



Blockchain

Emilio Francesquini
e.francesquini@ufabc.edu.br

Vladimir Rocha
vladimir.rocha@ufabc.edu.br

Agenda

1. O que é uma Blockchain?
2. Fundamentos
3. Revisão histórica
4. Como funciona?
5. Consenso ← importante
6. Ataques
7. Aplicações
8. Tendências
9. Mineração de Bitcoins

1. O que é uma Blockchain?

- Blockchain é uma tecnologia que permite registrar eventos realizados de forma imutável, transparente e descentralizada

onde eventualmente todos os participantes enxergarão os eventos **na mesma ordem**.

Dr. Vincent		
1847		
Jan 28	To Sundries	10 16
30 "	Making 10 ¹⁰ / ₁₂ Hrs	5 "
" 2	Day & Evening Star	10 "
March 19	Taping & whitening Boxes	2 "
23 "	Taping & Boxes	2 9
25 "	Mending 10 Books	1 "
April 3	Taping & Wall Box	2 "
26 "	Mending 2 10 ¹⁰ / ₁₂ Hrs	3 "
May 3	Mending 10 Books	2 6
		511 1 9
1848		
May 27	To Balance Due	1 " 8
29 "	Making 10 Boxes	6 "
June 12	Making 10 Boxes	3 6
21 "	Making 10 ¹⁰ / ₁₂ Hrs	1 6
August 9	Taping 10 Boxes	2 6
Sept 1	Rent	2 7
24 "	To Fresh Paint	4 "
" 1 Day haying	" 9 "	
" with boy	" 3 "	
" Day cutting grass	" 8 "	
" with boy	" 3 "	
9 "	Making 10 Boxes	3 6
20 "	Making 10 Boxes	3 6
" 1 Day haying	" 2 "	
24 "	Making 10 Boxes	6 "
Dec 24	Mending 10 Boxes	2 6
Jan 12	Mending 10 Boxes	2 6
		49 5
Stillwill C ^o		
1847		
Jan 28	To Sundries	9 16 1
May 17	Porter & Poor	2 2 48
"	Balanc. Due	2 11 1 9
This day record & settled all accts & paid due two dollars fifty eight. Cate Durham May 29 th 1848		
Cristo Salvatoris		
Vincent Stillwill		
Settled		
July 1 To Bushel Plaster " 4 6		
" horse to Stone Corn " 2 "		
" Hamper " 2 "		
Oct 5 " Horses & Mow " 6 "		
" Glass Goods " 1 " 0		
" Carting plastered " 3 9		
Dec 1 " 8 lbs. Lamb meat " 1 41 "		
" 3 2 3		
1848		
To Sundries		
" Mending 1 Pottery Cook " 1 6		
March 3 " Mending 3 Boxes " 2 3		
12 " Taping 1 Box " 6 "		
20 " Mending 10 Boxes " 4 6		
" 49 71		

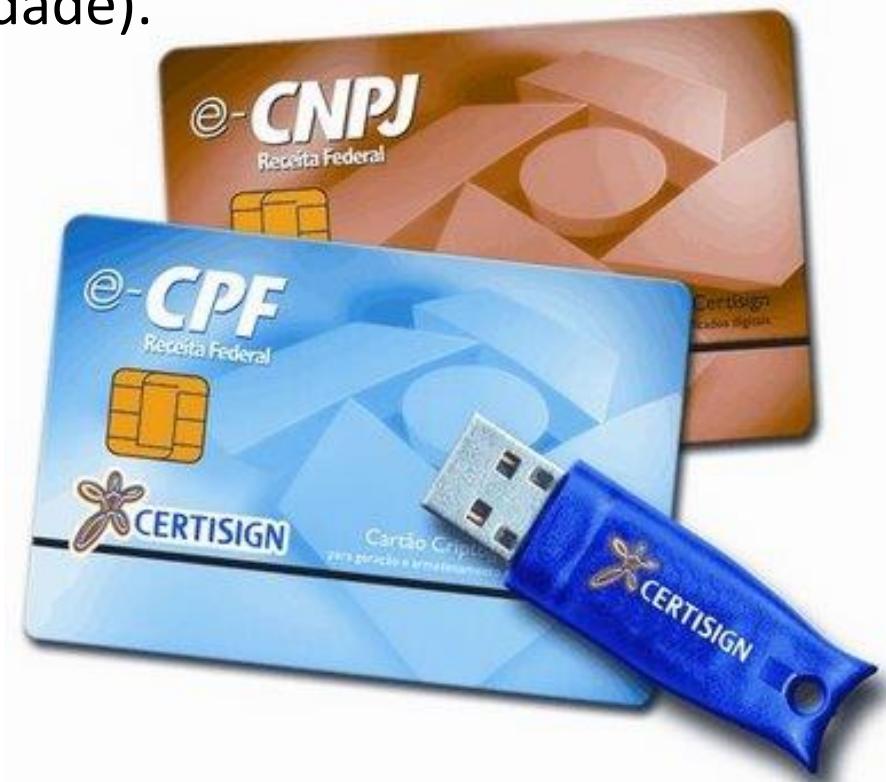
2. Fundamentos da Blockchain

Blockchain é uma tecnologia que permite registrar eventos realizados de forma
imutável, transparente e descentralizada

- Autenticidade (integridade)
- Imutabilidade
- Transparência (auditabilidade)
- Tolerância a falhas (disponibilidade)

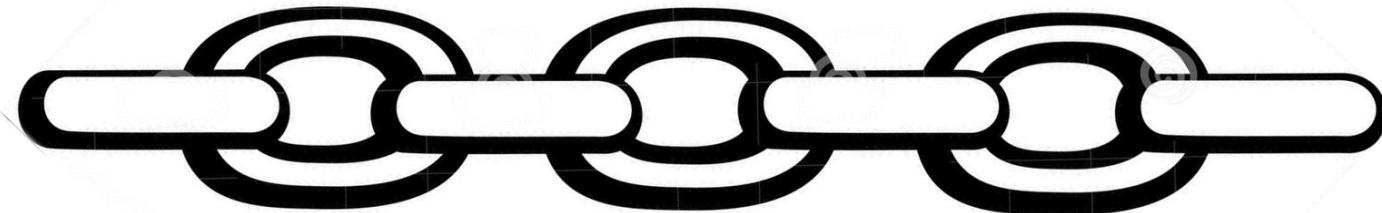
Fundamentos: Autenticidade

- Assinatura Digital que substitui a assinatura física.
- É possível confirmar que a assinatura foi feita pelo dono (não repúdio).
- Evita alterações ao documento assinado (integridade).



Fundamentos: Imutabilidade

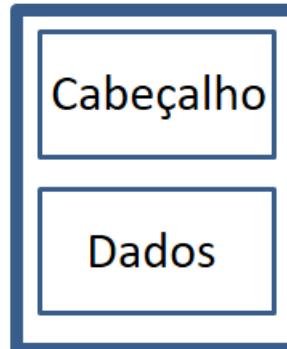
- Uma vez que um evento* for autenticado e registrado, ninguém poderá mudá-lo
- Intuitivamente, cada elo de uma cadeia é um evento, encadeado com outros



* Por evento entenda-se a dados que podem representar uma transação financeira, o vencimento de um medicamento, a venda de um imóvel, etc.

Fundamentos: Imutabilidade

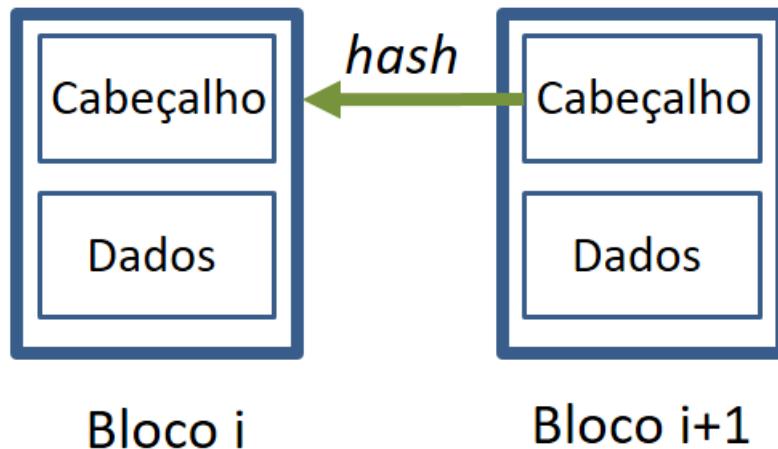
- Uma vez que um evento for autenticado e registrado, ninguém poderá mudá-lo
- Intuitivamente, cada elo de uma cadeia é um evento, encadeado com outro



Bloco i

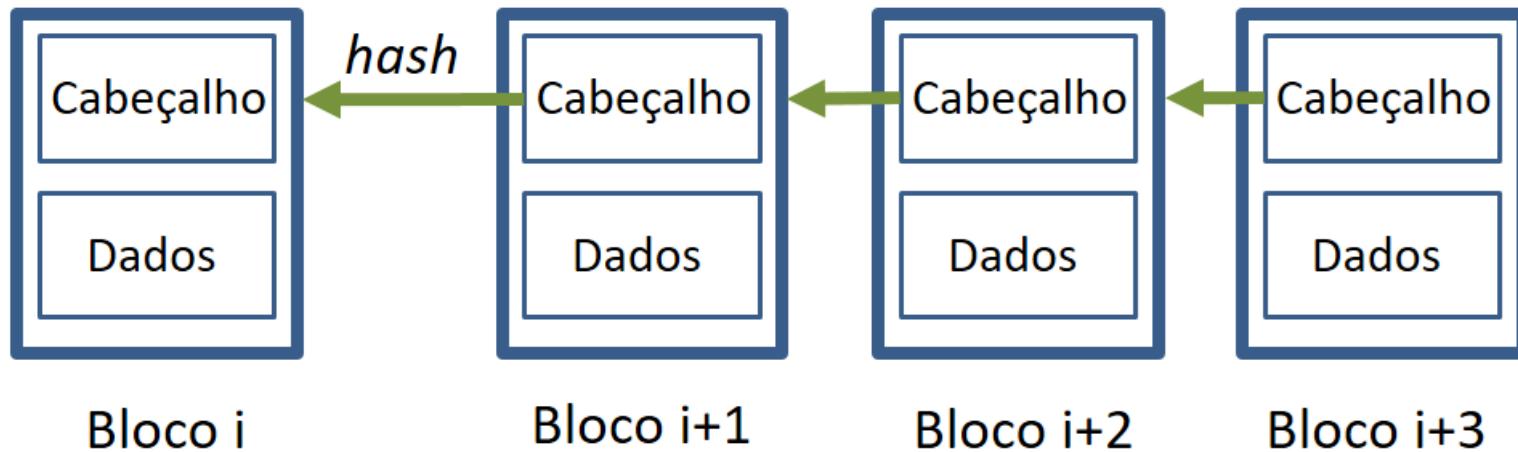
Fundamentos: Imutabilidade

- Uma vez que um evento for autenticado e registrado, ninguém poderá mudá-lo
- Intuitivamente, cada elo de uma cadeia é um evento, encadeado com outro



Fundamentos: Imutabilidade

- Uma vez que um evento for autenticado e registrado, ninguém poderá mudá-lo
- Intuitivamente, cada elo de uma cadeia é um evento, encadeado com outro



Fundamentos: Transparência

- Como os eventos são autênticos e imutáveis, podem ser rastreados e auditados
- Mas, se o registro for anônimo, não será possível saber quem é o(a) responsável



Imagen: <https://www.pwc.co.uk/issues/futuretax/how-blockchain-technology-could-improve-tax-system.html>

Fundamentos: Tolerância a Falhas

- Os dados de uma Blockchain são sempre distribuídos em redes *peer-to-peer*
- Todos os nós (computadores) "devem" eventualmente **ter a mesma cadeia de eventos**
- Se um nó sair da rede, a cadeia não será perdida (replicação).



Imagen: <https://medium.com/@vdenotaris/how-i-did-implement-my-first-blockchain-network>

3. Revisão histórica

1ª geração: Moedas Digitais

- Moeda virtual alternativa que surge em 2009
- Não atrelada a bancos ou governos
- Criadas através de um processo computacional
- As transações são realizadas entre pessoas anônimas (sem intermediários)
- Tão anônimo que até hoje não se sabe quem é Satoshi Nakamoto
- Tem como base a tecnologia Blockchain onde os eventos são movimentos financeiros



Atualmente existem mais de 9600 moedas virtuais parecidas ao Bitcoin (2100 em 2018) !

<https://coinmarketcap.com/pt-br/>

2ª geração: Contratos Inteligentes

- Surgem em 2015 (6 anos após o Bitcoin)
- Os eventos não estão atrelados ao contexto financeiro
- Permitem inserir funcionalidades de forma dinâmica

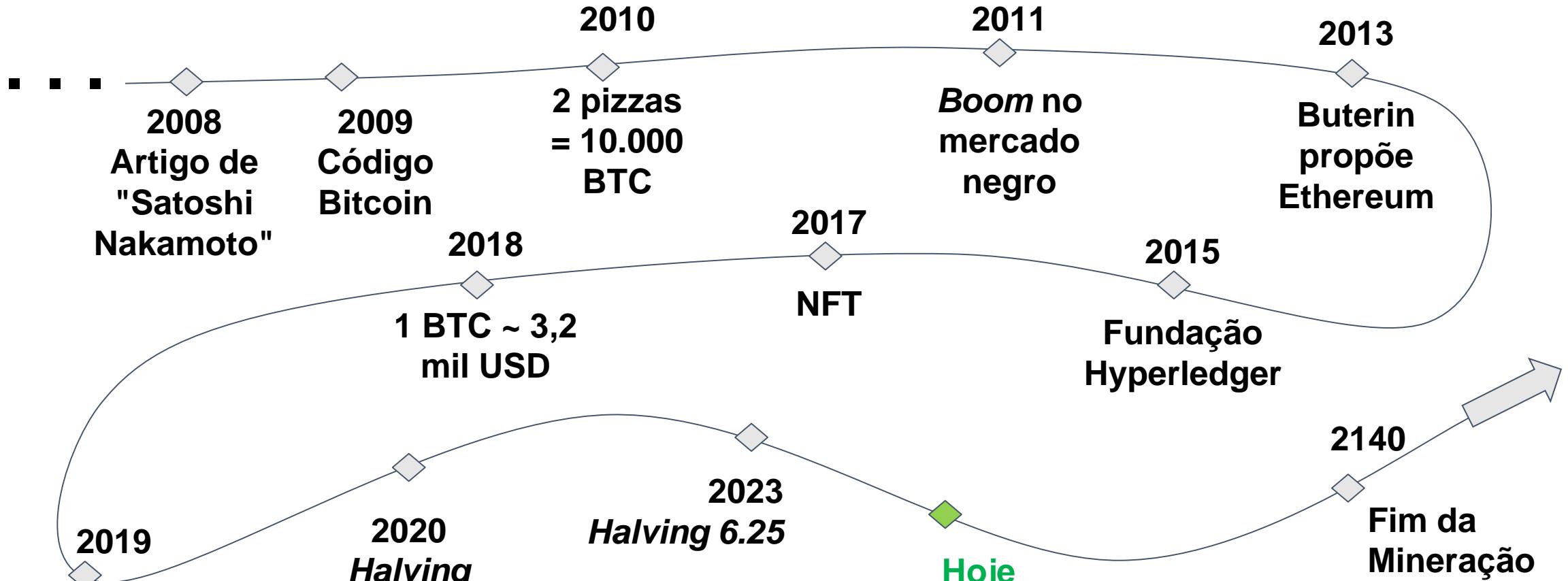
smartcontract

Verificar a data de vencimento de um lote

1. Obter os lotes gerenciados pelo hospital.
2. Recuperar as informações do lote (data, email responsável).
3. Verificar se a data de vencimento é maior que a data atual.
4. Se for maior, enviar um email para o responsável.



Linha do tempo (incompleta)



* Valores e datas aproximadas

4. Como funciona a Blockchain?

Como funciona a Blockchain?

- Visão geral
- Assinatura Digital
- Bloco
- Transação
- Tipos de Blockchain
- Consenso

Como funciona: Visão Geral

1. A pessoa “A” cria um evento, assina o mesmo e o envia para a rede

Exemplos de eventos:

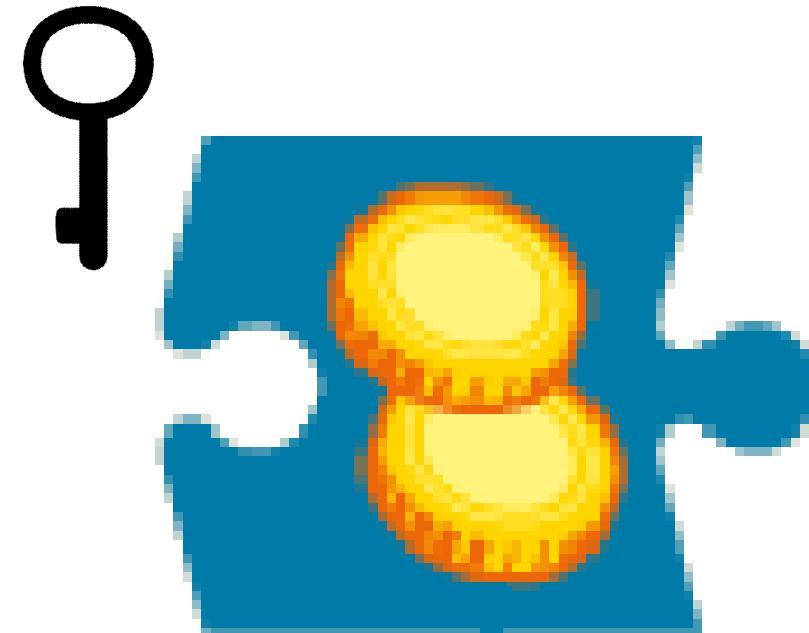
- Transferência de dinheiro de A para B
- Certidão de posse de uma casa
- Registro de um prontuário médico
- Inserção da quilometragem do carro



Para o exemplo a seguir veremos um evento de transferência de dinheiro de A para B como no Bitcoin.

