TECH DAY RECIFE 2019

Blockchain

Como um sistema implementa consenso sem confiar em ninguém

Palestrante

Estêvão Chaves Monteiro, M.Sc.

Analista Desenvolvedor de Sistemas

SERPRO/DIDES/SUPDG/DGGOV/DGGO3

https://estevao.altervista.org

Cadeia de blocos?

- Registro inadulterável de transações
- Segurança
- Integridade
- Criptografia
- Criptomoedas

Cadeia de blocos

É a bala de prata para qualquer registro seguro de dados?

Nada disso.

É primordial entender o modelo

para subsidiar as inovações.

Descentralização

Descentralização

- Estamos habituados a serviços que pressupõem nossa confiança em uma autoridade central e a quem podemos responsabilizar judicialmente (sistemas fiduciários):
  - bancos;
  - instituições financeiras; *fintechs;*
  - sistemas de pagamento;
  - governo.

Descentralização

“Não confie.

Verifique.

Porque Bitcoin não é sobre confiança.

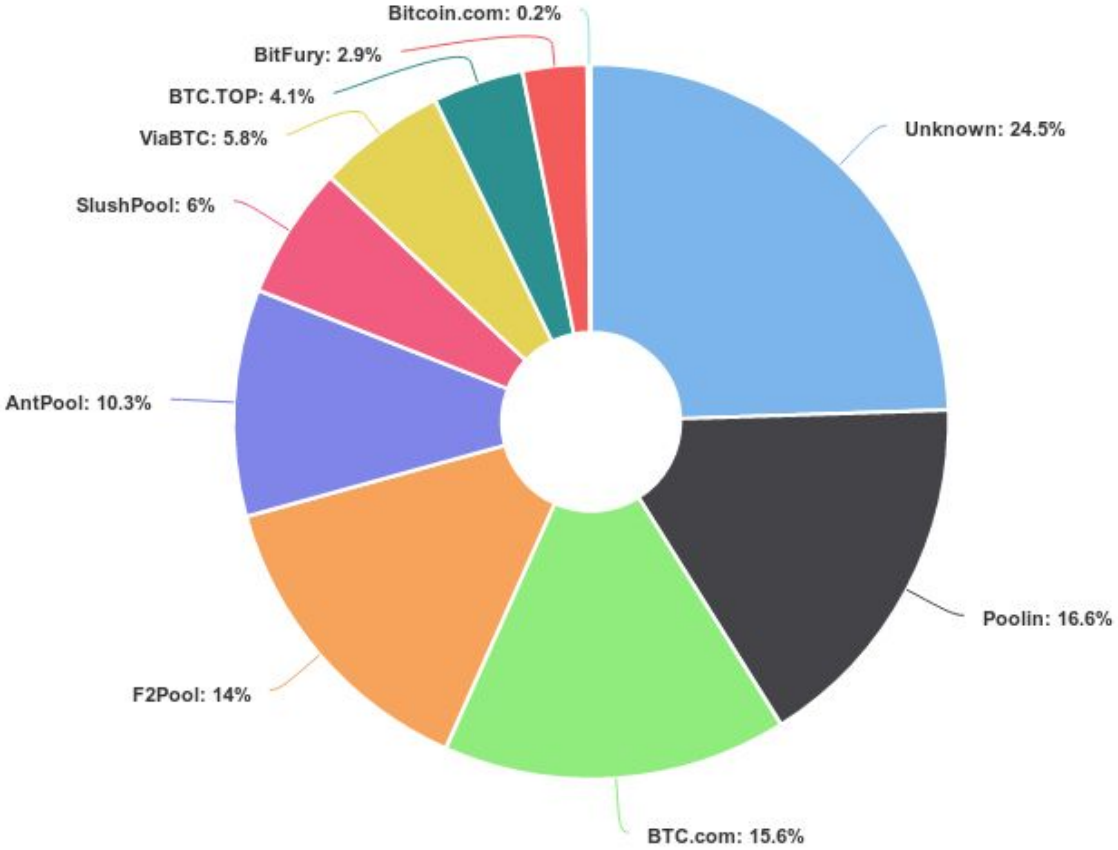
É sobre liberdade e independência.”

– Electrum Wallet

Cadeia de blocos

- Rede ponto-a-ponto descentralizada, igualitária, na qual nenhum dos participantes confia em outro.
- Qualquer um pode baixar, auditar e validar todas as transações do sistema.
- As regras (protocolos) e o reconhecimento de registros são definidos por consenso de 51% dos participantes.

Processamento descentralizado



Cadeia de blocos

- Repositório público de registros imutáveis assinados digitalmente.
- Resistente a falhas de consenso (problema dos generais bizantinos).
- Resistente a duplicação de transação.

