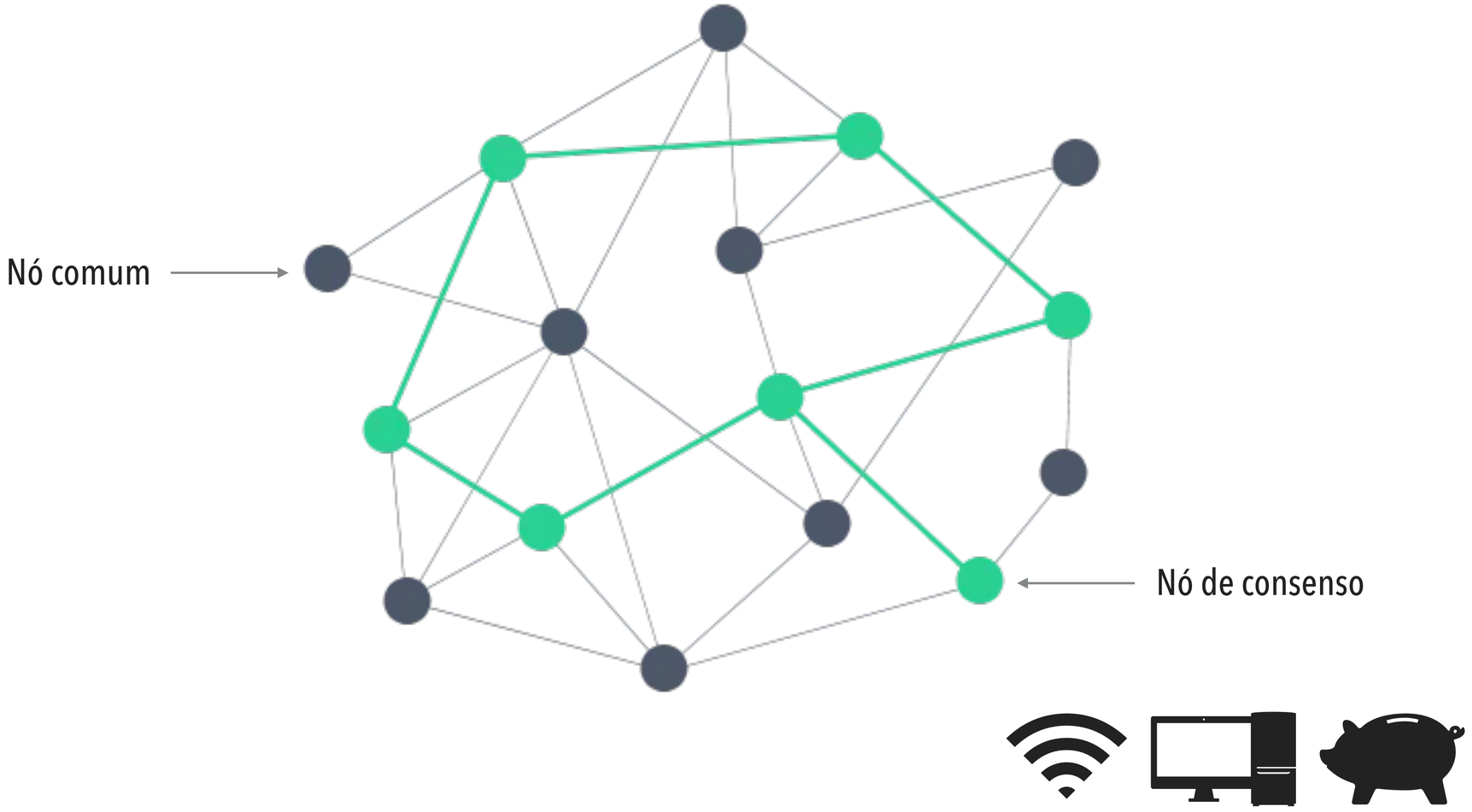
PROOF-OF-STAKE: ETH2.0



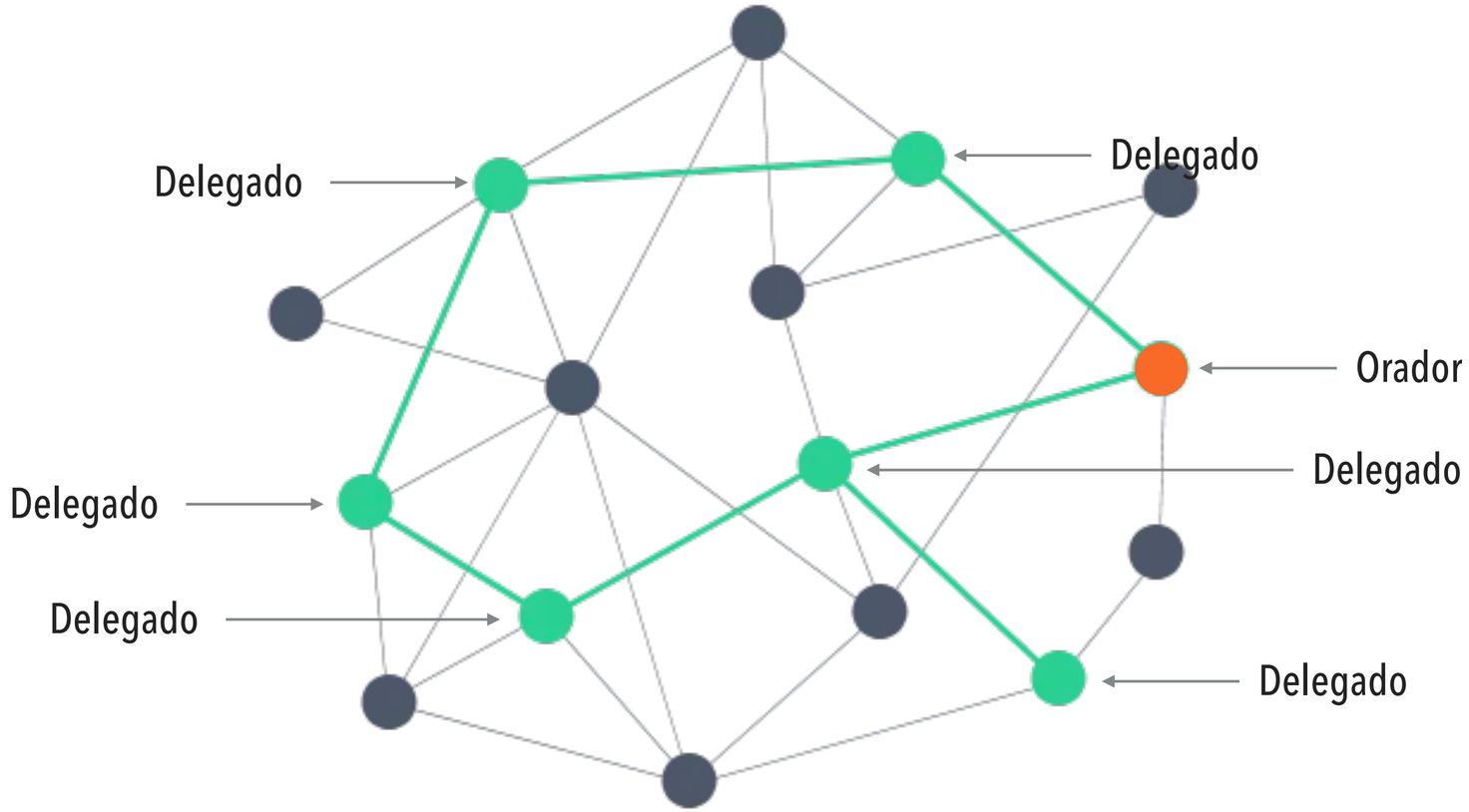
dBFT (*Delegated Byzantine Fault Tolerance*)

Algoritmo de consenso baseado na definição de diferentes papéis aos nós para auxiliar na organização do consenso.