Como funciona: Visão Geral

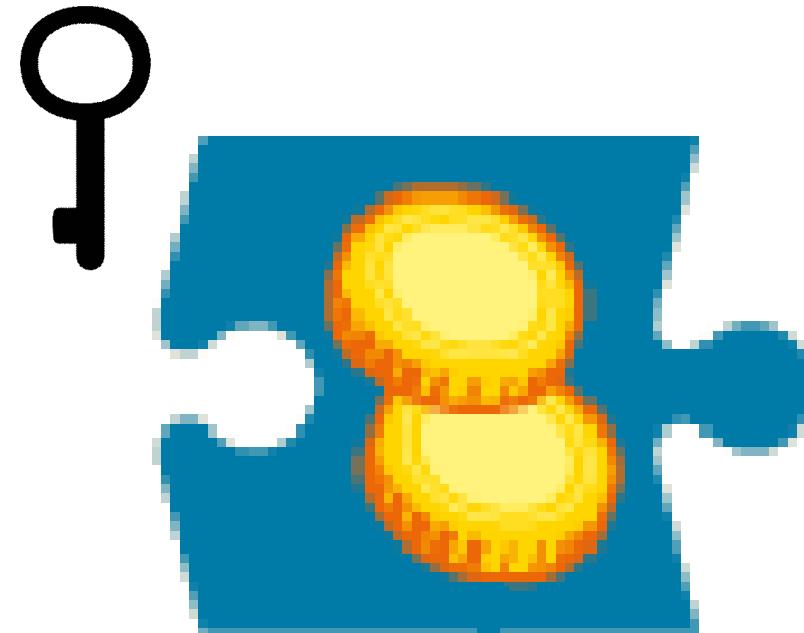
2. O evento assinado pela pessoa “A” é inserido em um “bloco” por um minerador



Como funciona: Visão Geral

2. O evento assinado pela pessoa “A” é inserido em um “bloco” por um minerador usando um mecanismo denominado prova de trabalho – PoW

(mais adiante veremos como funciona esse mecanismo)



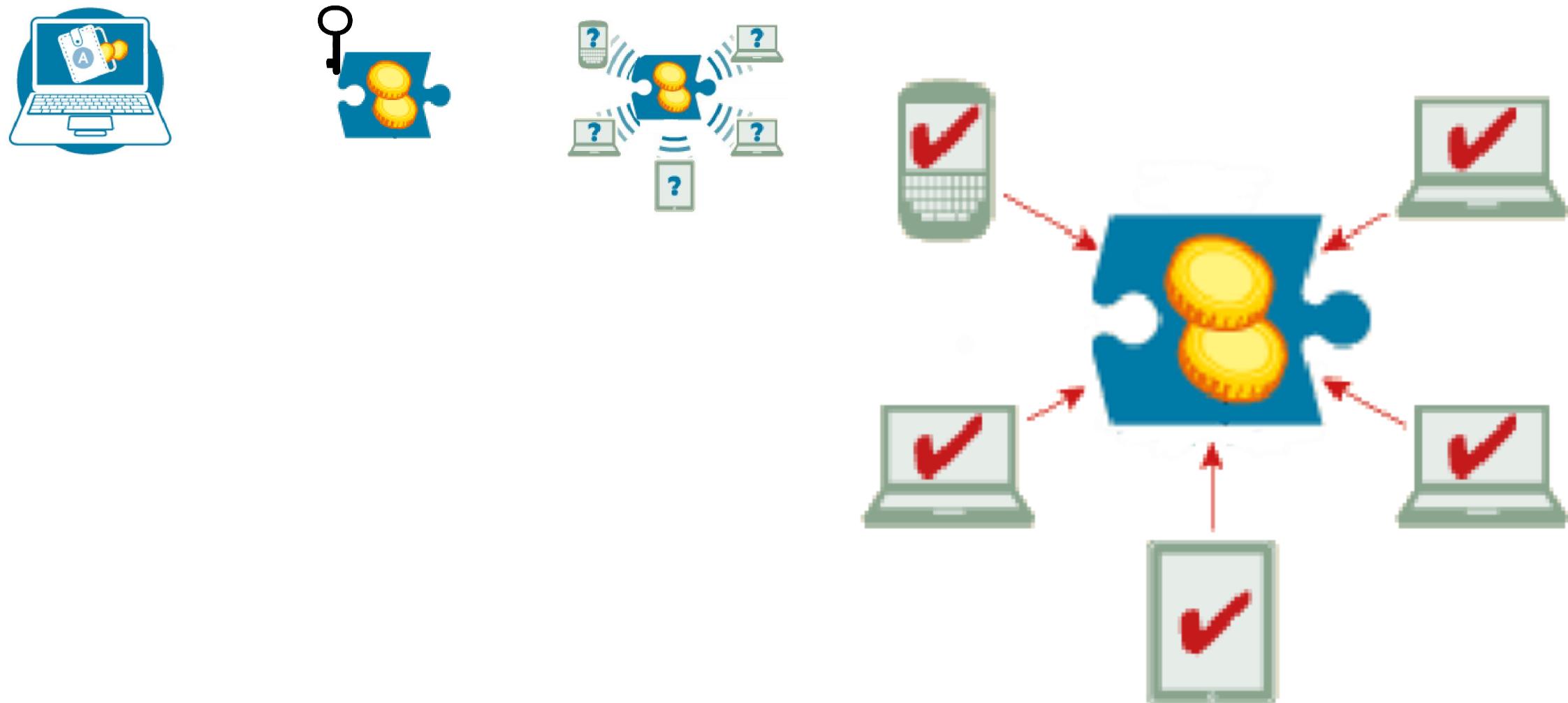
Como funciona: Visão Geral

3. O bloco é transmitido a todos os participantes da rede



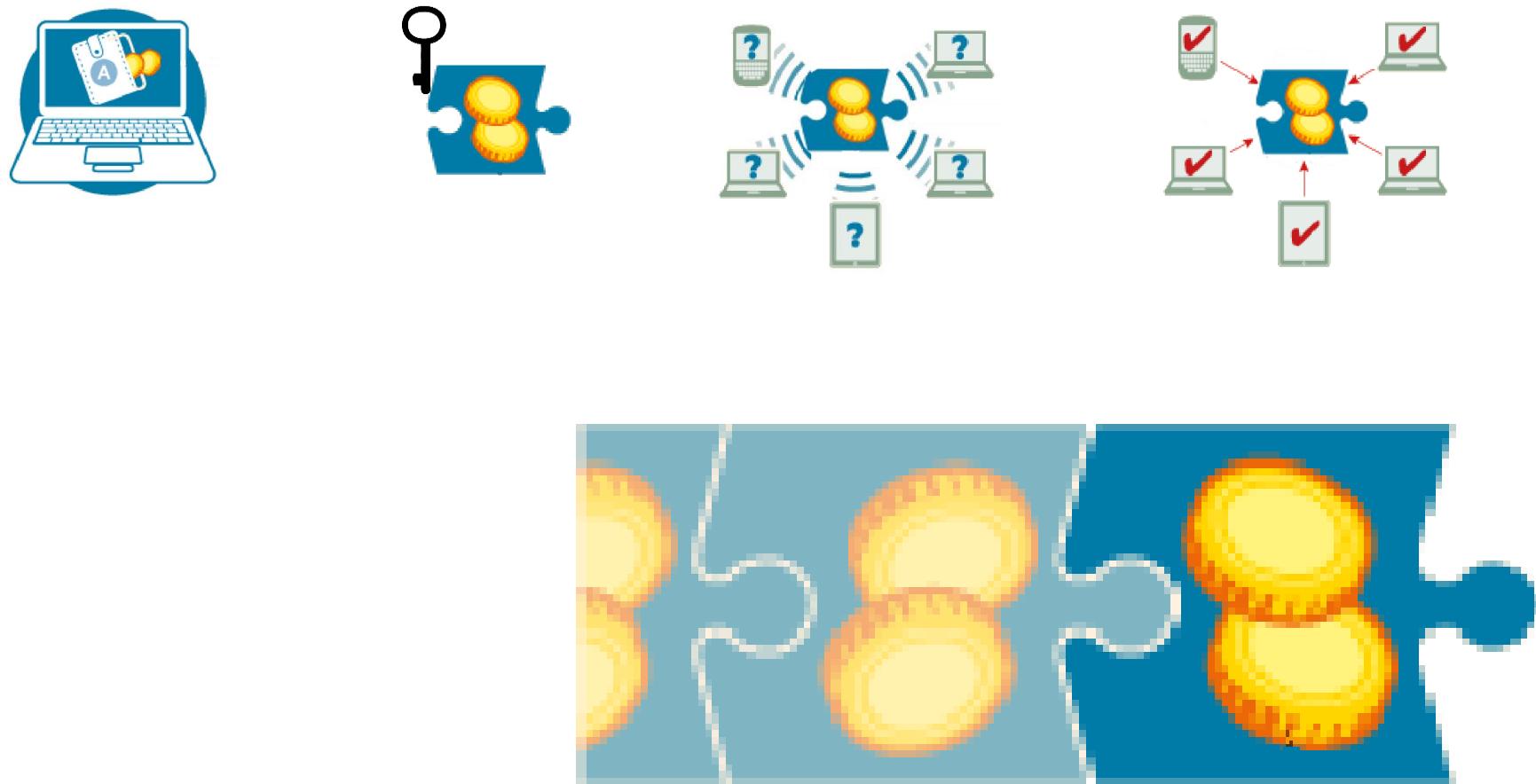
Como funciona: Visão Geral

4. Os participantes da rede validam o bloco e os eventos contidos nele



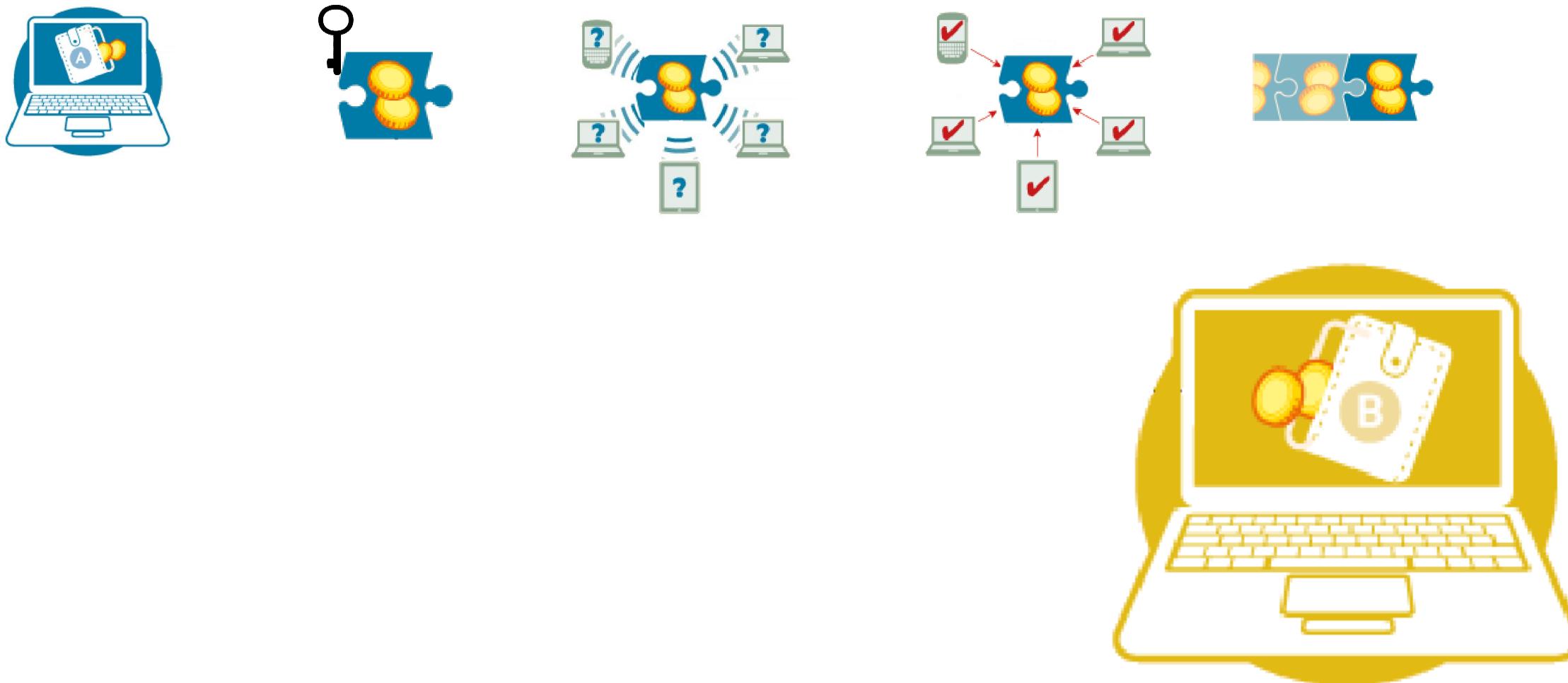
Como funciona: Visão Geral

4. O bloco é adicionado à cadeia por todos os participantes usando consenso



Como funciona: Visão Geral

5. A pessoa “B”, que esperava o evento (transferência de dinheiro), retira o dinheiro

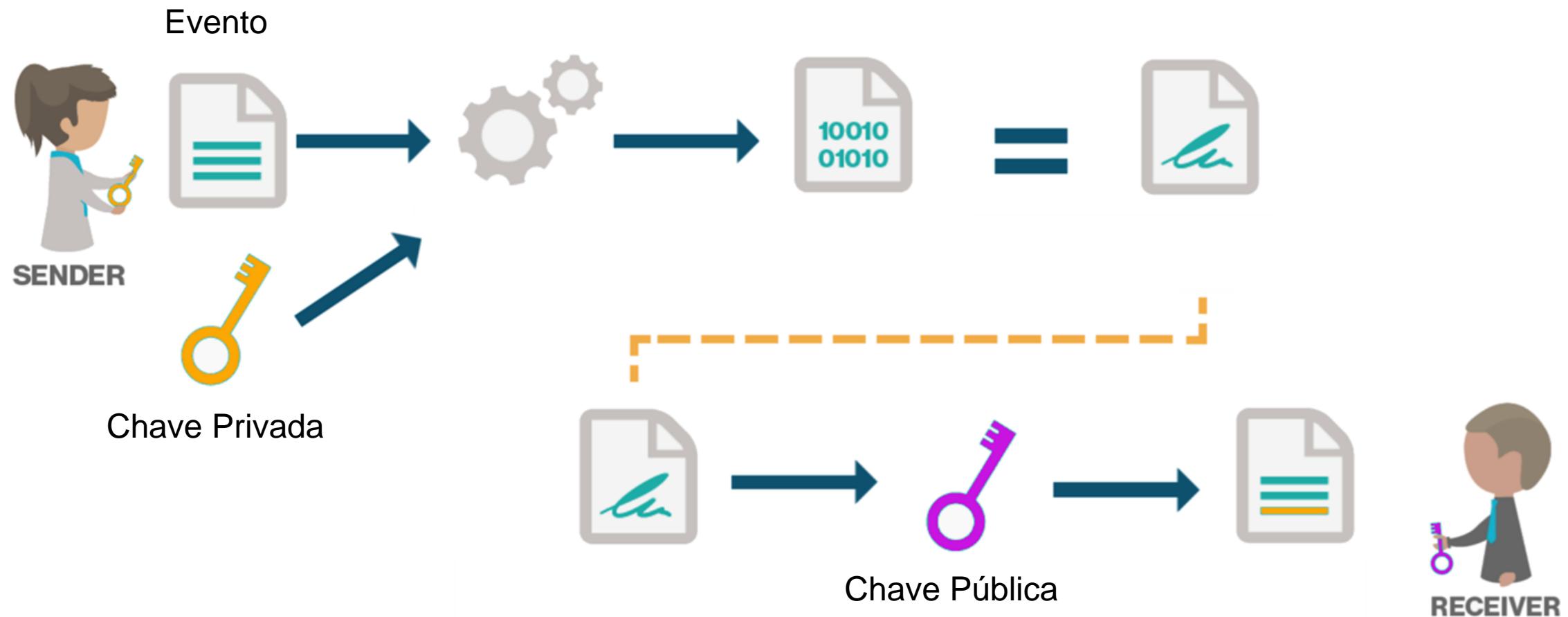


Como funciona a Blockchain?