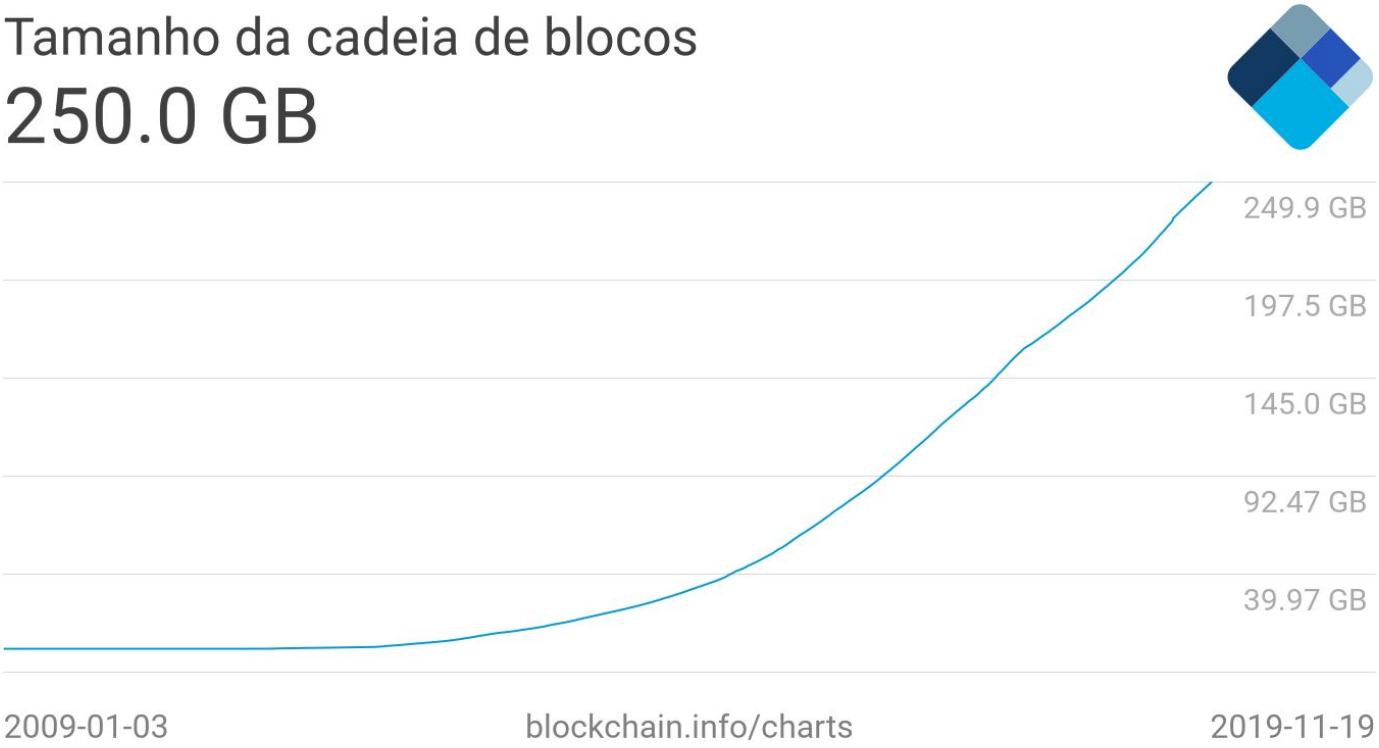
Cadeia de blocos

- Redundância distribuída e descentralizada.
  - Quanto maior a redundância, mais robusto e inviolável o registro de dados.
  - A cadeia de blocos do Bitcoin inteira tem mais de 10 mil cópias ao redor do globo.