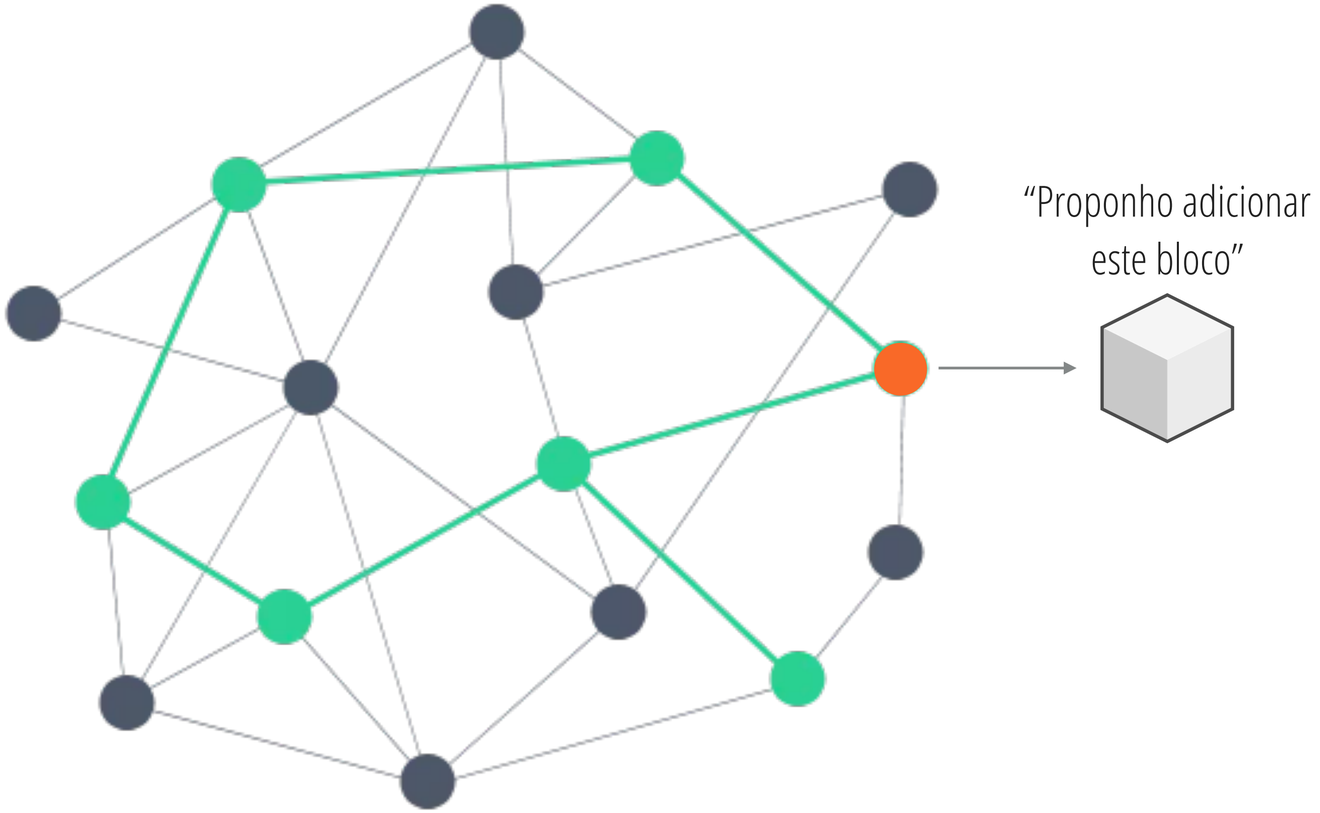
DBFT – COMO FUNCIONA?