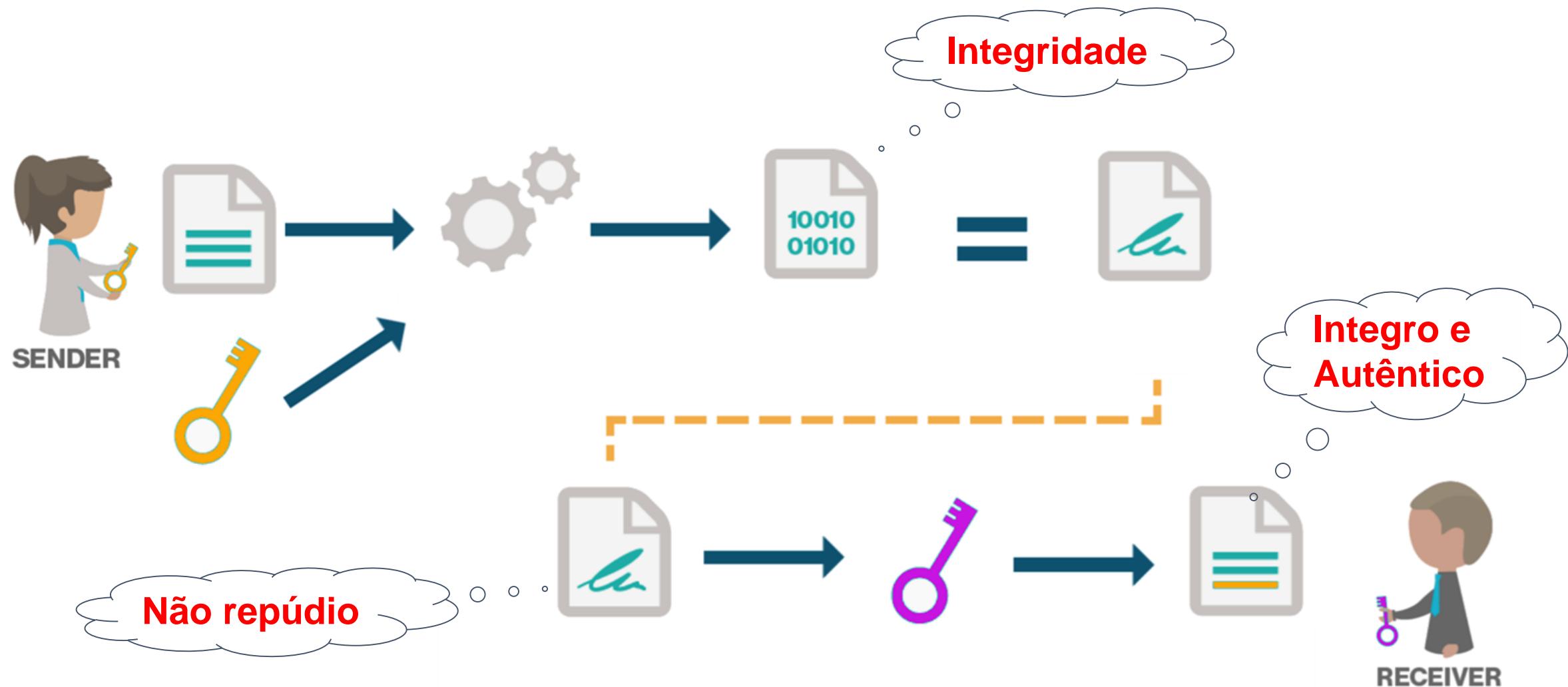
- Visão geral
- Assinatura Digital
- Bloco
- Transação
- Tipos de Blockchain
- Consenso

Como funciona: Assinatura Digital

Usada para autenticar o evento e verificar que não foi alterado



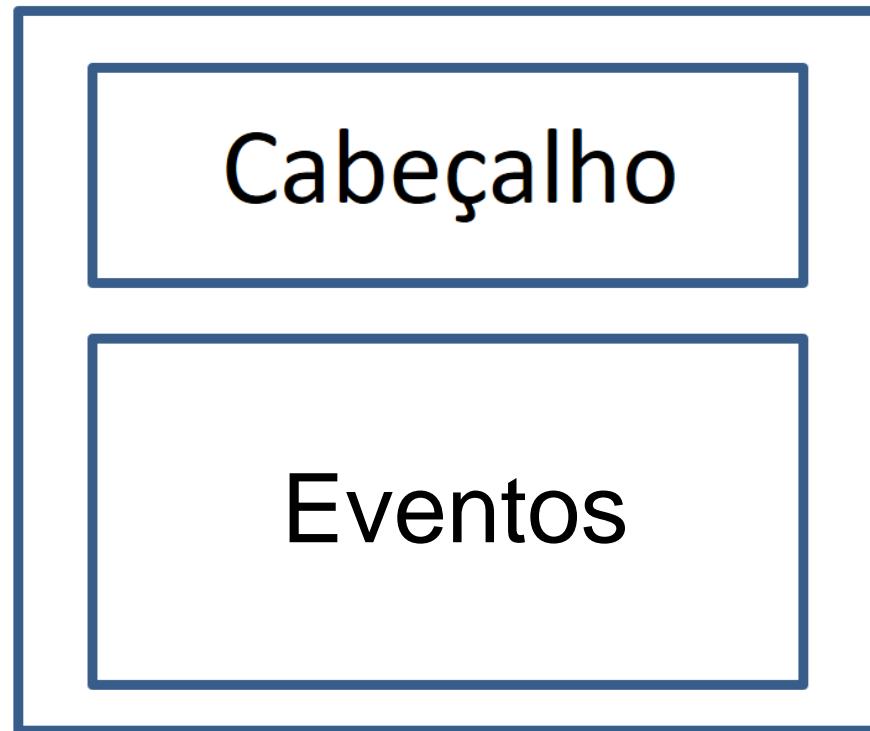
Como funciona: Assinatura Digital



Como funciona a Blockchain?

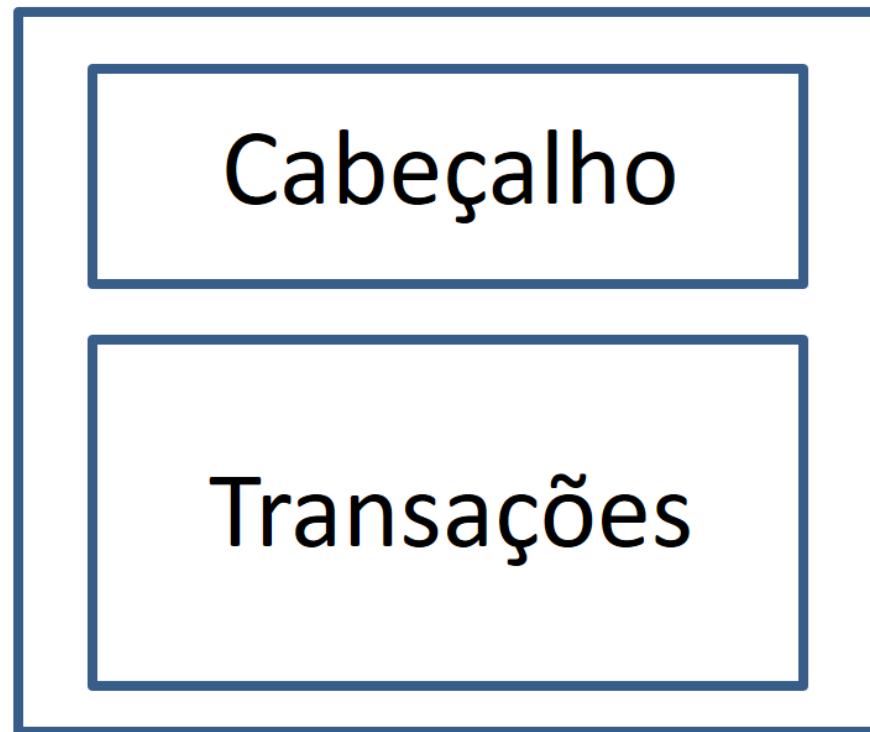
- Visão geral
- Assinatura Digital
- **Bloco**
- Transação
- Tipos de Blockchain
- Consenso

Como funciona: Bloco

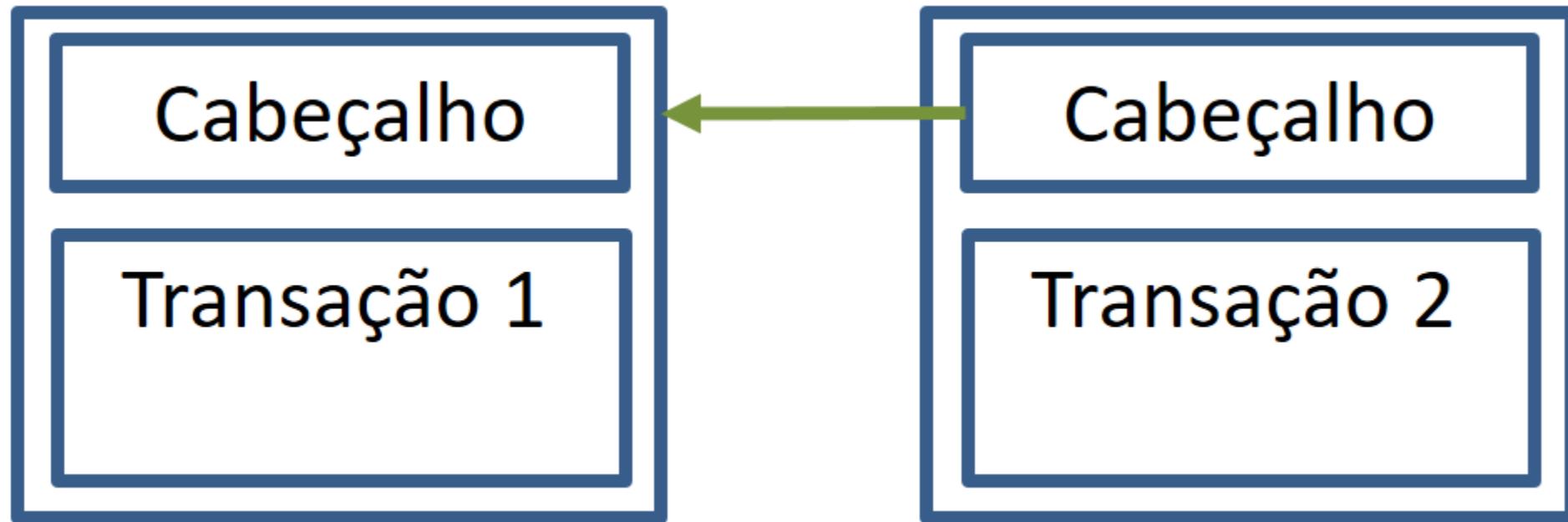


Chamaremos os eventos de transações para manter o padrão das blockchains

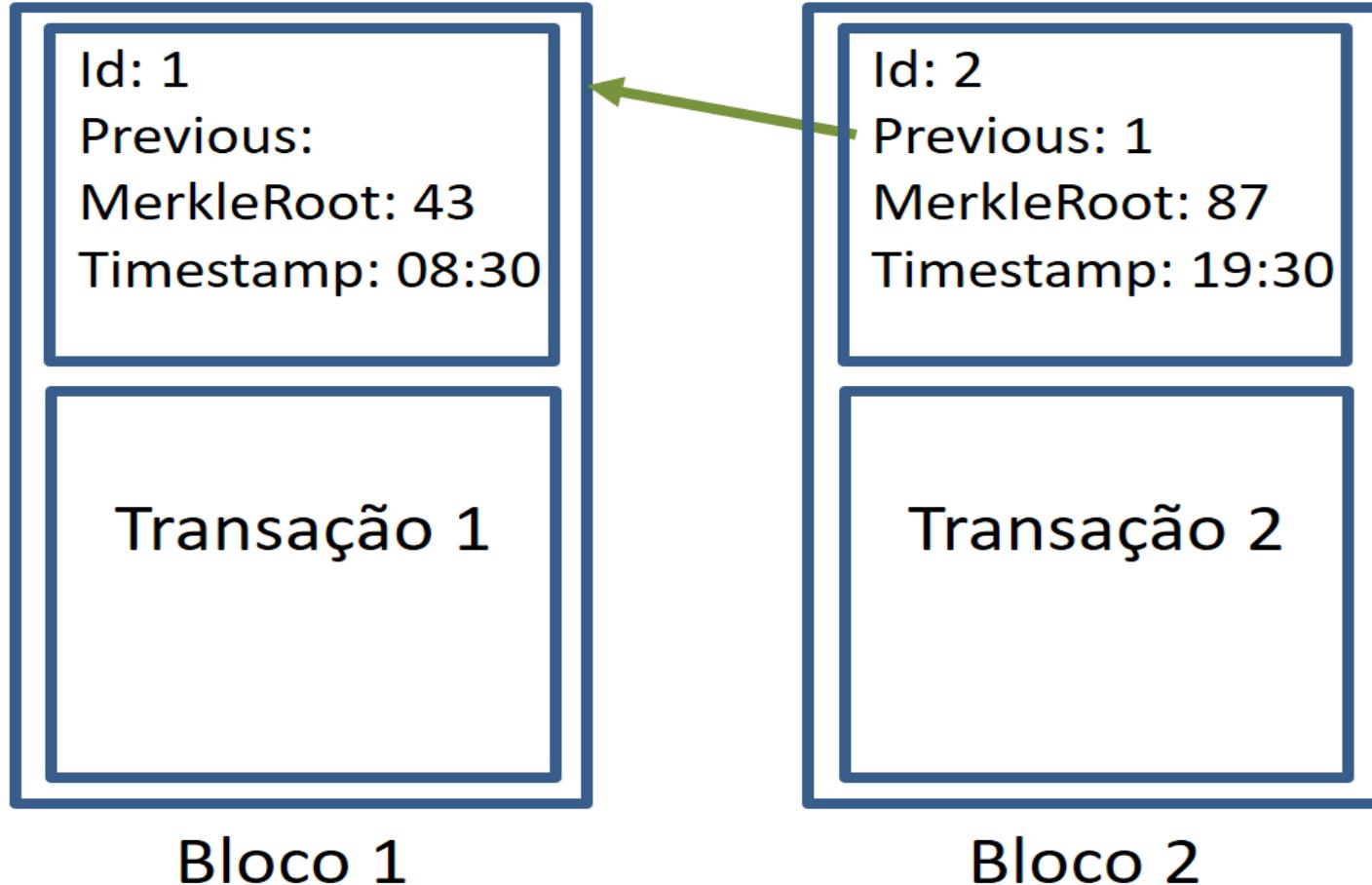
Como funciona: Bloco



Como funciona: Bloco

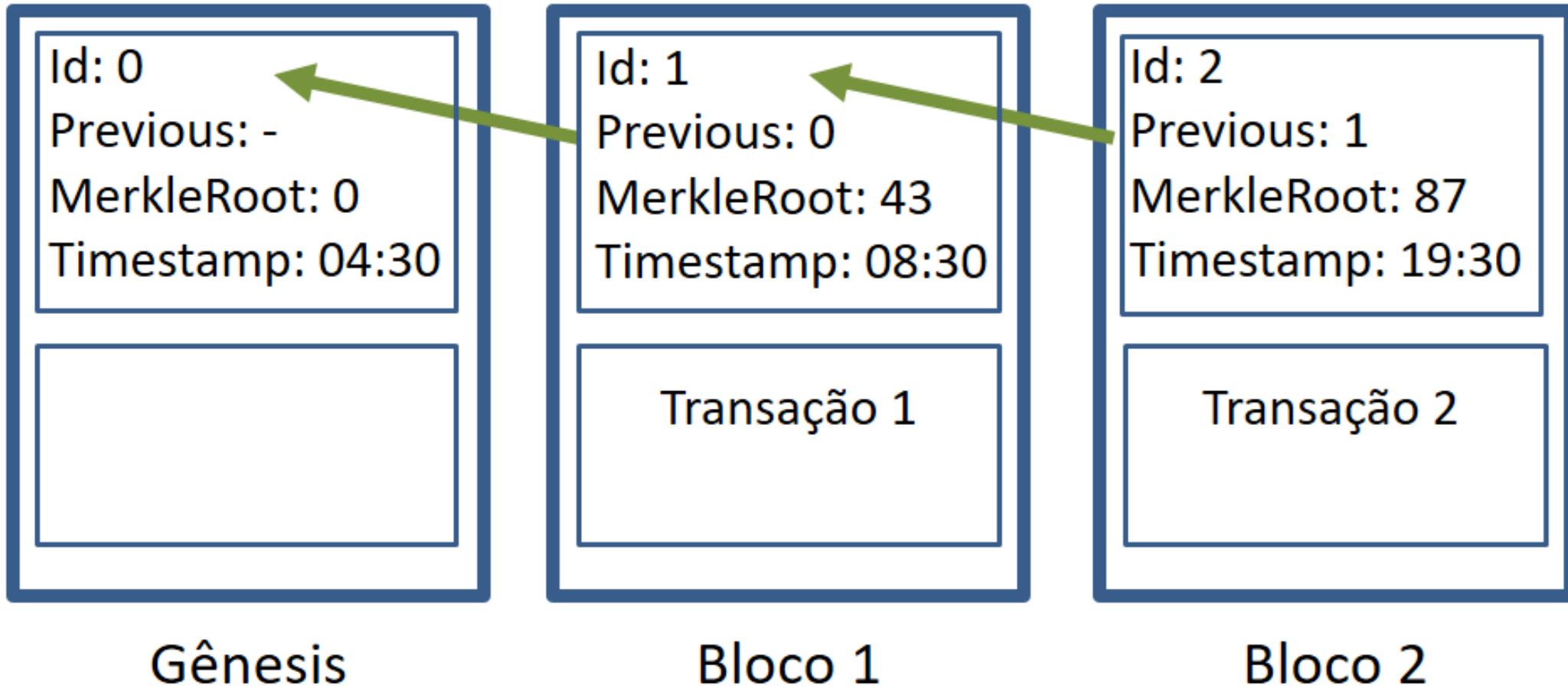


Como funciona: Bloco



Id é obtido do hash do header

Como funciona: Bloco



Como funciona: Cadeia de Blocos

Bitcoin block 784000  mined by

<https://blockexplorer.com/>

Time 2023-04-05 03:27:25

Transactions 1 617

Size 2 329 981 bytes

Stripped size 554 359 bytes

Weight 3 993 058

Block difficulty 83 762 632 792 124

Network difficulty 46 843 400 286 276

Version 0x2a978000

Bits 0x1706023e

Nonce 0x3ebac564

Block [00000000000035c3f0d31e71a5ee24c5aaaf3354689f65bd7b07dee632](#) 

Previous block [0000000000000000488601fd3bcc7913bb9089595bd49f1990981d6366390](#) 

Next block [0000000000000000000022dda59323a317f53ec9ddf80a9e5a7764cd81390eece](#) 

Merkle root a48cf882d8573f4d6ec1438415953ad0773d4a74d4be1151b5e34158434b4206 

Id é obtido do
hash do header

Como funciona a Blockchain?