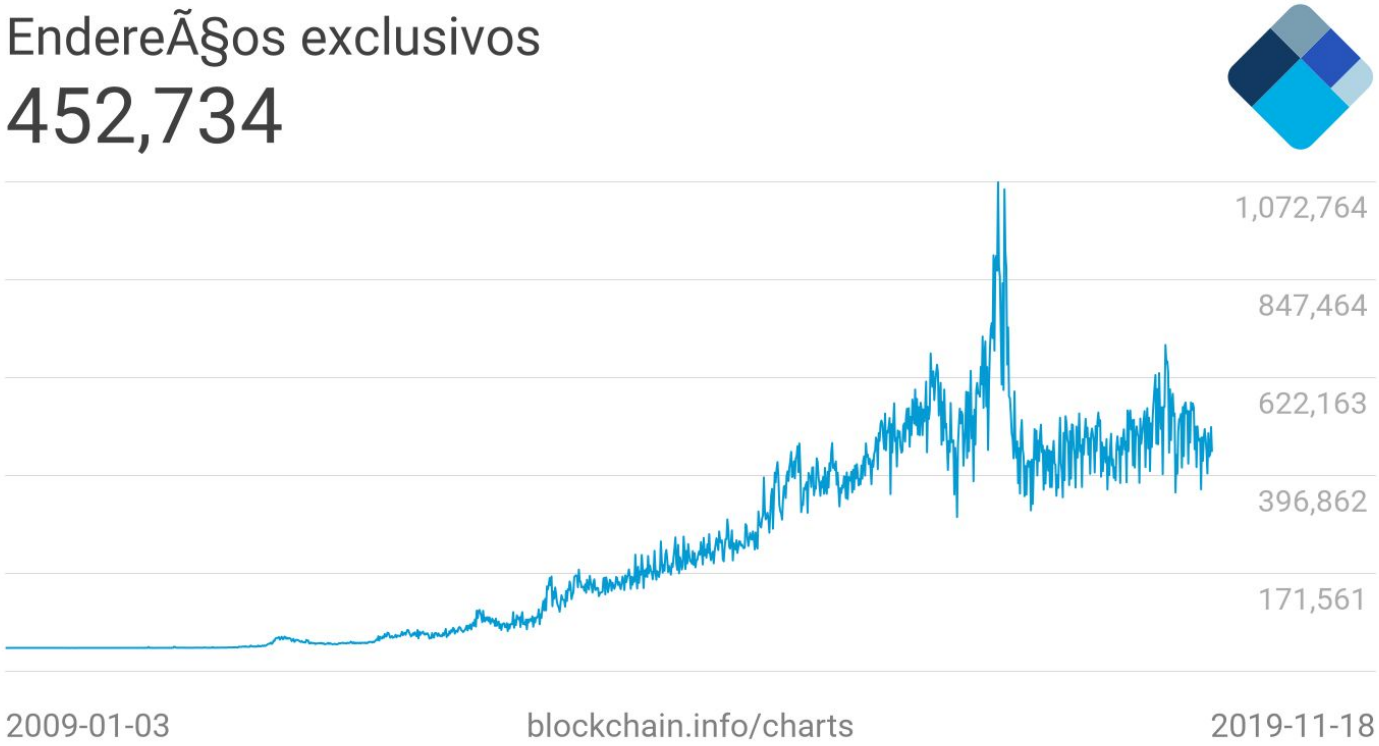
Estudo de caso: Bitcoin

- Rede ponto-a-ponto descentralizada para pagamentos.
- Bitcoin Core: software livre de código aberto que define:
  - protocolo para pagamentos seguros;
  - protocolo para validação de transações e evitar duplicações;
  - protocolo para produção periódica de novas unidades de valor em ritmo controlado.