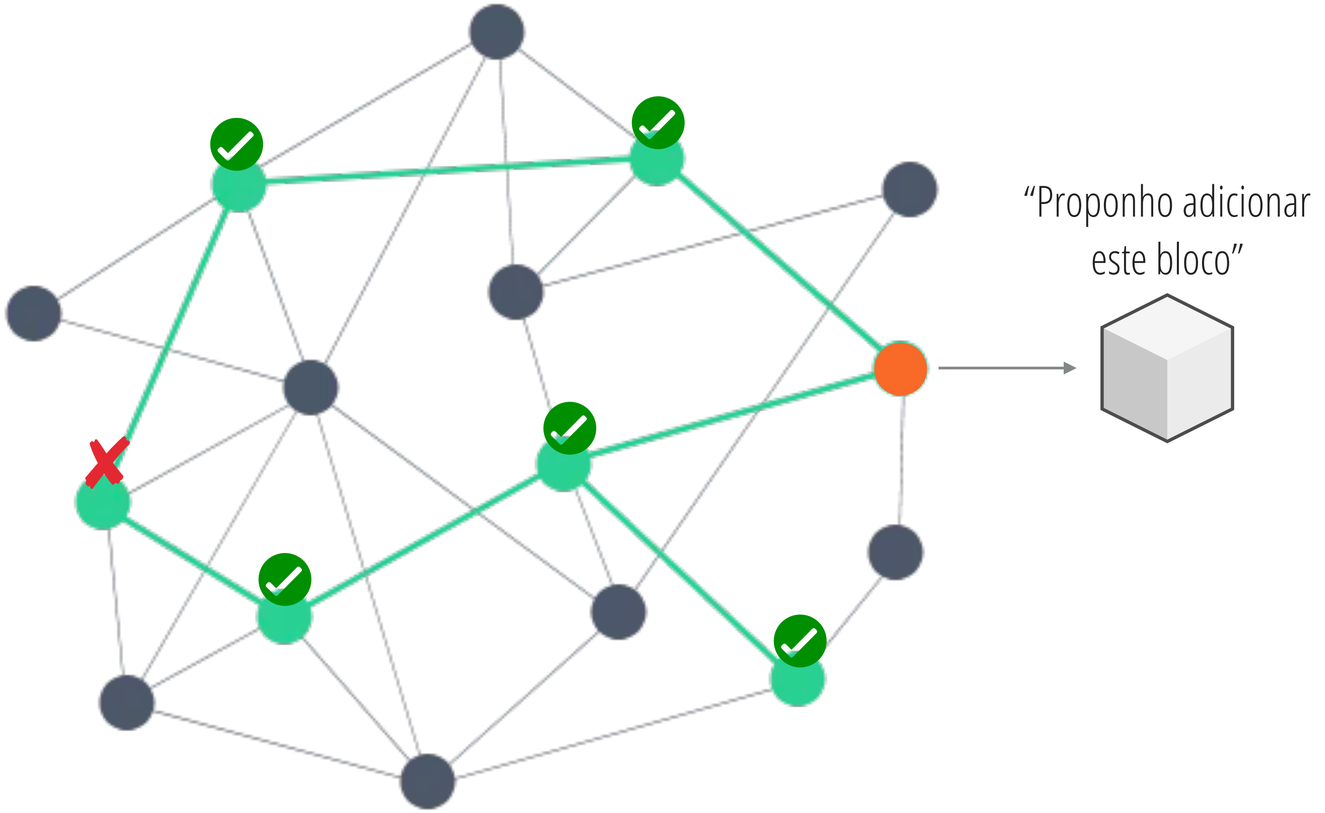
DBFT – COMO FUNCIONA?



DBFT – COMO FUNCIONA?