- Visão geral
- Assinatura Digital
- Bloco
- **Transação**
- Tipos de Blockchain
- Consenso

Como funciona: Transação

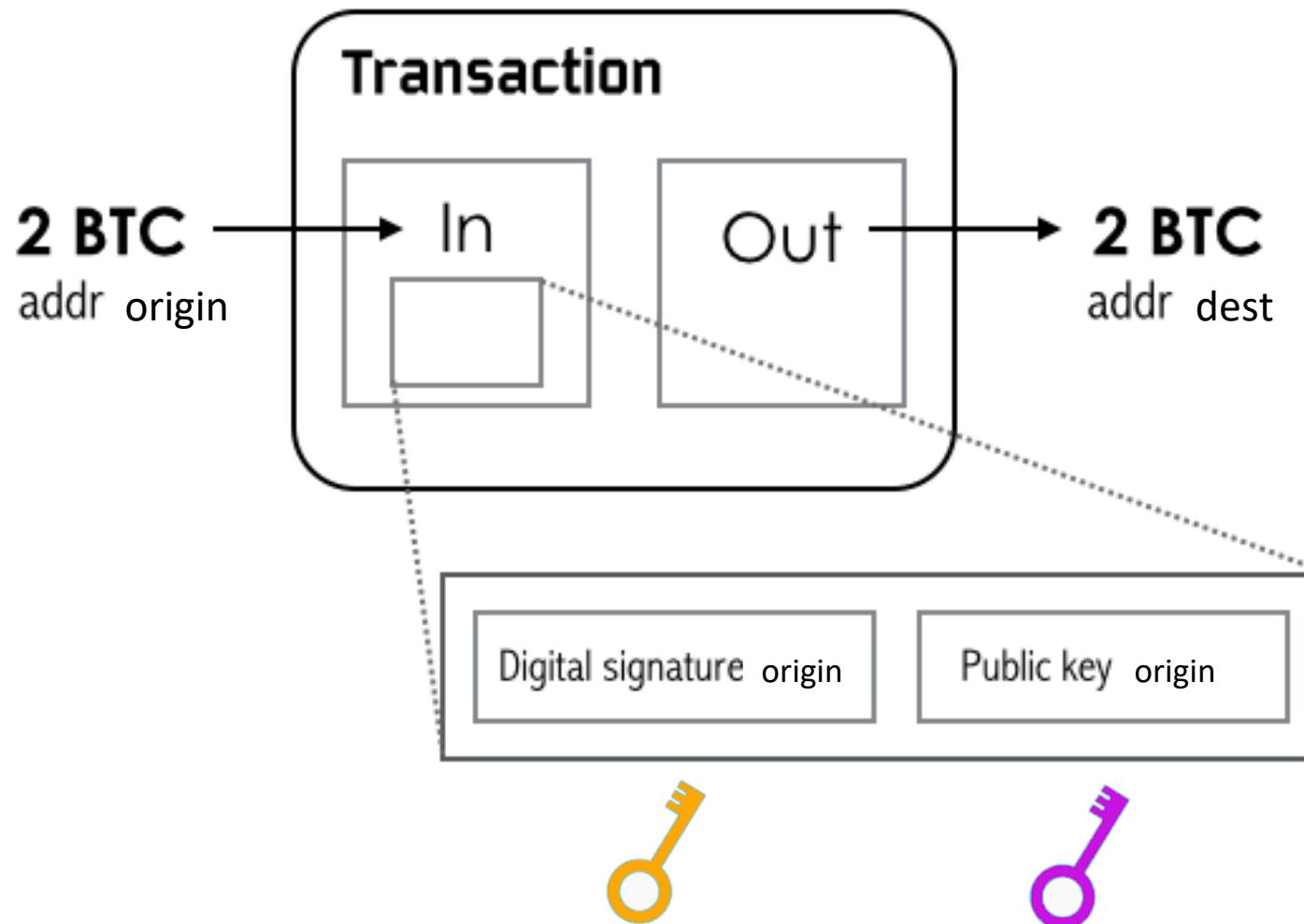
Nas Blockchains, o evento a ser registrado é denominado de transação

Transação foi o nome escolhido, pois nas Blockchains de 1^a geração só eram realizadas transações financeiras.

Porém, nas Blockchains de 2^a geração, uma transação pode representar diversos tipos de eventos, tais como:

- Transferência de dinheiro de A para B
- Certidão de posse de uma casa
- Registro de um prontuário médico
- Gestão da cadeia de suprimentos de medicamentos

Como funciona: Transação

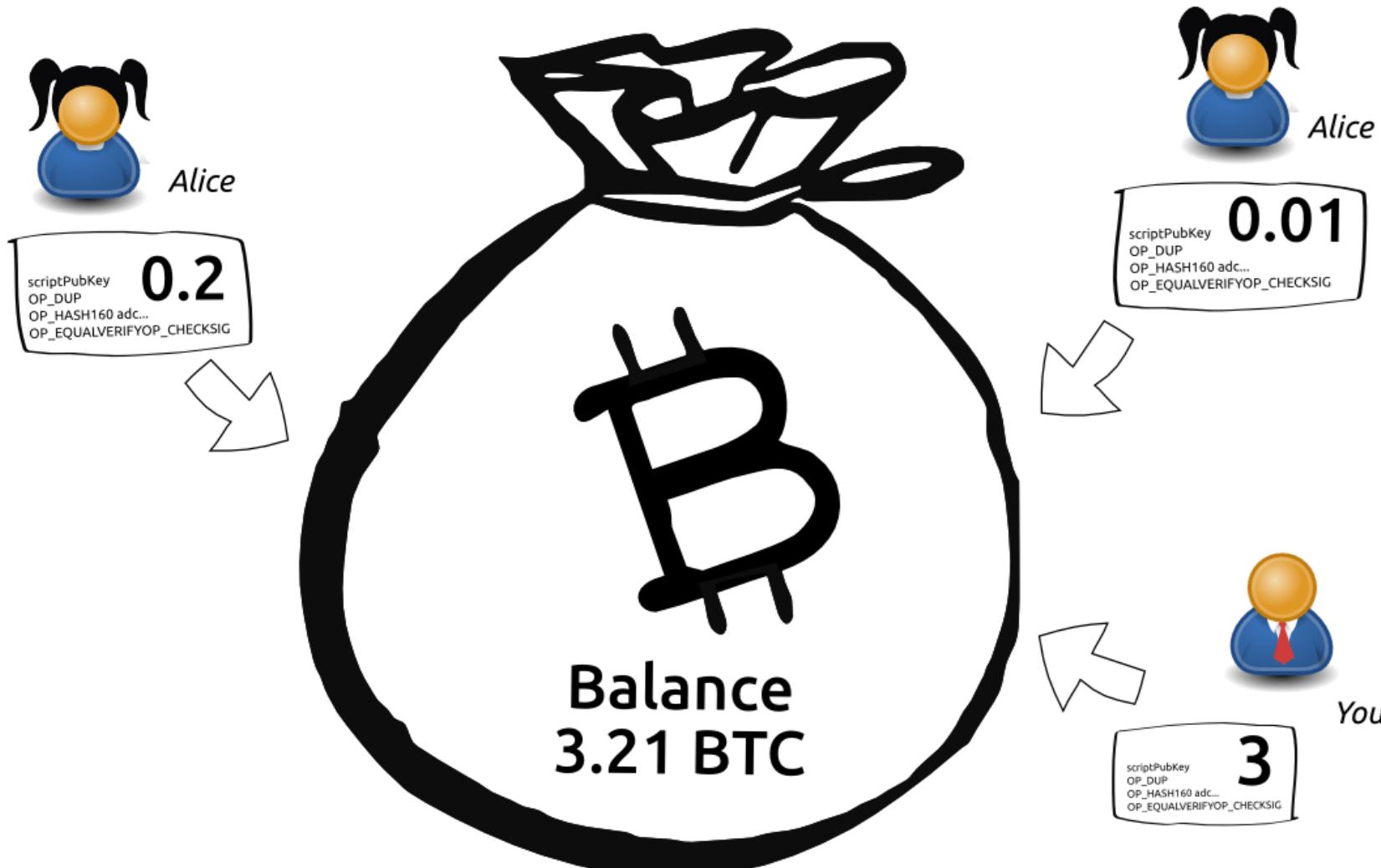


Como funciona: Transação

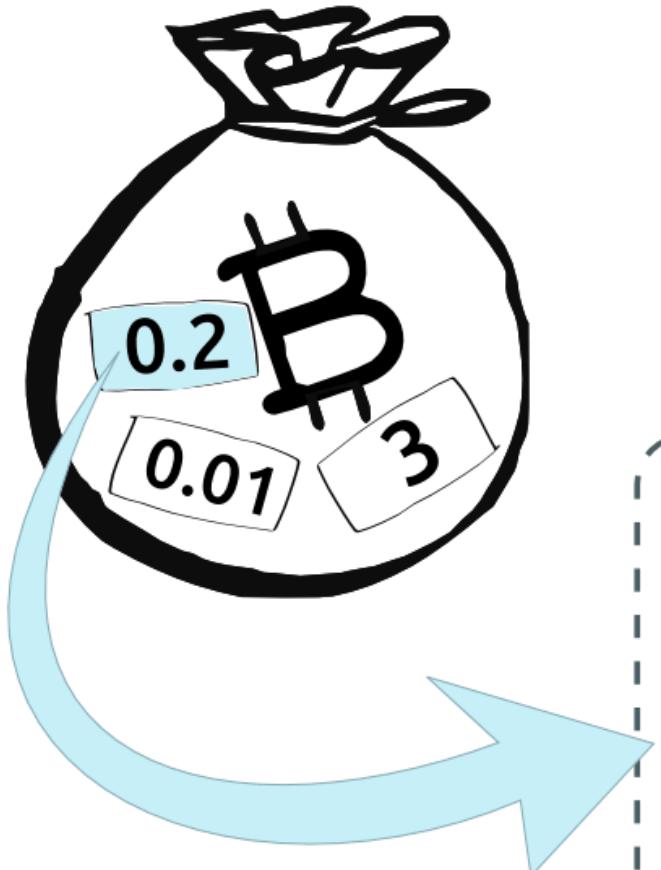
txid 90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219

```
"in": [
  {
    "prev_out": {
      "hash": "18798f8795ded46c3086f48d5bdabe10e1755524b43912320b81ef547b2f939a",
      "n": 0
    },
    "scriptSig": "3045022100c1efcad5cdcc0dcf7c2a79d9e1566523af9c7229c78ef71ee8b6300ab...[snip]"
  }
],
"out": [
  {
    "value": "5.93100000",
    "scriptPubKey": "OP_DUP OP_HASH160 4b358739fc7984b8101278988beba0cc00867adc OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
    "value": "1678.06900000",
    "scriptPubKey": "OP_DUP OP_HASH160 55368b388ccfe22a3f837c9eee93d053460db339 OP_EQUALVERIFY OP_CHECKSIG"
  }
]
```

Como funciona: Transação



Como funciona: Transação



input
0.2 BTC

IN OUT

0.2 0.2



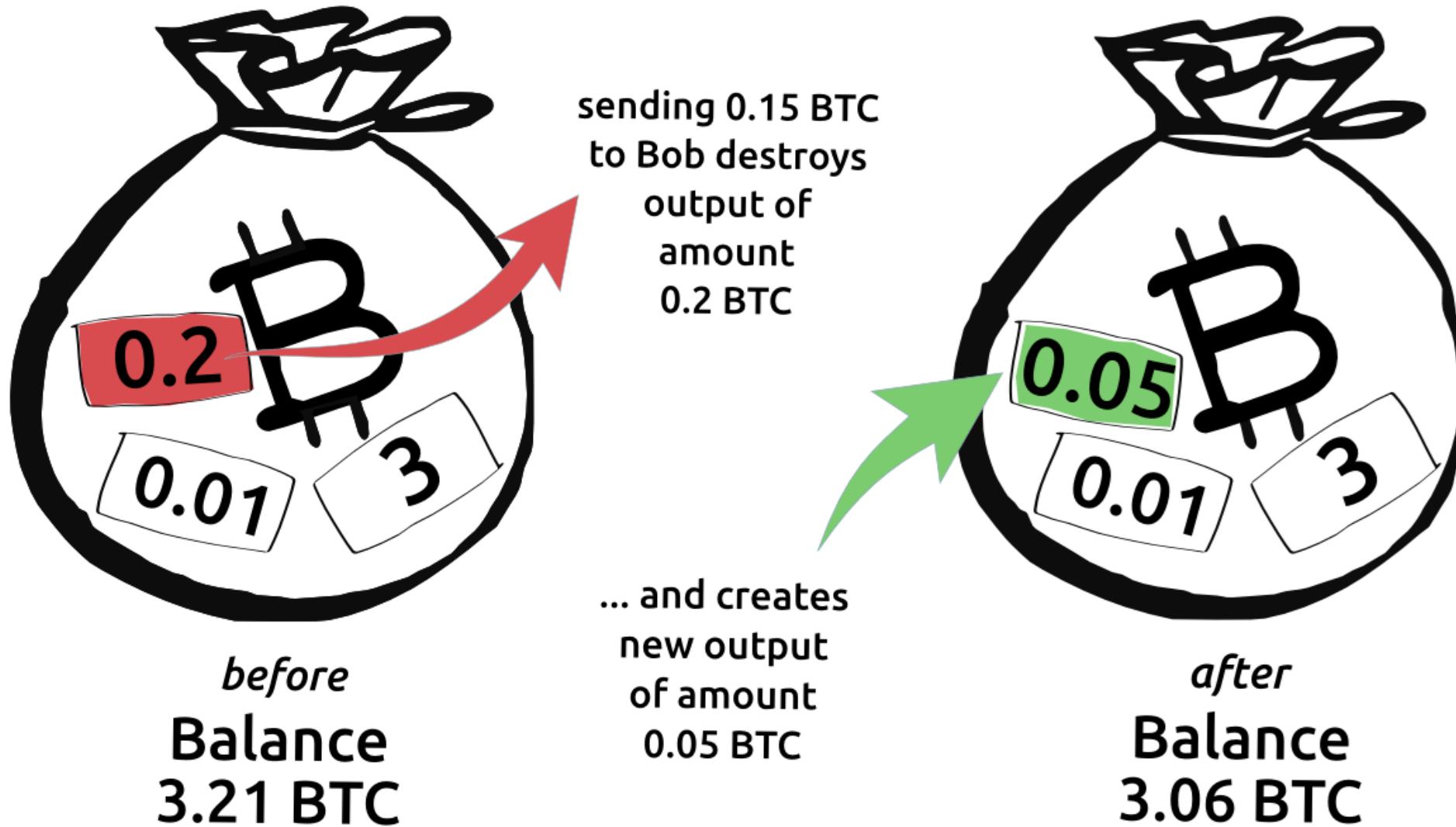
 **Bob**
output
0.15 BTC

spend output to address
1BOBgLmrdrtLCrDzBjuT4MZV1zBNw5HwJK1
(belonging to Bob)

output
0.05 BTC

"change" of the spend to Bob
is returned to your wallet as a
new output

Como funciona: Transação



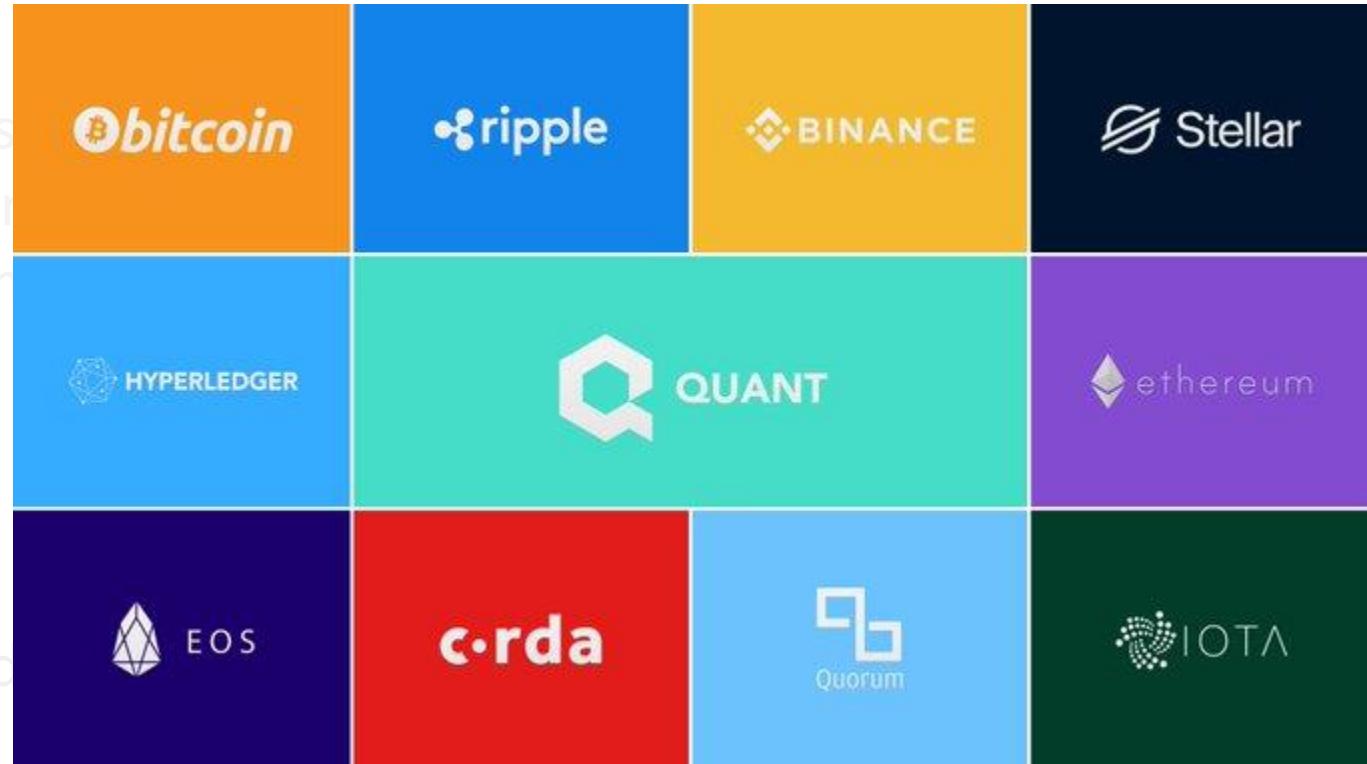
Como funciona a Blockchain?