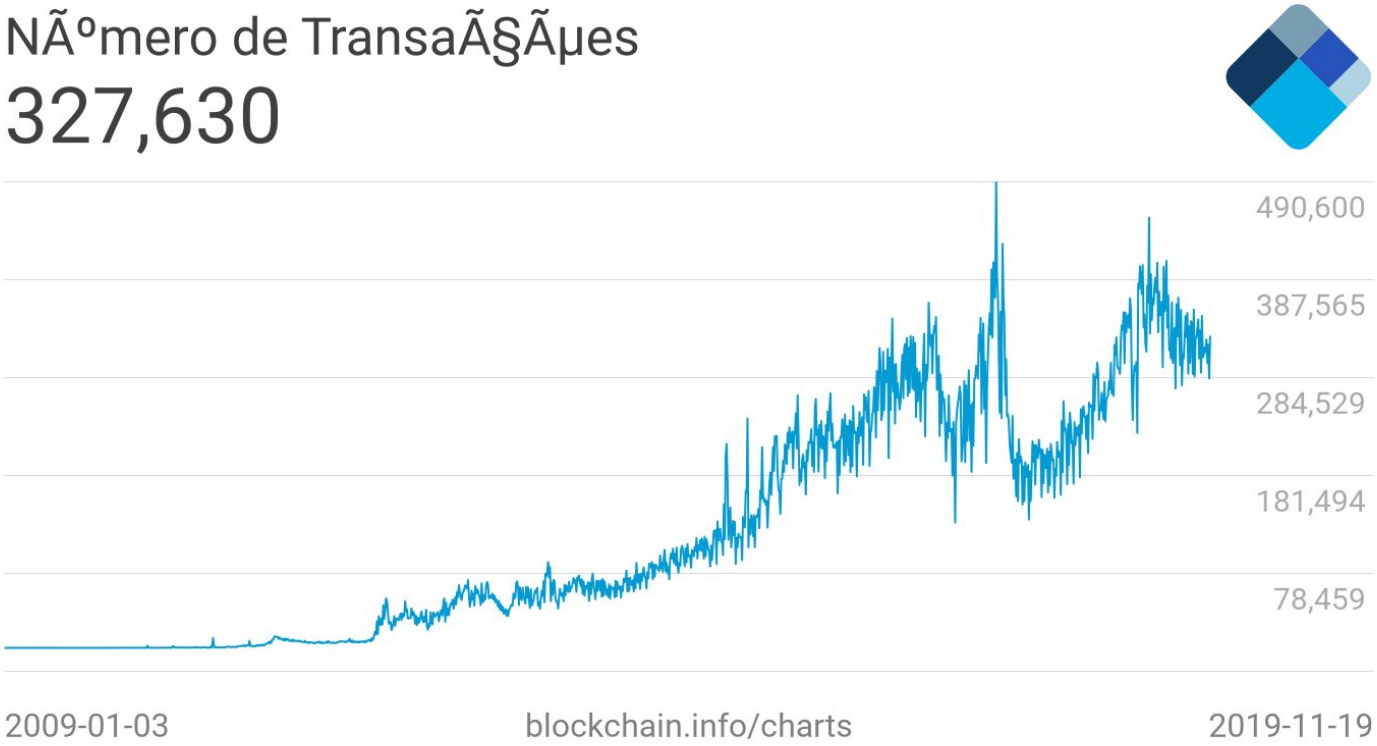
Dimensões do sistema Bitcoin



Dimensões do sistema Bitcoin



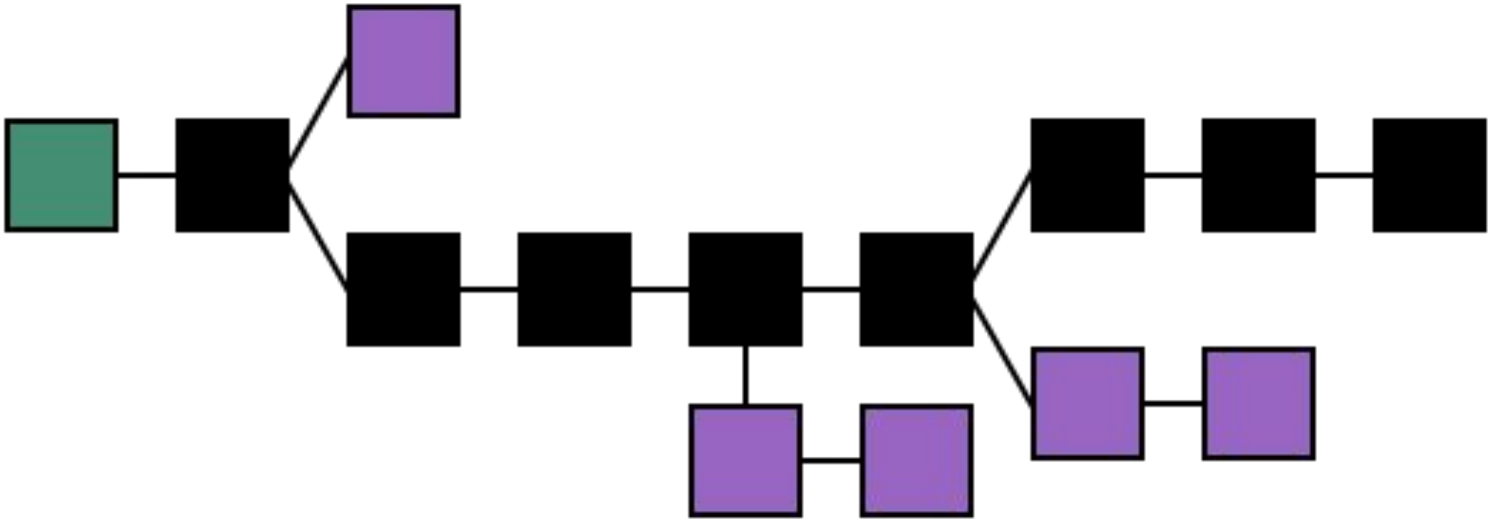
Dimensões do sistema Bitcoin



Submissão de transação

- Clientes do sistema enviam transações para a rede, que vão para o **“balde virtual”** (mempool).
- Para uma transação ser efetivada, ela deve ser inserida em um **bloco**.
- O novo bloco deve se propagar pela rede e ser validado pelo **consenso**.

Montando a cadeia



Montagem do bloco

- Cada transação paga uma **taxa** (escolhida pelo próprio pagador) para ser confirmada.
- Qualquer participante da rede pode **propor** o próximo bloco de transações a anexar na cadeia.
- Um **“minerador”** monta um novo bloco a partir das transações no balde, priorizando as de maiores taxas.

Validação do bloco

- Um novo bloco só é aceito se vencer o **desafio computacional** imposto pelo sistema (prova de trabalho).
- Além das taxas de confirmação das transações no bloco, o “minerador” é premiado pelo desafio de validação do bloco: novas unidades de bitcoin são **“mineradas”** (criadas pelo sistema após a prova de trabalho).

Códigos hash

- Cada transação é identificada por um código de resumo/dispersão (hash SHA-256)
  - código binário
  - tamanho fixo
  - identifica unicamente qualquer sequência de dados
  - irreversível (não revela o conteúdo original)