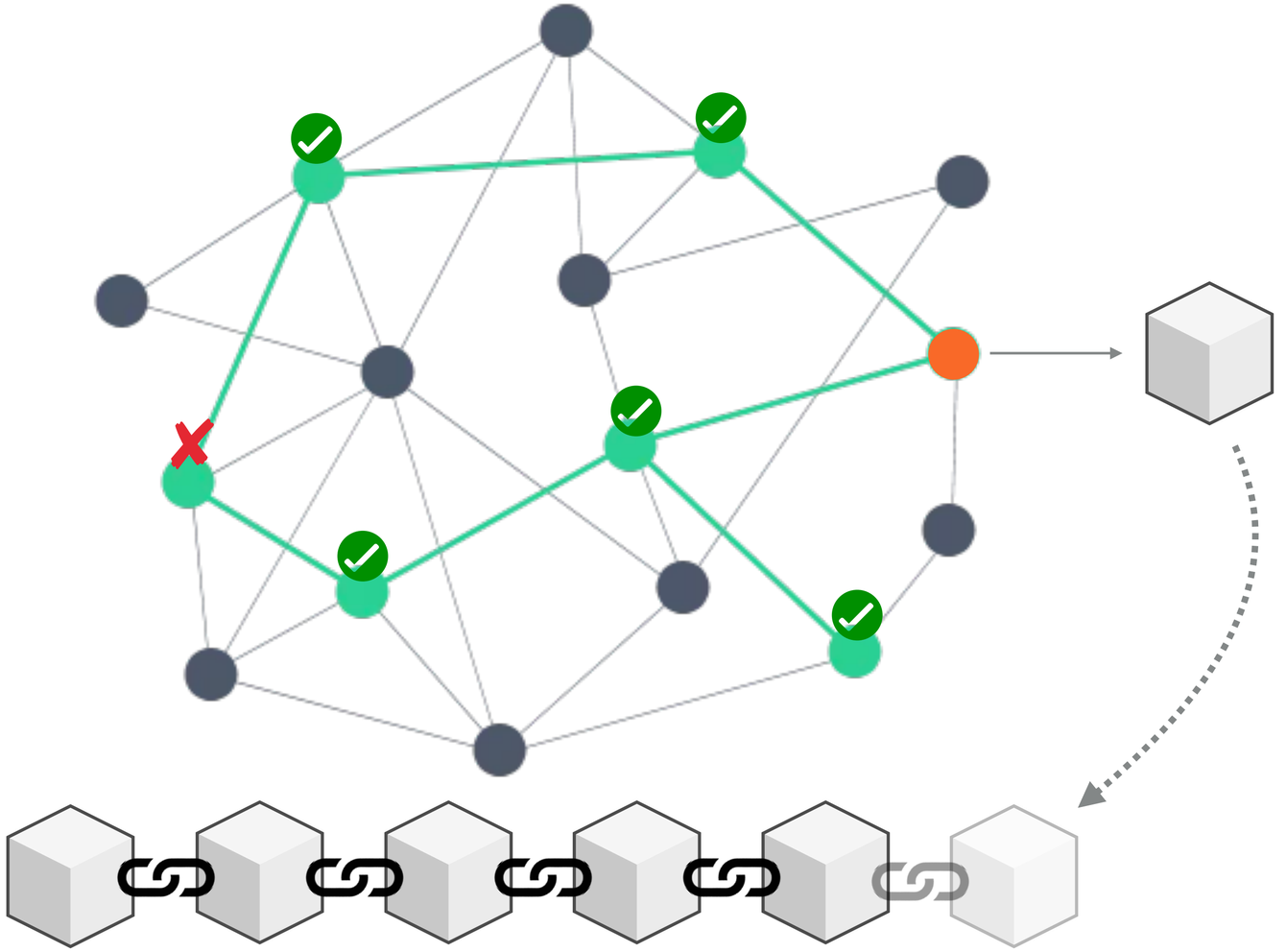


DBFT – COMO FUNCIONA?



Receber 2/3 dos votos dos delegados

DBFT – COMO FUNCIONA?



DBFT