- Visão geral
- Assinatura Digital
- Bloco
- Transação
- Tipos de Blockchain
- Consenso

Como funciona: Tipos

Não Permissionada

- Os participantes não precisam ser identificados
- Qualquer membro pode auditar o blockchain
- Total descentralização da informação
- Bitcoin e Ethereum



Permissionada

- Os participantes precisam ser identificados (real)
- Somente alguns membros autorizados podem auditar o blockchain (<https://twitter.com/DreadBong0/status/1173554670914154497>)
- A informação está descentralizada, porém em alguns participantes
- Hyperledger.

Como funciona: Tipos

Não Permissionada

- Os participantes não precisam ser identificados (total anonimato)
- Qualquer membro pode auditar a cadeia
- Total descentralização da informação
- Bitcoin e Ethereum

Permissionada

- Os participantes precisam ser identificados (sem anonimato, geralmente na vida real)
- Somente alguns membros autorizados podem auditar a cadeia
- A informação está descentralizada, porém em alguns participantes
- Hyperledger.

Como funciona: Tipos

Não Permissionada

- Os participantes não precisam ser identificados (total anonimato)
- Qualquer membro pode auditar a cadeia
- Total descentralização da informação
- Bitcoin e Ethereum

Permissionada

- Os participantes precisam ser identificados (normalmente sem anonimato)
- Somente alguns membros autorizados podem auditar a cadeia
- A informação está descentralizada, porém em alguns participantes
- Hyperledger

Como funciona a Blockchain?

- Visão geral
- Assinatura Digital
- Bloco
- Transação
- Tipos de Blockchain
- Consenso

Como funciona: Consenso

Em geral, o objetivo do consenso é que os participantes cheguem a um acordo sobre um determinado valor.

No caso da Blockchain, o acordo determina qual bloco deve ser inserido no final da cadeia

Como funciona: Consenso

Em geral, o objetivo do consenso é que os participantes cheguem a um acordo sobre um determinado valor.

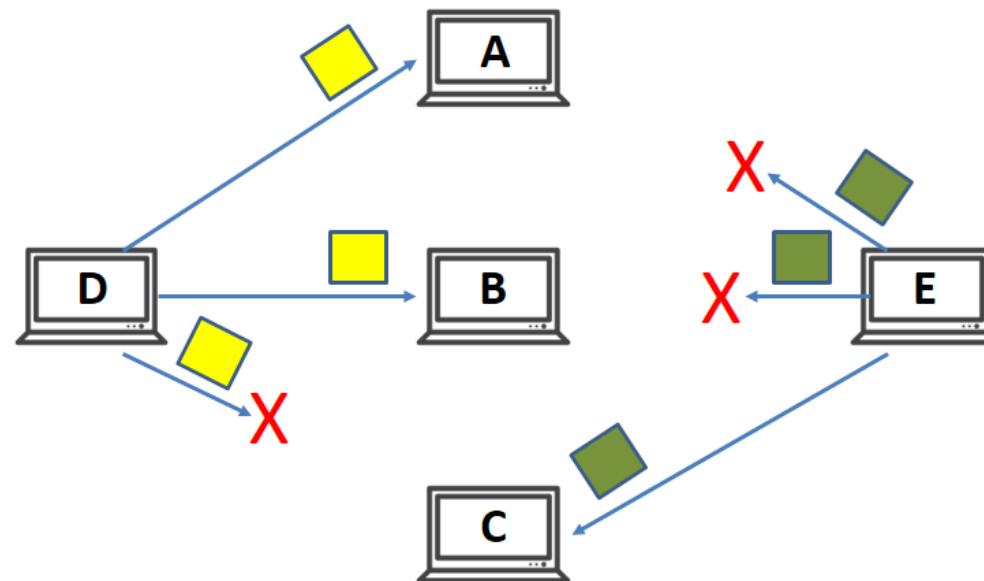
No caso da Blockchain, o acordo determina qual bloco deve ser inserido no final da cadeia



Como funciona: Consenso

Em geral, o objetivo do consenso é que os participantes cheguem a um acordo sobre um determinado valor.

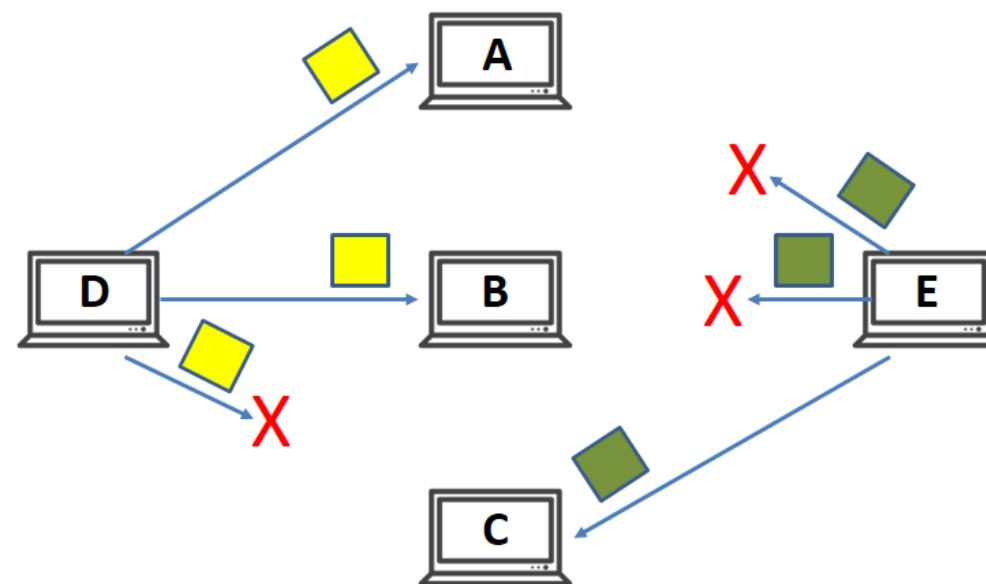
No caso da Blockchain, o acordo determina qual bloco deve ser inserido no final da cadeia



Como funciona: Consenso

Em geral, o objetivo do consenso é que os participantes cheguem a um acordo sobre um determinado valor.

No caso da Blockchain, o acordo determina qual bloco deve ser inserido no final da cadeia



Facebook e Instagram ficam fora do ar no Brasil e no mundo

Rede social passa pela segunda instabilidade neste mês. #FacebookDown já é o assunto mais comentado do mundo no Twitter

Por Nicolly Vimercate, da Redação
25/11/2018 | 11h21 · Atualizado há 5 meses



Google fora do ar? Analytics, Drive, Gmail e YouTube ficam instáveis

Estados Unidos é o país mais afetado pelos problemas de conexão

Por Nicolly Vimercate, da Redação
02/06/2019 16h16 · Atualizado há 6 dias

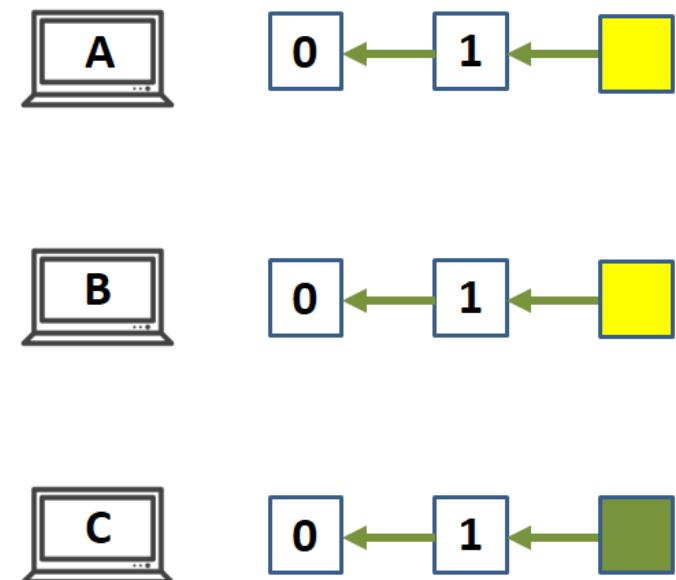


Como funciona: Consenso

Em geral, o objetivo do consenso é que os participantes cheguem a um acordo sobre um determinado valor.

No caso da Blockchain, o acordo determina qual bloco deve ser inserido no final da cadeia

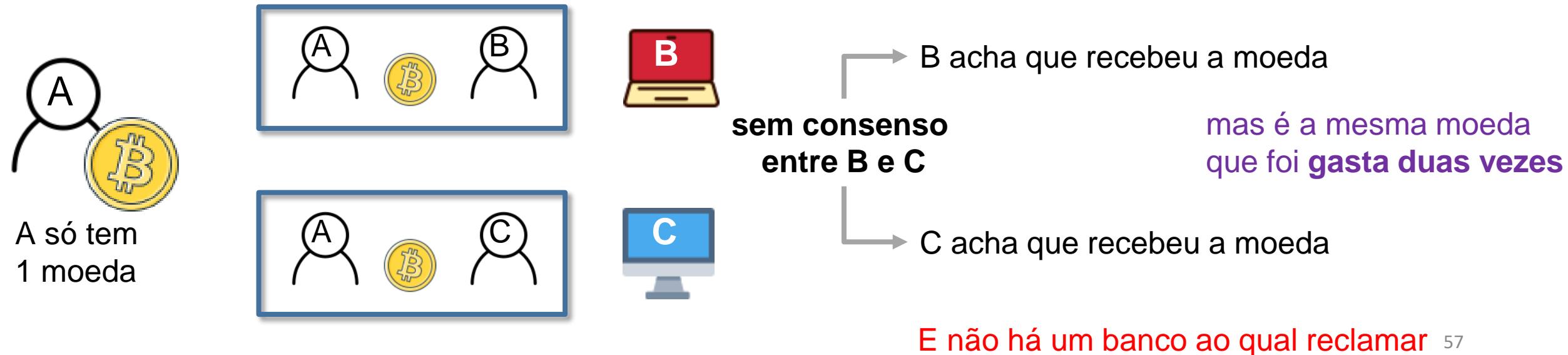
NÃO HOUVE ACORDO !!



Como funciona: Consenso

Na mídia, dizia-se em 2008 que a Blockchain do Bitcoin resolia o problema do consenso ...

- Para que seria necessário o consenso no Bitcoin?
Evitar o **gasto duplo** (no caso de criptomoedas)



Como funciona: Consenso

As Blockchains atuais utilizam diversos tipos de consenso:

- Consenso via Paxos/RAFT/BFT (permissionada) → Hyperledger
Estudos desde os anos 70
Ordem **total** dos blocos adicionados
Sim precisa conhecer os N participantes
- Consenso via Prova de Trabalho - *PoW* (não permissionada) → Bitcoin
Estudos desde 2008
Ordem **eventual** dos blocos adicionados
Não precisa conhecer os N participantes

Mudança radical na forma de ver o consenso

5. Consenso

Consenso via Paxos/RAFT

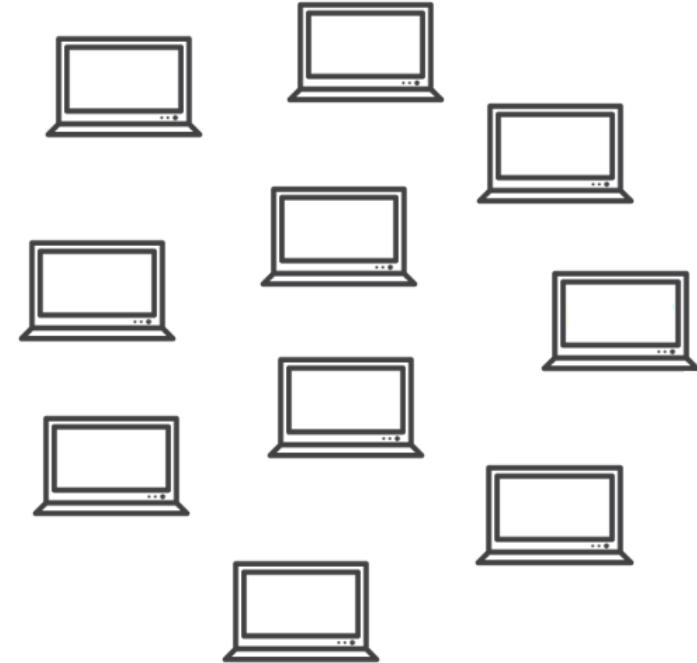


HYPERLEDGER

Consenso via Paxos/RAFT

Como adicionar um novo bloco no final da cadeia?

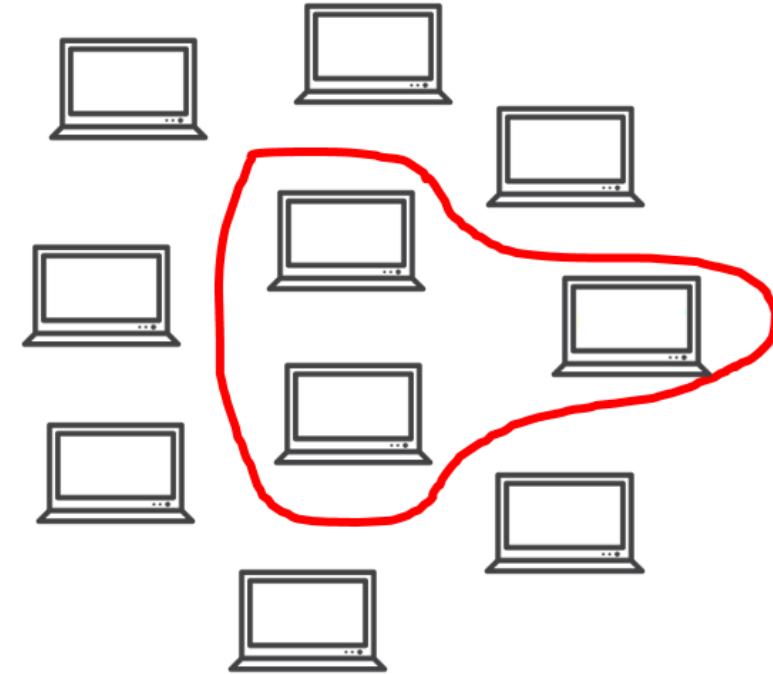
- **Alguns** participantes (bem definidos) serão encarregados por chegar ao acordo



Consenso via Paxos/RAFT

Como adicionar um novo bloco no final da cadeia?

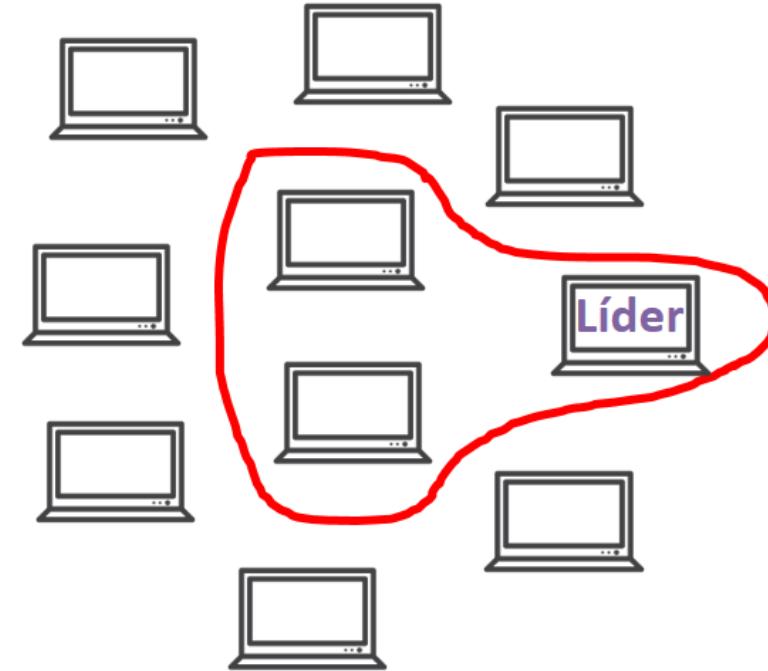
- **Alguns** participantes (bem definidos) serão encarregados por chegar ao acordo



Consenso via Paxos/RAFT

Como adicionar um novo bloco no final da cadeia?