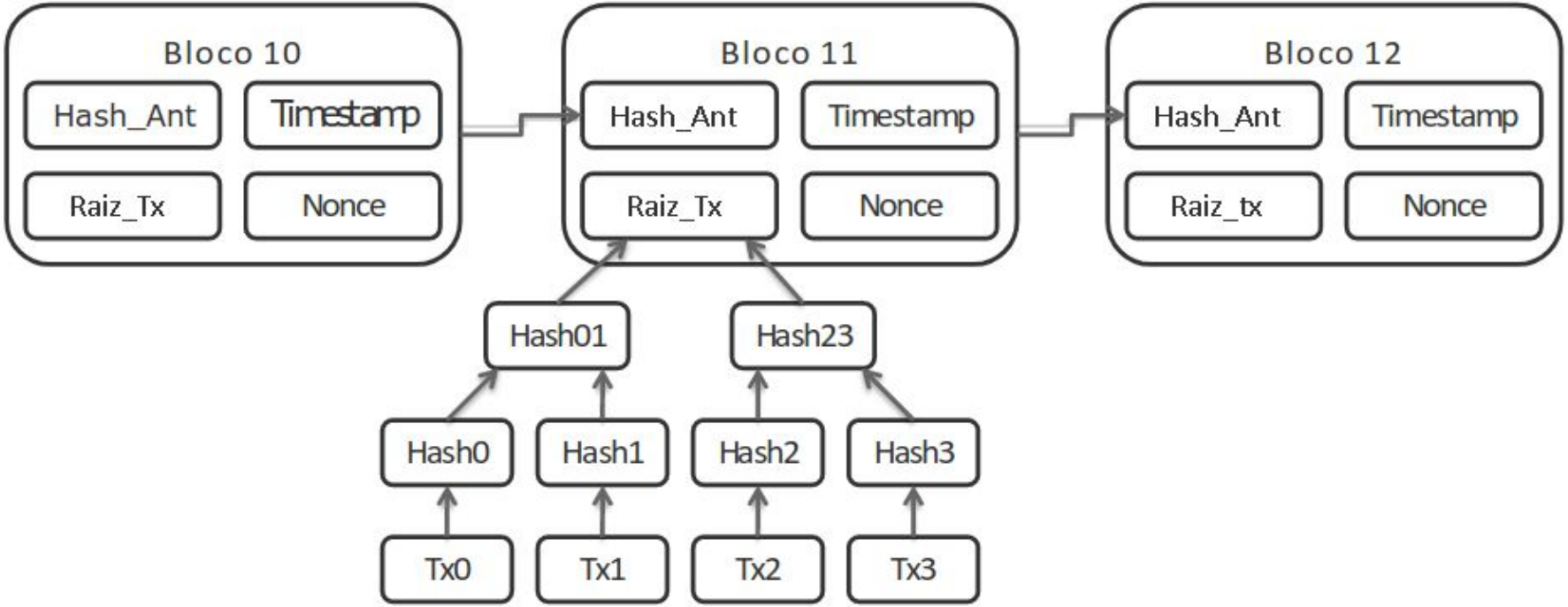
Códigos hash

- Exemplo: da palavra “Bitcoin” deriva-se o seguinte código SHA-256: b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4
  - 64 caracteres hexadecimais = 256 bits.

Códigos hash

- Cada bloco também é identificado por seu código hash.
- O hash do bloco consolida:
  - o hash do bloco anterior;
  - hashes consolidados de todas as transações;
  - o carimbo de tempo do bloco;
  - o *nonce* (número aleatório que resolve o desafio).

Árvore de Merkel



O desafio do hash

- O desafio computacional ao minerador é calcular um código hash com uma característica especial:
  - os dados do bloco devem gerar um código que inicie com uma quantidade de **zeros** definida pela **dificuldade** da rede;
  - computação de força bruta: descobrir o **nonce** que resolve o desafio.

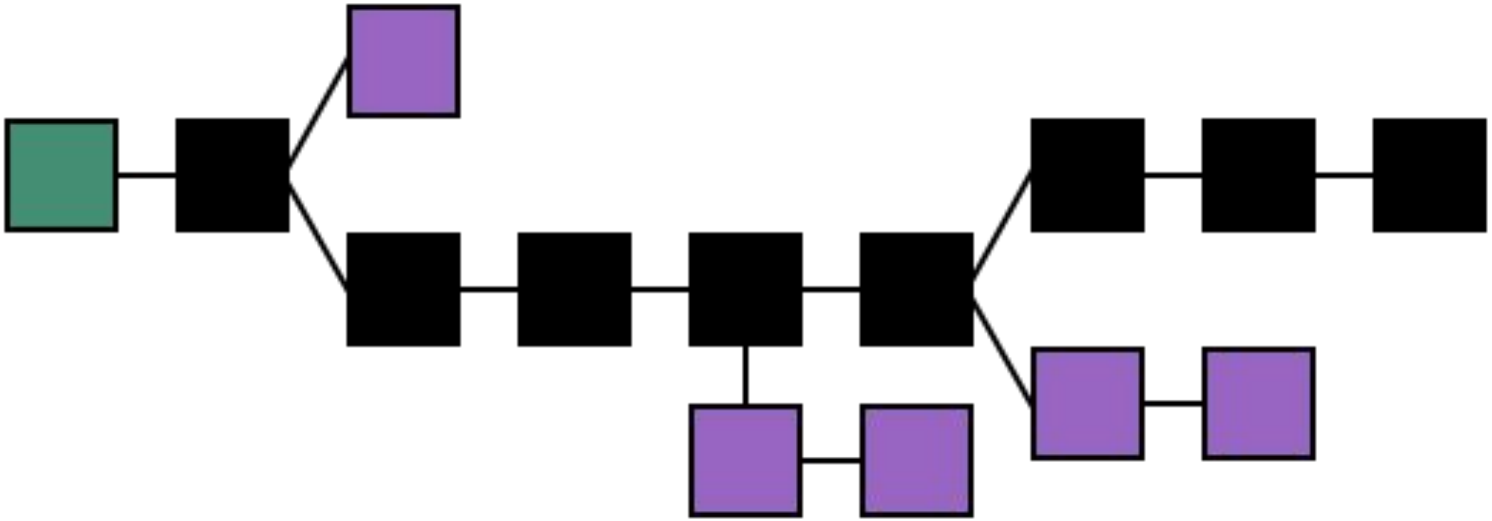
Nonce

- Nonce é um dado aleatório gerado apenas para modificar o código hash do bloco.
- Exemplo: O bloco 605496 gerou um código de 18 zeros: 0000000000000000013766ce12c3a6e03170b75028b12061fc65c8cf02718ab.
- O nonce do bloco 605496 foi o número “3 101 785 261”.
- Visualizado a partir de: https://www.blockchain.com/btc/block/0000000000000000013766ce12c3a6e03170b75028b12061fc65c8cf02718ab

Dificuldade da rede

- A dificuldade do desafio é automática e periodicamente ajustada pela rede para manter o ritmo médio de 1 bloco efetivado a cada 10 minutos.
  - **Escassez -> valor.**
- Todos os mineradores competem para produzir primeiro o próximo bloco válido.

Ramificação temporária



Ramificação temporária

- Temporariamente, a cadeia se ramifica como uma árvore, enquanto os blocos candidatos se propagam.
- Será consolidada somente a cadeia mais longa: aquela na qual foi **investido mais trabalho**.
- Blocos não consolidados são descartados e as recompensas, perdidas.

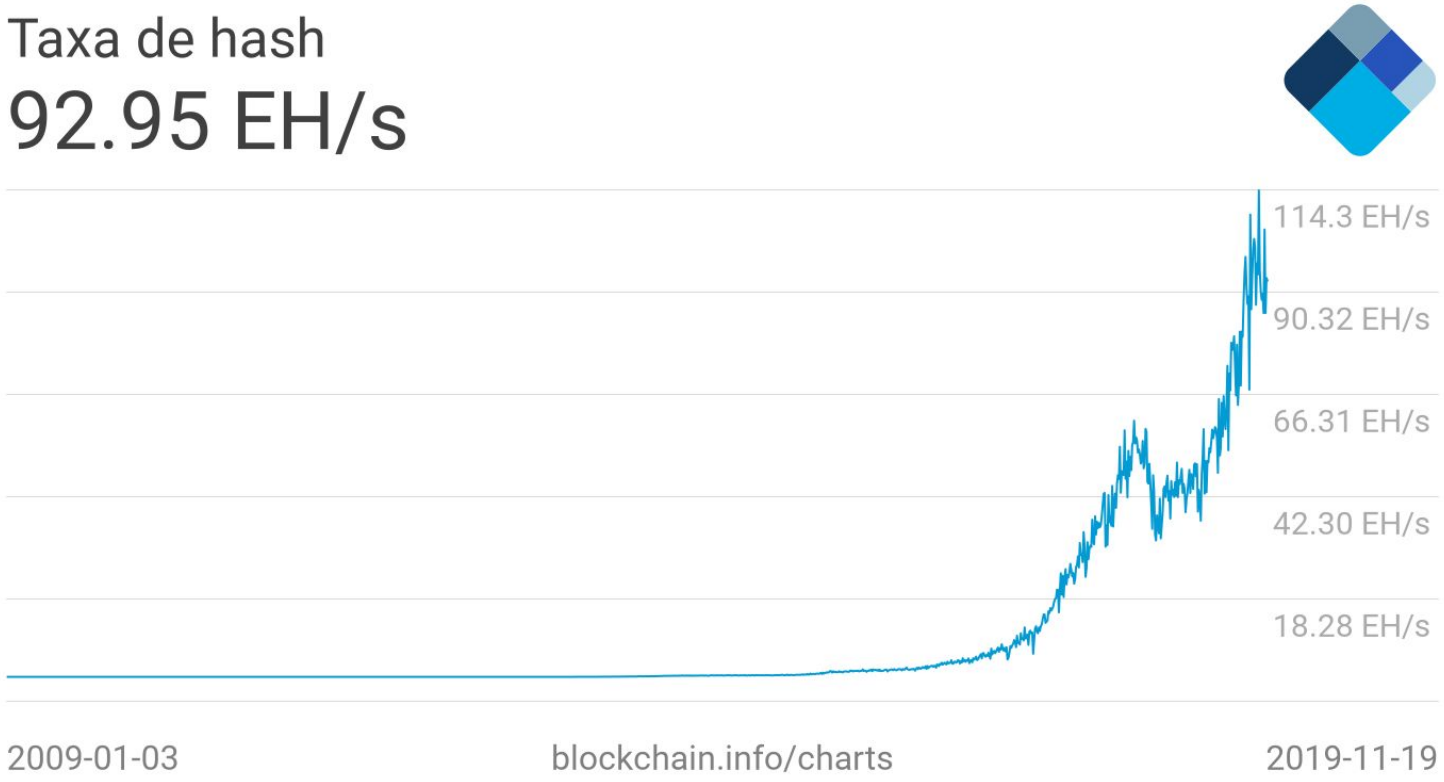
Integridade dos registros

- A **mínima alteração** na sequência de bits resulta em um código hash completamente diferente:
  - O código SHA-256 da palavra “bitcoin” é 6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b.
  - O código SHA-256 da palavra “Bitcoin” é b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4.