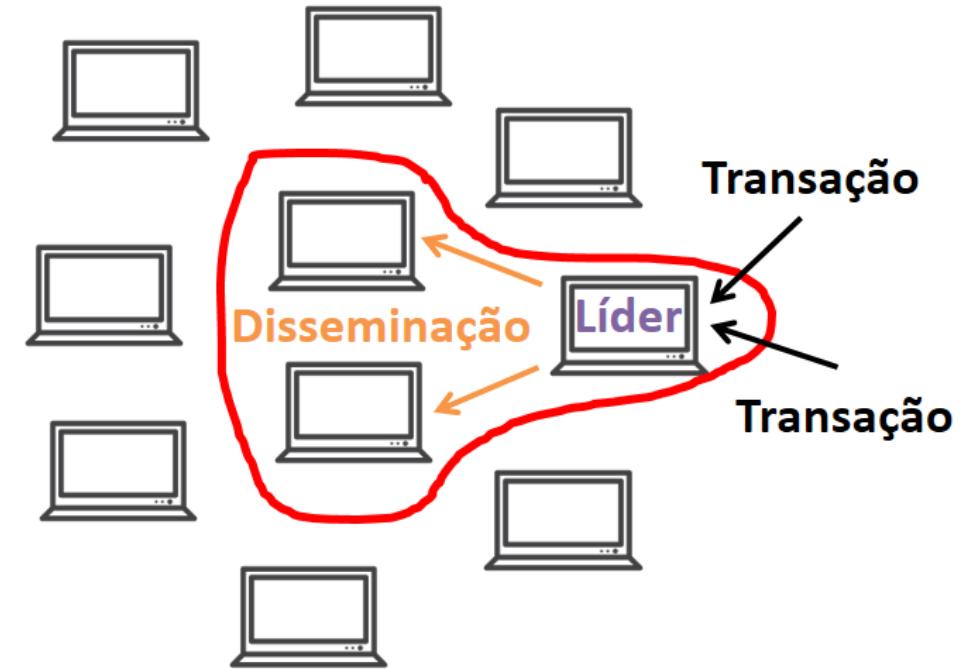
- **Alguns** participantes (bem definidos) serão encarregados por chegar ao acordo
- Escolha de um **Líder** entre esses participantes



Consenso via Paxos/RAFT

Como adicionar um novo bloco no final da cadeia?

- **Alguns** participantes (bem definidos) serão encarregados por chegar ao acordo
- Escolha de um **Líder** entre esses participantes
- Quando escolhido, o **Líder** será o responsável por receber as transações, criar o bloco e **disseminar** essa informação aos outros.
- Não há recompensa associada nesse processo



Capítulo 8

Consenso via PoW + Longest-Chain



bitcoin

Consenso via PoW + Longest-Chain

Como adicionar um novo bloco no final da cadeia?

- Qualquer participante da rede deve resolver um problema matemático complexo associado ao novo bloco (*proof-of-work PoW*)
- Processo denominado de **mineração**: cria o bloco com o uso do *nonce*, *difficulty target* e apontando o bloco para o *previous*
- Quando resolvido, o participante adiciona o novo bloco em sua cadeia e dissemina essa informação aos outros.
- Se conseguir adicioná-lo nos outros, receberá uma recompensa.

Consenso via PoW + Longest-Chain

Como adicionar um novo bloco no final da cadeia?

- Qualquer participante da rede deve resolver um problema matemático complexo associado ao novo bloco (*proof-of-work PoW*)
- Processo denominado de **mineração**: cria o bloco com o uso do *nonce*, *difficulty target* e apontando o bloco para o *previous*
- Quando resolvido, o participante adiciona o novo bloco em sua cadeia e dissemina essa informação aos outros.
- Se conseguir adicioná-lo nos outros, receberá uma recompensa.

Id: i

Previous: i - 1

MerkleRoot: 87

Timestamp: 19:30

Nonce

DifficultyTarget

Transações

Bloco i

Consenso via PoW + Longest-Chain

- Lembrando do Hash



- Sobre o *difficulty target*

Valor com uma quantidade de zeros no começo dele.

Definido pelo protocolo de forma dinâmica.

zeros

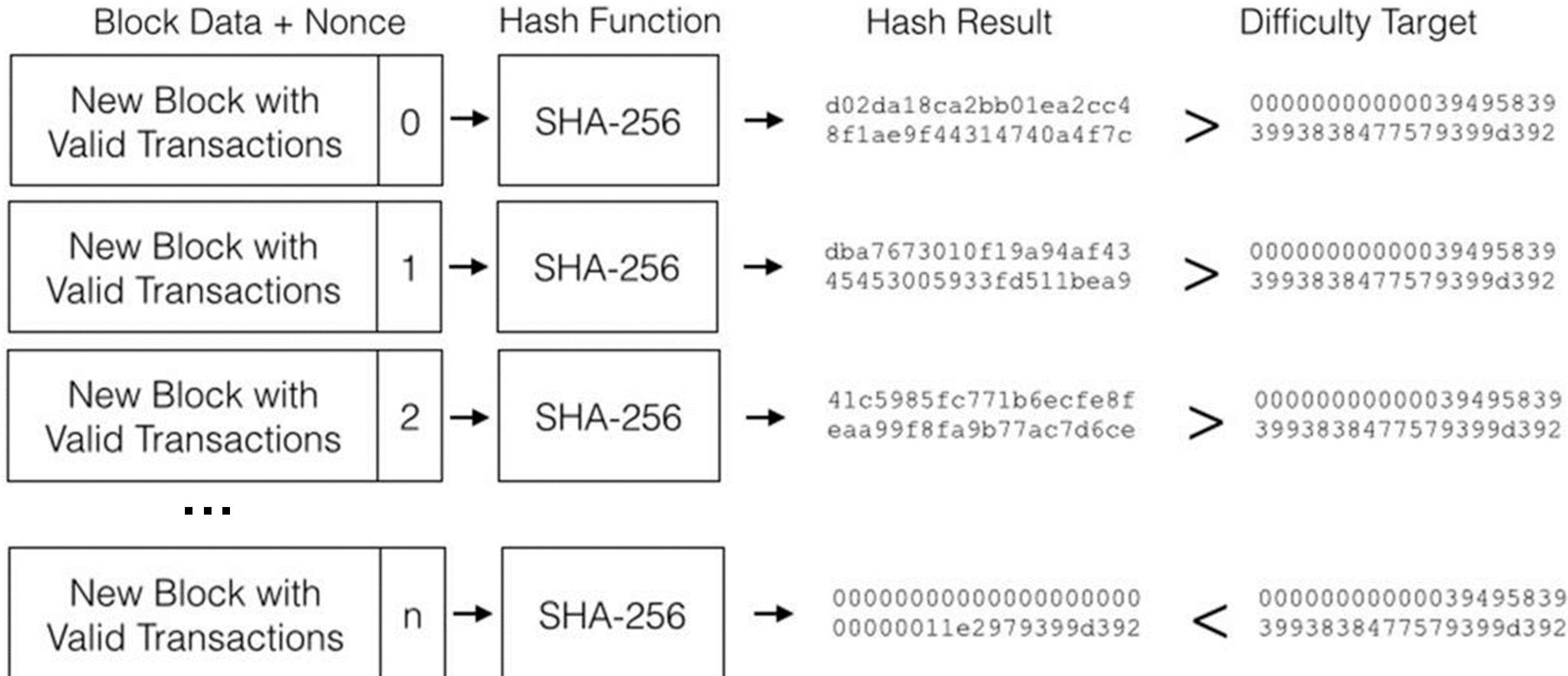
```
00000000000039495839  
3993838477579399d392
```

Id: i
Previous: i - 1
MerkleRoot: 87
Timestamp: 19:30
Nonce
DifficultyTarget

Transações

Bloco i

Consenso via PoW + Longest-Chain



Mineração → Houve um trabalho → Qualquer um pode proof que (i) *of work*; (ii) o bloco é válido

Consenso via PoW + Longest-Chain

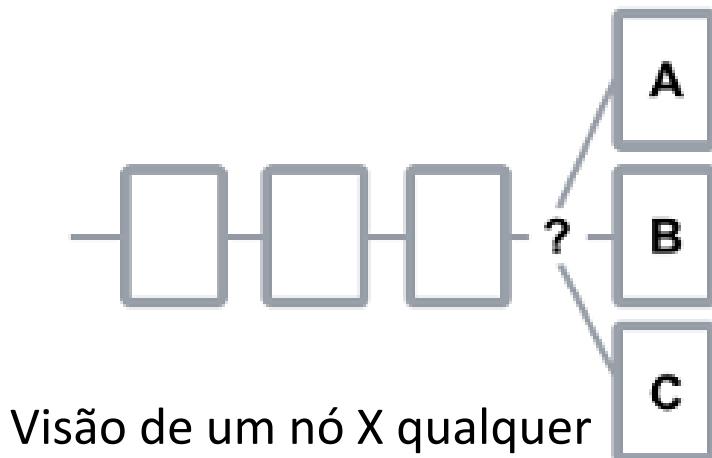
- Que acontece se vários mineradores resolvem o problema matemático e dissemelnam o bloco ao mesmo tempo?
- Em outras palavras, **como geramos o consenso de qual bloco usar?**



Visão de um nó X qualquer
(todos têm essa visão inicial)

Consenso via PoW + Longest-Chain

- Que acontece se vários mineradores resolvem o problema matemático e dissemelam o bloco ao mesmo tempo?
- Em outras palavras, **como geramos o consenso de qual bloco usar?**

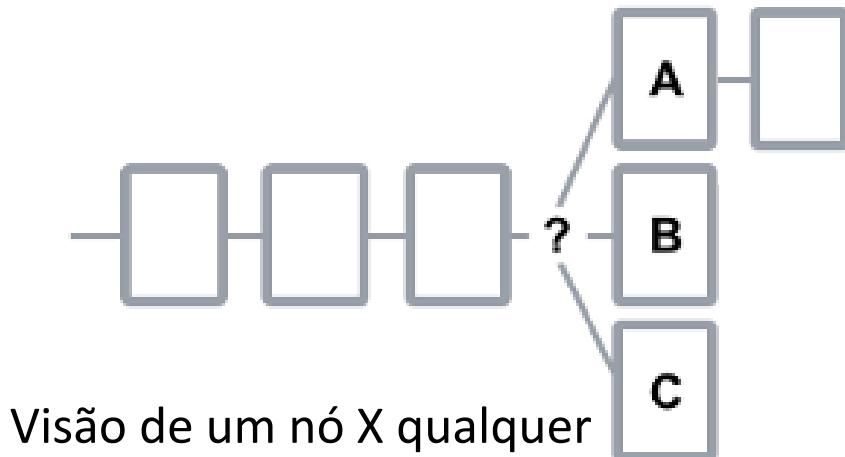


FORK:

- Nós A, B, C mineraram blocos válidos, mas diferentes.
- Nó X recebe os três blocos o que produzirá um '**fork**' na visão local.
- Note que isso gera **inconsistências** temporárias, pois a visão de outro nó Y pode ser diferente pelo delay das mensagens

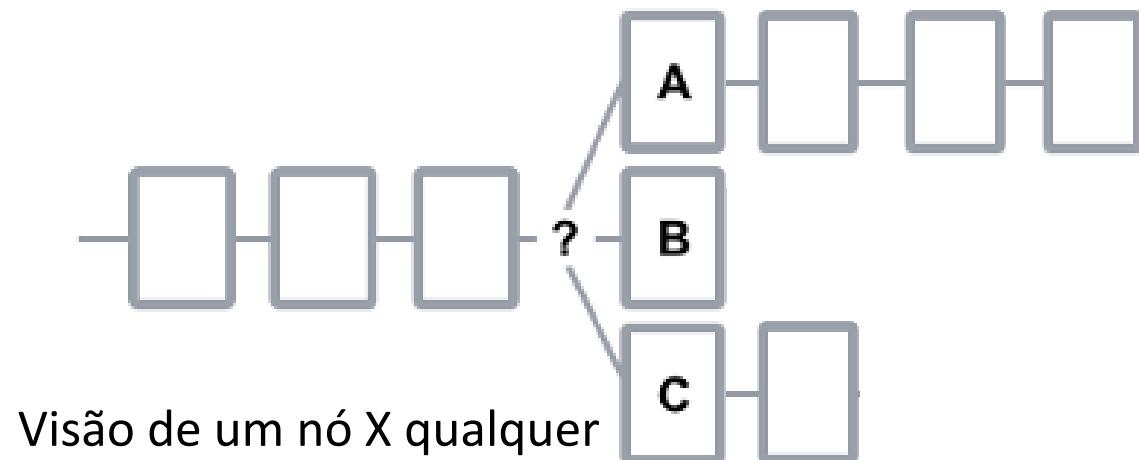
Consenso via PoW + Longest-Chain

- Regra: cada nó utilizará sempre a cadeia mais longa (**longest-chain**) disponível
- Mas note que “inicialmente” precisaremos manter todas



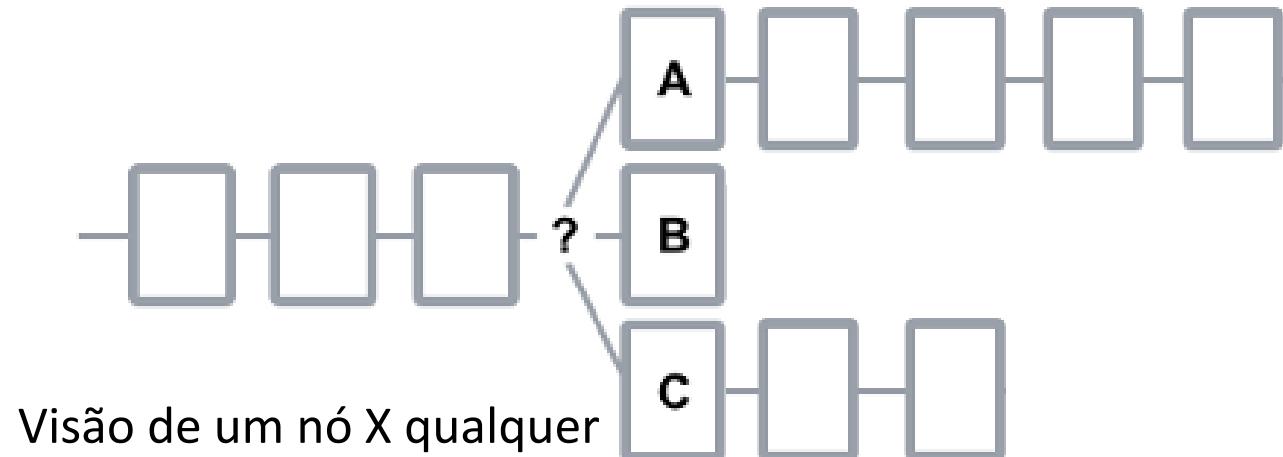
Consenso via PoW + Longest-Chain

- Regra: cada nó utilizará sempre a cadeia mais longa (**longest-chain**) disponível



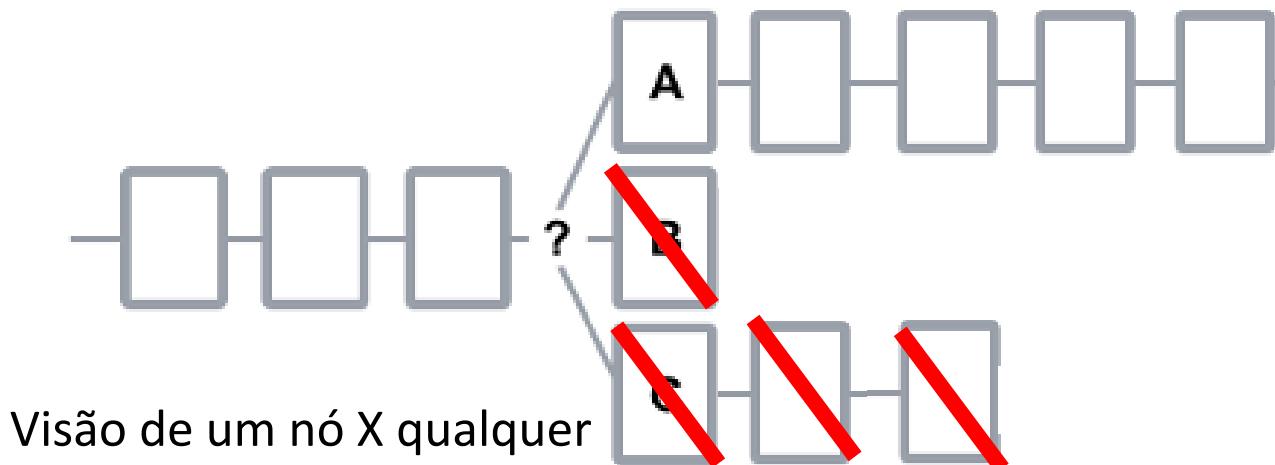
Consenso via PoW + Longest-Chain

- Regra: cada nó utilizará sempre a cadeia mais longa (**longest-chain**) disponível