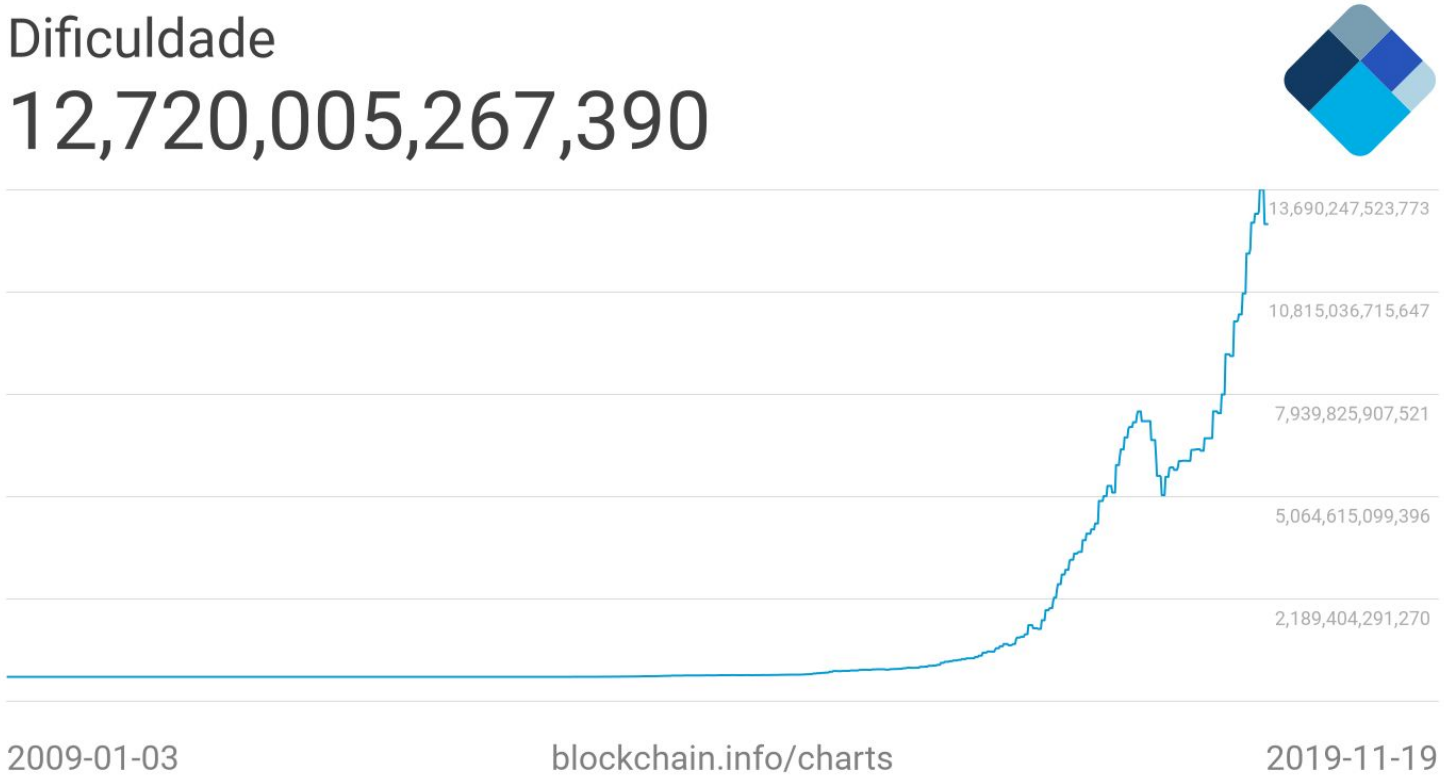
Integridade dos registros

- Cadeia de árvores de códigos hash (Merkel): não permite alterar qualquer dado sem alterar o bloco inteiro e todos os blocos subsequentes!
- A cadeia de blocos do Bitcoin foi projetada para que seja mais fácil e lucrativo **participar** da “brincadeira” (minerar) do que tentar **trapacear** (adulterar transações prévias para desviar valores).

Integridade dos registros



Integridade dos registros



Integridade dos registros

Integridade dos registros

Segurança

- Cadeias de blocos públicas como a do Bitcoin podem ser auditadas por qualquer um.
- Não requerem que se confie em entidade alguma, pois todas as validações são puramente matemáticas.
- Cada participante deve cuidar da sua própria chave criptográfica secreta (arquivo, token, papel…), a partir da qual pode receber e enviar valores.