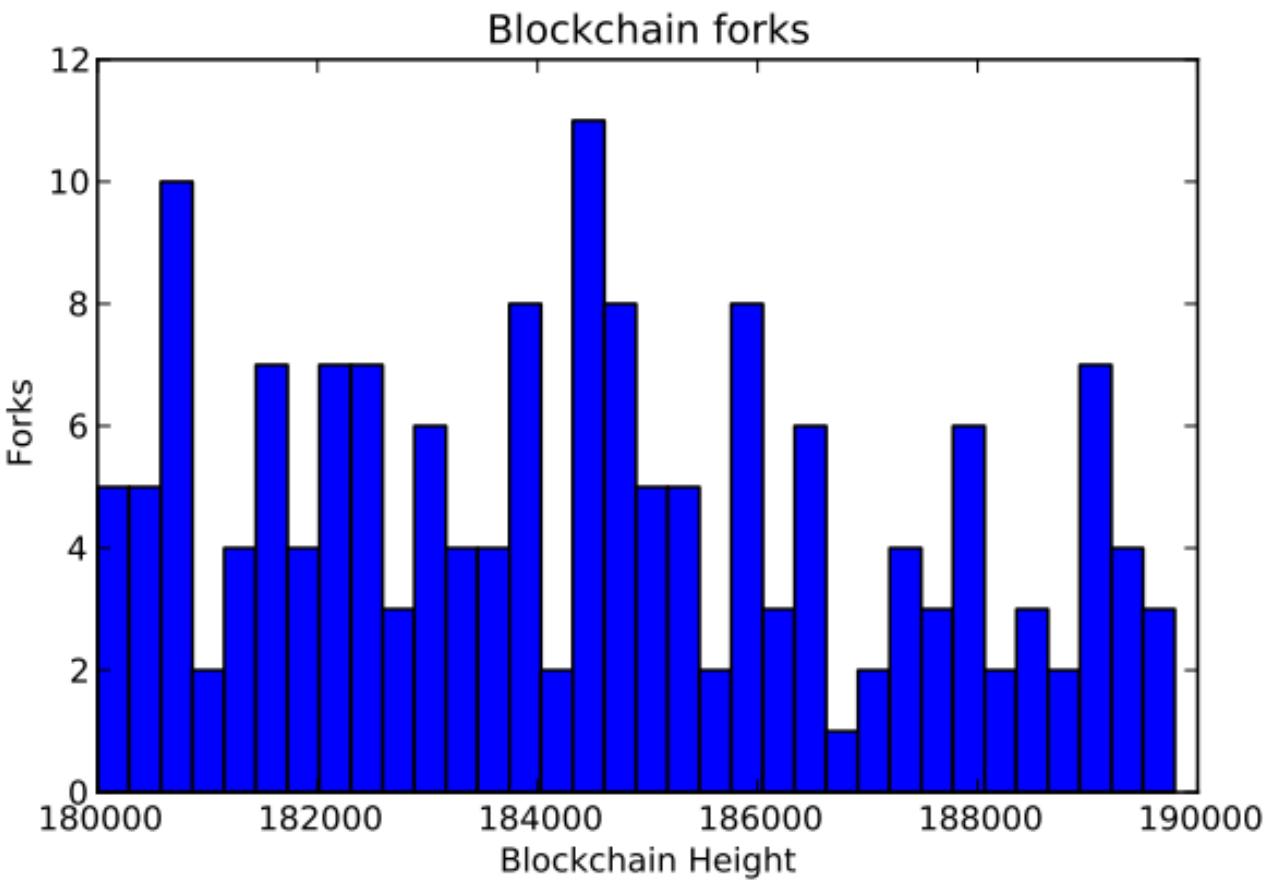
Consenso via PoW + Longest-Chain

- Regra: cada nó utilizará sempre a cadeia mais longa (**longest-chain**) disponível
- Em “algum momento” o nó X abandonará B e C, assimilando só A. Note que outros nós farão a mesma coisa. Normalmente “algum momento” corresponde a 6 blocos.
- **Eventualmente**. todos os nós convergirão na cadeia A



Consenso via PoW + Longest-Chain

- Um bloco é gerado aproximadamente a cada 10 minutos no Bitcoin.
- A cada duas semanas é ajustado o *difficulty target*.
- A cada quatro anos, a recompensa pela geração do bloco diminui à metade.
- O uso do PoW, na realidade, gera *forks* ou é só algo conceitual?



C Decker. Information propagation in the Bitcoin network, 2013.

Consenso: outros tipos

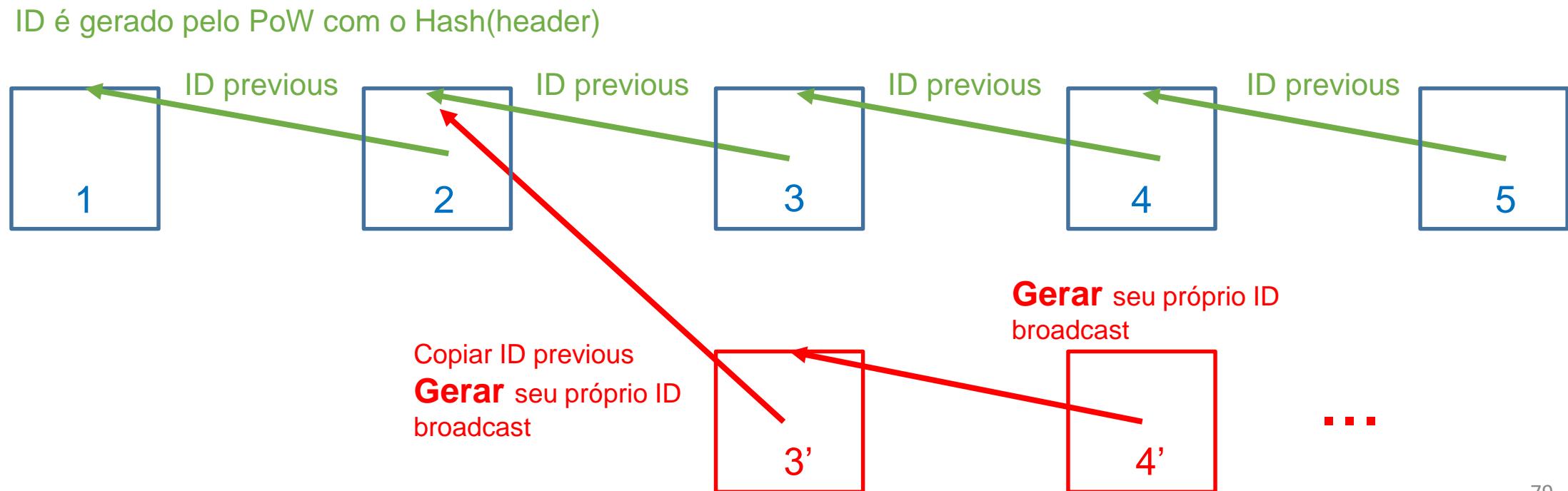


6. Ataques

Ataque na cadeia

Considere uma cadeia de 5 blocos gerada por PoW.

Uma entidade **maliciosa** (i.e., com comportamento bizantino), tenta alterar a cadeia inserindo um bloco entre o segundo e o terceiro. A) O que essa entidade deveria fazer? B) Será que o resto dos participantes perceberia?



Ataque do 51%

No PoW, se alguém controla mais de 50% dos mineradores, poderá ter total controle dos blocos gerados.

Em outras palavras, poderiam criar forks e ganhar todo o dinheiro da recompensa pela criação de blocos.

Porém, o ataque é difícil de realizar no Bitcoin, pela enorme quantidade de mineradores, mas bem frequente em redes menores ou novas.

Ataque do Gasto Duplo – *double spending*

É o ataque que possibilita gastar a mesma moeda (i.e., transação) duas vezes.

Para pensar

Como o gasto duplo se relaciona com a cadeia de blocos, o consenso PoW e o longest-chain na Blockchain do Bitcoin? (lembre dos *forks*)

7. Aplicações

Aplicações

- Usando os contratos inteligentes na blockchain, surgiram aplicações em diversas áreas, tais como:

1. Saúde:

- Prontuários eletrônicos compartilhados
- Carteira internacional de vacinação (COVID-19)

2. Identidades digitais descentralizadas:

- CPF e profissão, via organizações confiáveis
- Informações pessoais, via auto-declaração (SSI)

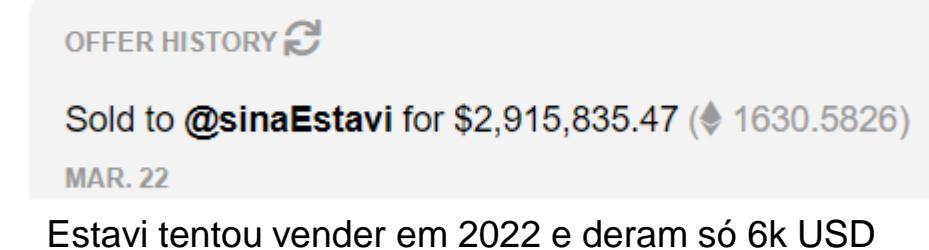
3. Certificação

- Diplomas, *skills* e experiência profissional

4. Registro e comercialização de coleções digitais (NFT)



Owned by [@sinaEstavi](#)



8. Tendências na Blockchain

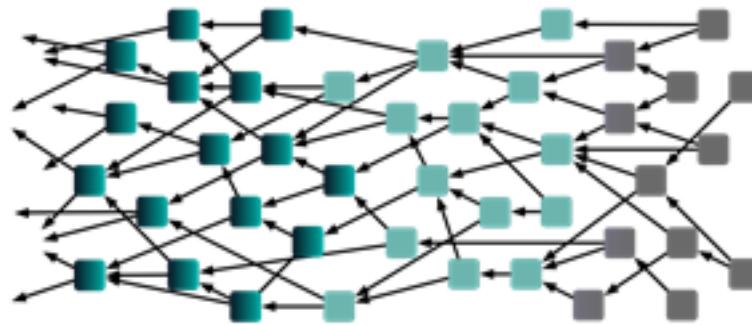
Tendências na Blockchain

Desempenho cai quando cresce a quantidade de eventos em uma única cadeia

- Novas estruturas de armazenamento



Blockchain



Tangle (Directed Acyclic Graph)

Tendências na Blockchain

- Novos algoritmos de consenso (especificamente PoS – *Proof of Stake*)



&

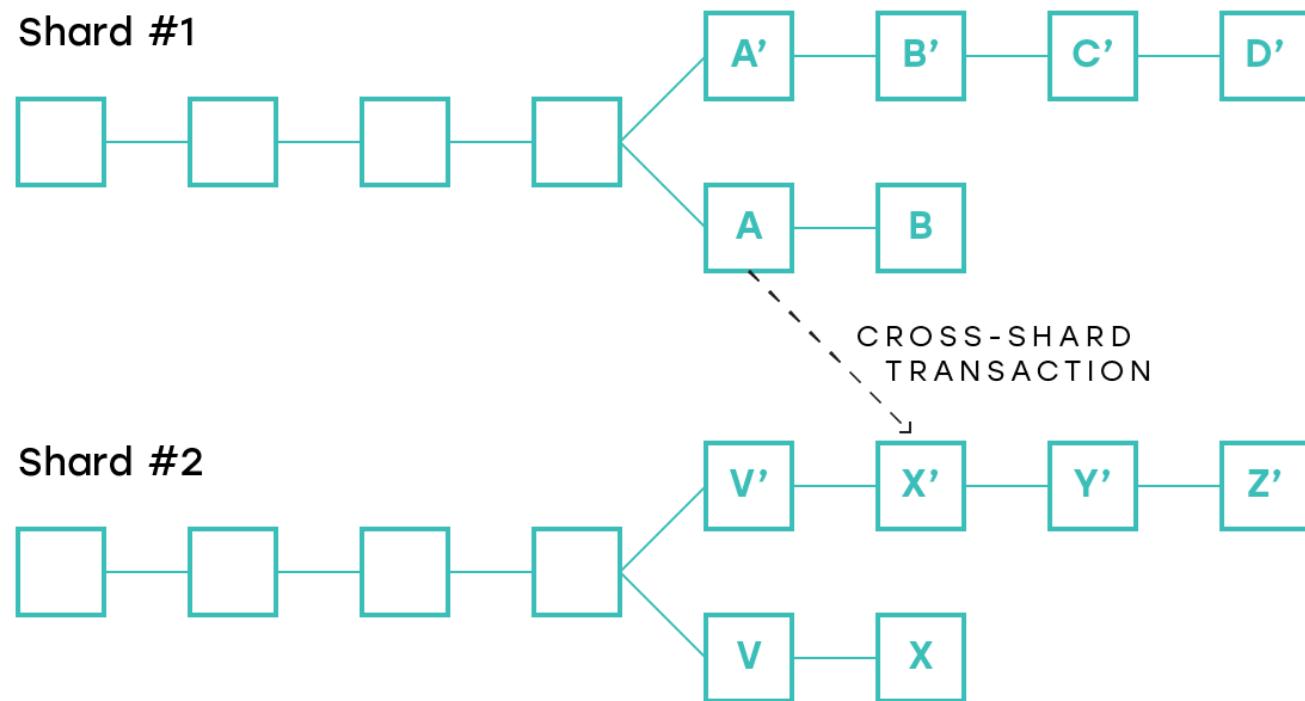


Tendências na Blockchain



ethereum **2.0**

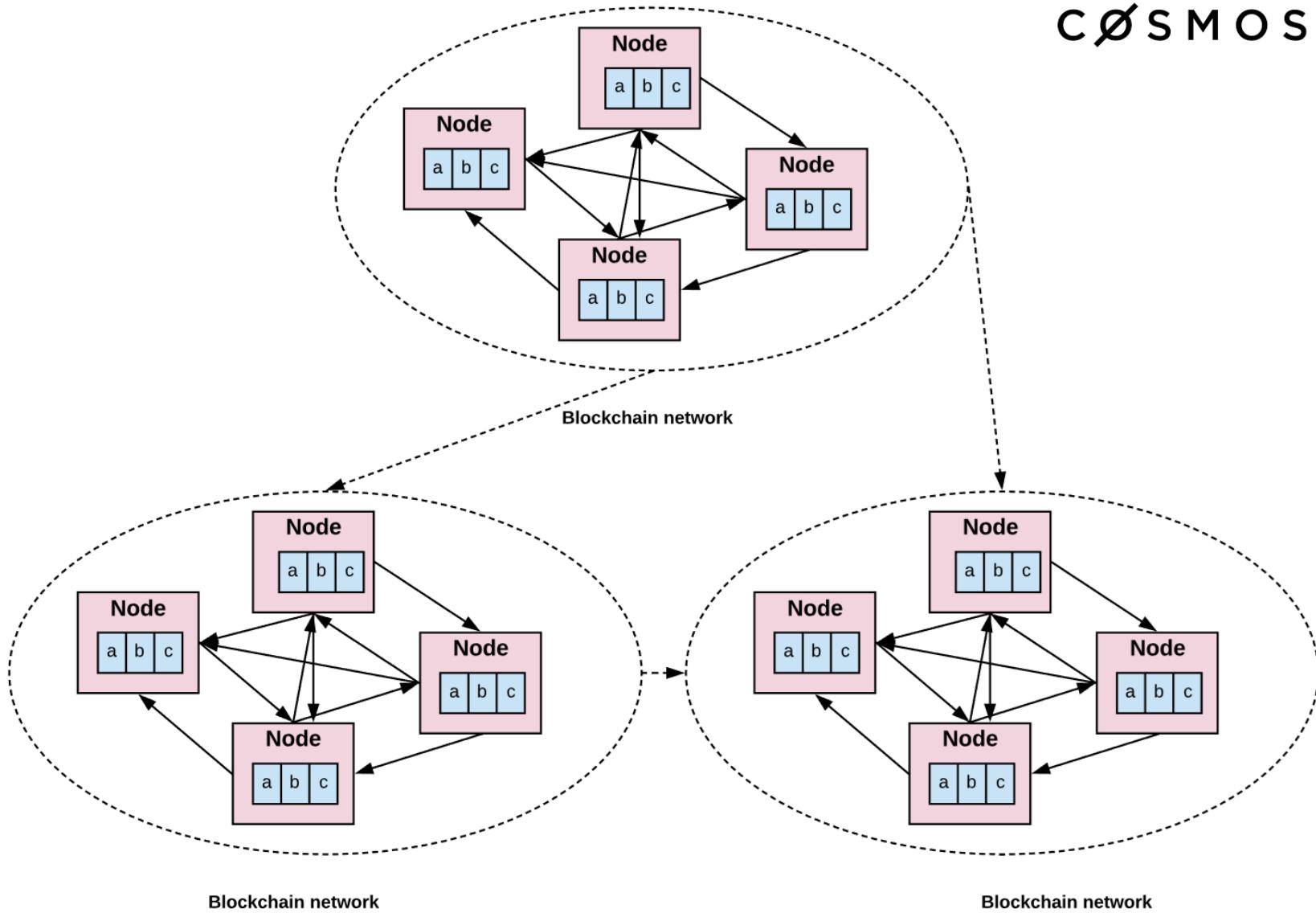
Escalabilidade



Tendências na Blockchain

COSMOS

Interoperabilidade



9. Mineração de Bitcoin

Mineração de Bitcoin

- Como exatamente se minera?
 - Cálculo do hash do bloco calculado usando SHA-256 levando em conta a dificuldade atual *difficulty target* da rede
 - Mineração está mais para adivinhação do que para resolução
 - Recompensa (6,25 BTC ~ 180k USD ~ R\$ 850k) para quem encontrar a solução