Privacidade

- Todas as transações são públicas: valores, endereços de entrada, endereços de saída e datas.
- A cadeia de blocos não contém qualquer identificação pessoal do participante, apenas os endereços derivados e controlados pela sua chave criptográfica secreta.

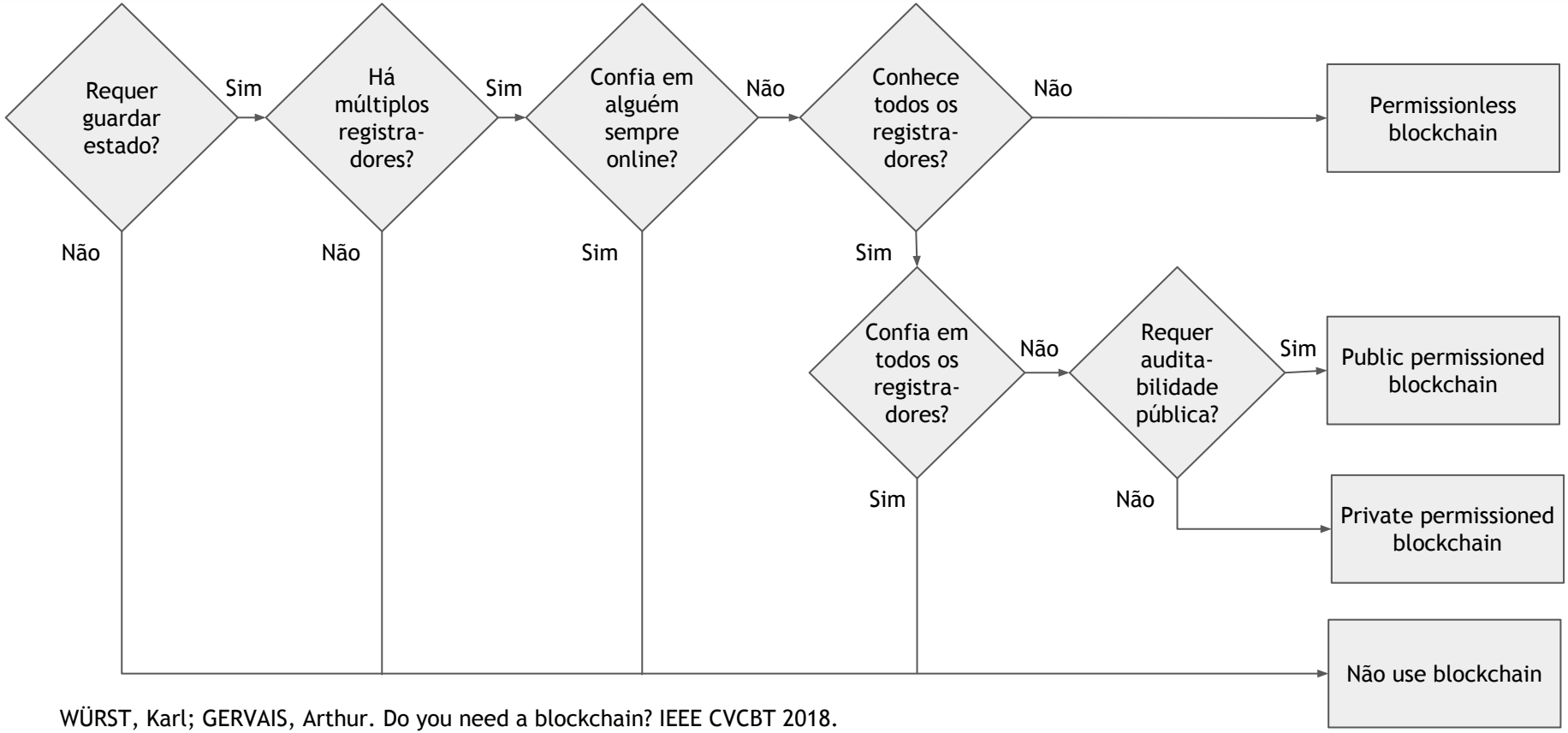
Privacidade

- Os endereços são como **caixas postais** geradas a partir da chave secreta quase sem limite.
- Mas é possível rastrear e identificar um participante por suas relações e fatores comportamentais **(colapso de identidade)**.

Desvantagens

- Cadeias de blocos tradicionais são caras!
  - custo de processamento;
  - custo de energia;
  - demora na confirmação das transações.
- A maior justificativa é o consenso sem confiança.
  - Se tiver que confiar, não precisa de cadeia de blocos.
  - A resiliência da rede depende da redundância dos dados e do *hashpower* da rede.

Você precisa de uma blockchain?



WÜRST, Karl; GERVAIS, Arthur. Do you need a blockchain? IEEE CVCBT 2018.

ENCORAJE-SE

OLHE POR OUTROS ÂNGULOS

BORA FAZER DIFERENTE?

O QUE VOCÊ TEM NA CABEÇA?

OBRIGADO!

TECH DAY

RECIFE
2019