Height	Time	Relayed By	Hash	Size (kB)
528051 (Main Chain)	2018-06-18 11:19:33	BTC.TOP	000000000000000000000000000000001b704af44ac2b63f59948de276f181ab4a3dbe2e37a080	803
528050 (Main Chain)	2018-06-18 11:10:10	F2Pool	0000000000000000000000000000000037497d7dffdbbb69f70d3d59f438e7d2239c107195fec8	664.91
528049 (Main Chain)	2018-06-18 11:08:52	F2Pool	0000000000000000000000ccb9f131074d1ab3e8bd62a33844736c3cbfd71e02f2b	1,170.68
528048 (Main Chain)	2018-06-18 10:42:42	BitClub Network	0000000000000000000000000000000019dded40f072c08f0b3ec453134e6b2f952451848188e4	184.28
528047 (Main Chain)	2018-06-18 10:39:33	Unknown	000000000000000000000000000000006755955b7f17625af22386c18989d0124552892767472	486.31
528046 (Main Chain)	2018-06-18 10:32:30	ViaBTC	00000000000000000000000000000000108e0bd29d1a9cfcbf503f0430c0af47190ca89bfaf08d	389.72
528045 (Main Chain)	2018-06-18 10:28:50	BTC.com	000000000000000000000000000000002ea2de35934f6d0a3d63a3bfac9702eae510da85eda4da	354.38
528044 (Main Chain)	2018-06-18 10:24:44	BTC.TOP	000000000000000000000000000000005407710f0041460-00005501-0050073-0051040	440.00

Mineração de Bitcoin

Resumo

Altura	528049 (Main chain)
Jogo da velha	0000000000000000000ccb9f131074d1ab3e8bd62a33844736c3cbfd71e02f2b
Bloco Anterior	000000000000000000019dded40f072c08f0b3ec453134e6b2f952451848188e4
Próximos Blocos	000000000000000000037497d7dffdbbb69f70d3d59f438e7d2239c107195fec8
Hora	2018-06-18 11:08:52
Transmitido Em	2018-06-18 11:08:52
Enviado Por	F2Pool
Dificuldade	4,940,704,885,521.83
Bits	389609537
Número de Transações	2270
Total de Saída	17,831.90207363 BTC
Valor Estimado de Transações	656.5932441 BTC
Tamanho	1170.685 KB
Versão	0x20000000
Merkle Root	6fb3f05a2368c097fa0491be720b61f87bdb6f1ab868f242e85575ec6c0b25e9
Nonce	3229975828
Recompensa pelo Bloco	12.5 BTC
Taxas de Transação	0.30484879 BTC

Mineração de Bitcoin

Resumo

Altura	528049 (Main chain)
Jogo da velha	000000000000000000ccb9f131074d1ab3e8bd62a33844736c3cbfd71e02f2b
Bloco Anterior	00000000000000000019dded40f072c08f0b3ec453134e6b2f952451848188e4
Próximos Blocos	00000000000000000037497d7dffdbbb69f70d3d59f438e7d2239c107195fec8
Hora	2018-06-18 11:08:52

Nonce **3229975828**

Recompensa pelo Bloco **12.5 BTC**

Taxas de Transação **0.30484879 BTC**

Valor Estimado de Transações	656.5932441 BTC
Tamanho	1170.685 KB
Versão	0x20000000
Merkle Root	6fb3f05a2368c097fa0491be720b61f87bdb6f1ab868f242e85575ec6c0b25e9
Nonce	3229975828
Recompensa pelo Bloco	12.5 BTC
Taxas de Transação	0.30484879 BTC

Mineração de Bitcoin - CPUs

- A ideia original de se utilizar PoW visava dar igual poder de voto a todos os participantes da rede: “1 CPU = 1 VOTO”. A mineração começou com CPUs.

CPU	Mining speed (KH/s)	Power used (Watts)	# of cores
Athlon 64 X2 5600+	6.07	89	2
Athlon II X3 425	9.5	125	4
Phenom II X4 955	22	125	4
FX-8120	46	125	8
FX-8350	65	125	8
Core 2 Quad Q6600	9.68	100	4
Core 2 Quad Q9550	32.2	125	4
Core i3-2130	23	65	4
Core i5-2500K	48	90	4
Core i5-3570K	55	90	4
Core i7-3930K	98	200	12



Mineração de Bitcoin - GPUs

- Oferecem um grau de paralelização muito maior do que CPUs

GPU	Mining speed (MH/s)	Power used (Watts)
AMD 4870	90	150
AMD 5770	240	100
AMD 5830	300	125
AMD 5850	400	180
AMD 5870	480	200
AMD 5970	800	350
AMD 6990	800	400
NVIDIA GT-210	4	30
NVIDIA GTX-280	60	230
NVIDIA GTX-480	140	250
NVIDIA Tesla S1070	155	800
NVIDIA Tesla S2070	750	900



Mineração de Bitcoin - FPGAs

- Circuitos desenhados exclusivamente para calcular SHA-256 (e nada mais!)

FPGA	Mining speed MH/s	Power used watts	Efficiency W/MH/s
ModMiner Quad	800	40	0.05
Butterflylabs Mini Rig	25,200	1250	0.05



Mineração de Bitcoin - ASICs

- Mais eficientes que FPGAs... ...e muito mais baratos!

ASIC	MH/s	Watts	MH/J
Ebit E10	18.000.000	1620	11.111
AntMiner S9	14.000.000	1375	10.181
Avalon821	11.000.000	1200	9.166



Qual o retorno esperado?

MININGKZ

Taxa atual: ~ 338.000.000 TH/S ~ 338 EH/s
ou o equivalente a aproximadamente
19.000.000 Ebit E10



Qual o retorno esperado?

- Vamos considerar
 - Média de 10 minutos por bloco, 6 por hora, 144 por dia
 - Prêmio atual por bloco descoberto: 12.5 BTC
 - Média de taxas de transação: 0.5 BTC
 - Rede: 38.500.000 TH/s (em 2019)
 - Custo da energia: **Grátis!**
 - Cotação do Dólar/BTC: US\$ 6450

Qual o retorno esperado?

	Hash Speed (TH/s)	%	US\$/Dia	Preço (US\$)	Break Even
Core i7-3930K	0,0000001	0,000000000003	0,00000003	160	13.977.267,88
AMD Radeon HD 6990	0,0008650	0,000000022468	0,00027128	250	2.524,80
Butterflylabs Mini Rig	0,0252	0,000000654545	0,00790324	15295	5.302,14
Ebit E10	18	0,0000467532468	5,64517403	2800	1,36

Quão otimista é essa estimativa?

- Assume que há uma distribuição igualitária entre os participantes
- Assume que o usuário, por conta, vai ter a sorte de encontrar um bloco
 - São suposições irreais na prática
- Isso levou usuários a formarem **pools de mineração**
 - Usuários compartilham o trabalho e as recompensas
 - Tipicamente o organizador cobra um % dos ganhos
 - Permite que mesmo pequenos mineradores consigam algum retorno

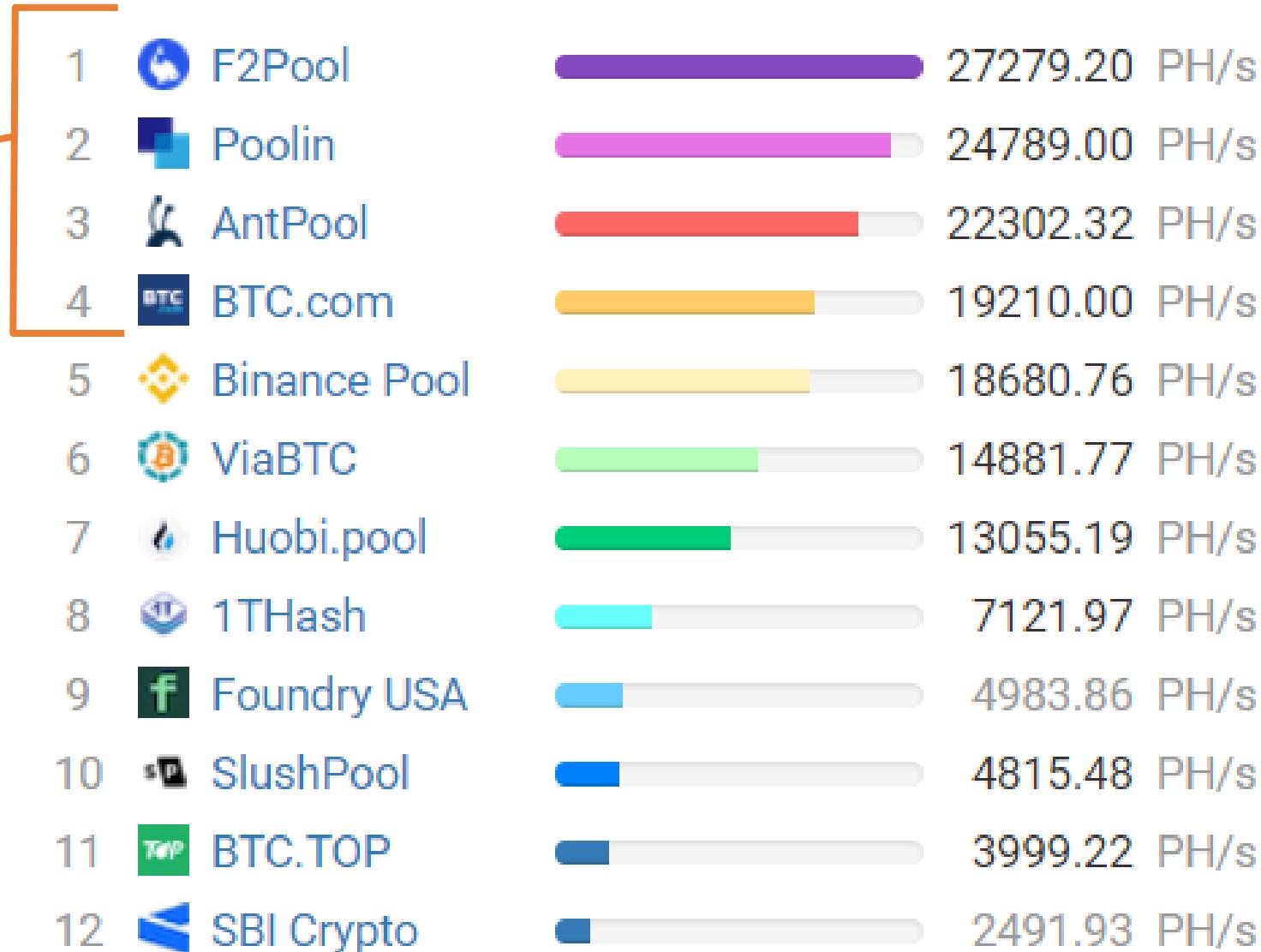


UFABC

Pools de mineração

Aproximadamente
57% da rede

Note que eles poderiam
realizar o ataque de 51%

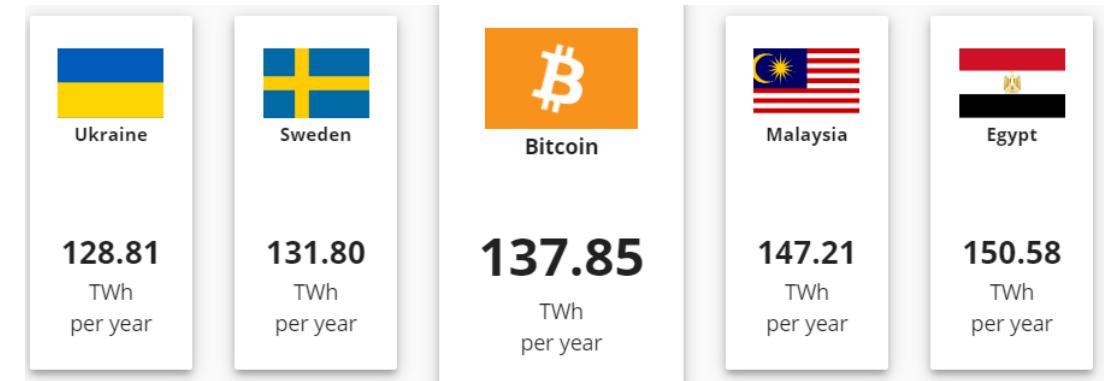


Mineração Profissional

- Alguns fabricantes perceberam que é mais lucrativo fabricar ASICs para “consumo próprio” do que vendê-los
- Já outros vendem o processamento no melhor estilo Cloud Computing
- Há muita especulação sobre a atual tecnologia empregada pelos mineradores profissionais
 - O vazamento de um segredo pode custar milhões!
 - Sabe-se contudo que diversos já utilizam ASICs com tecnologia de 16 nm
 - Para se ter uma ideia, a Intel passou do processo de 22 nm para 14 nm apenas em 2014!

Consumo na Mineração

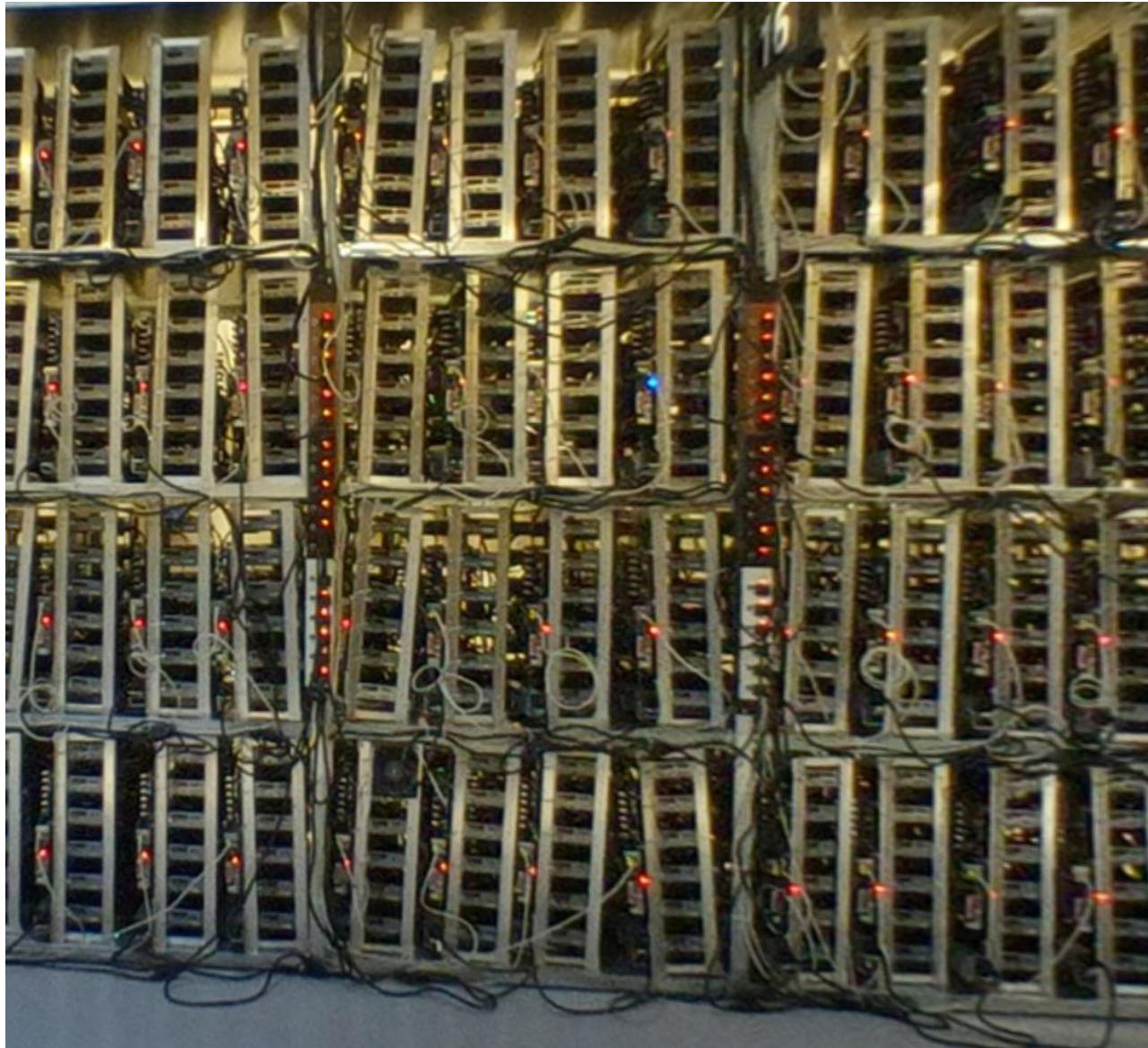
- Há dados públicos sobre data centers de mineração consumindo de 0,5 a 5MW e planos para centros de mineração até 100MW (1 MW ~ consumo de 1000 casas)
 - O computador mais rápido do mundo, o Sunway TaihuLight com 10.649.600 cores consome “apenas” ~15MW
- Em 2021, a mineração do Bitcoin consumiu:
 - 0,63 % do consumo de eletricidade mundial.
 - Mais do que a eletricidade de 15 países, como: Suécia, Ucrânia, Argentina, Holanda, Chile.



Mineração Profissional



Mineração Profissional



Mineração Profissional



Resumo

- Blockchain é uma tecnologia que registra eventos de forma imutável, transparente e descentralizada.
- Usa o conceito de transações (i.e., eventos) e blocos interligados em uma cadeia.
- Existe a permissionada (usuários identificáveis) e a não permissionada (usuários completamente anônimos).
- Na permissionada, a inserção do bloco no final da cadeia é realizada pelo líder.
- Na não permissionada, a inserção é realizada pela prova de trabalho e longest-chain.
- Nas blockchains de 2^a geração é possível inserir funcionalidades específicas do domínio, denominadas contratos inteligentes, levando a novas aplicações, e.g. NFT.

Conceitos adquiridos

- Blockchain.
- Imutabilidade.
- Permissionada e não permissionada.
- Ataque do 51% e do Gasto Duplo
- PoW (Proof-of-Work) e longest-chain.
- Nonce, Difficulty Target, Fork.
- Mineração.