Blockchain e Criptomoedas

Prof. Jó Ueyama

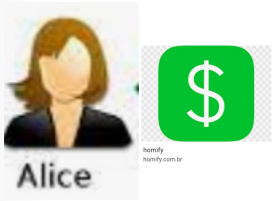
Sumário

- O que é blockchain?
- Por que blockchain?
- Tipos de implementação
- Primeira aplicação da blockchain: criptomoeda
- Principais componentes
  - Funções Hash
  - Livro-contábil imutável
  - Mineração
  - Protocolo de consenso

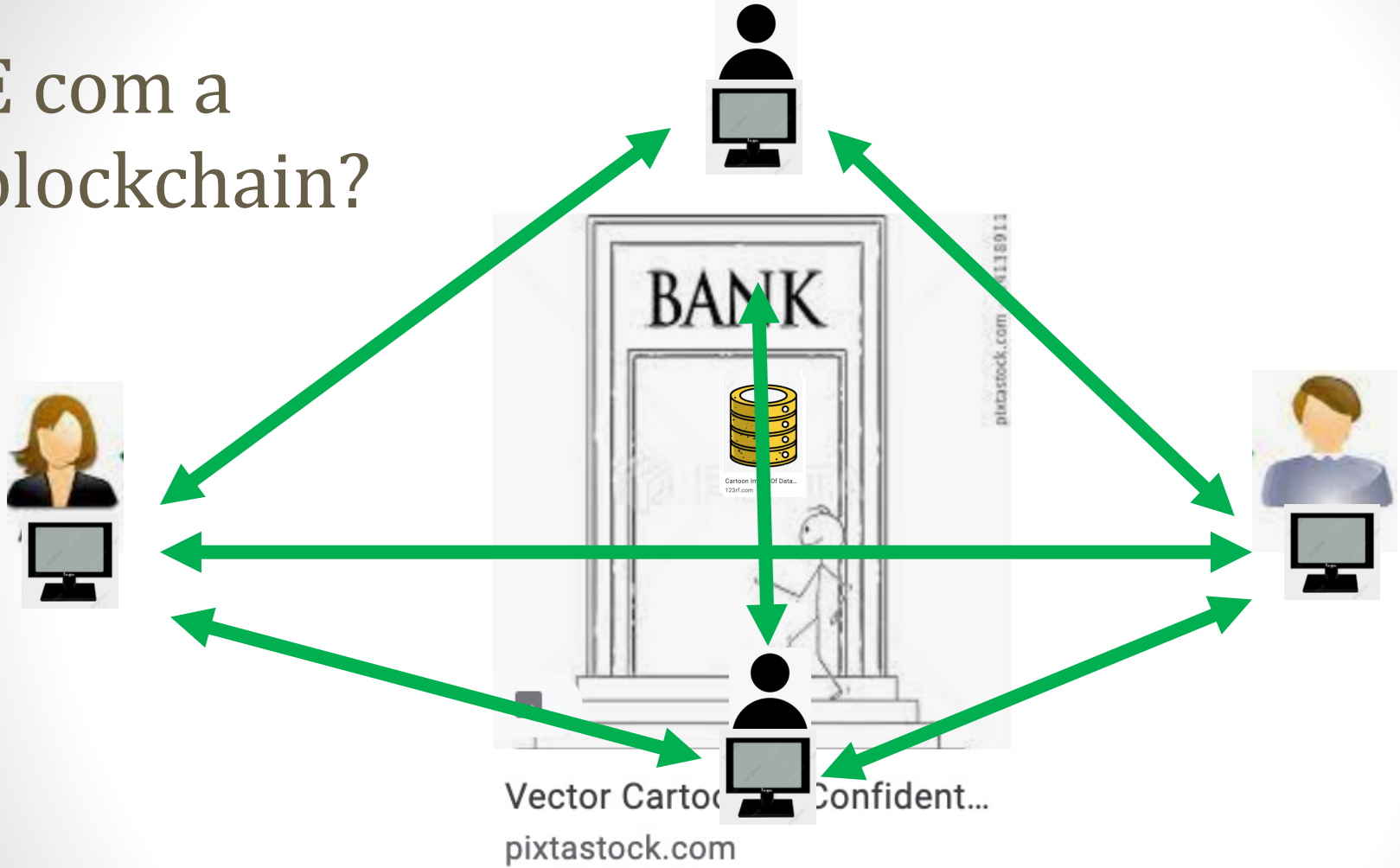
O que é blockchain?

Alice quer transferir $$ para Bob

Alice vai a um banco centralizado



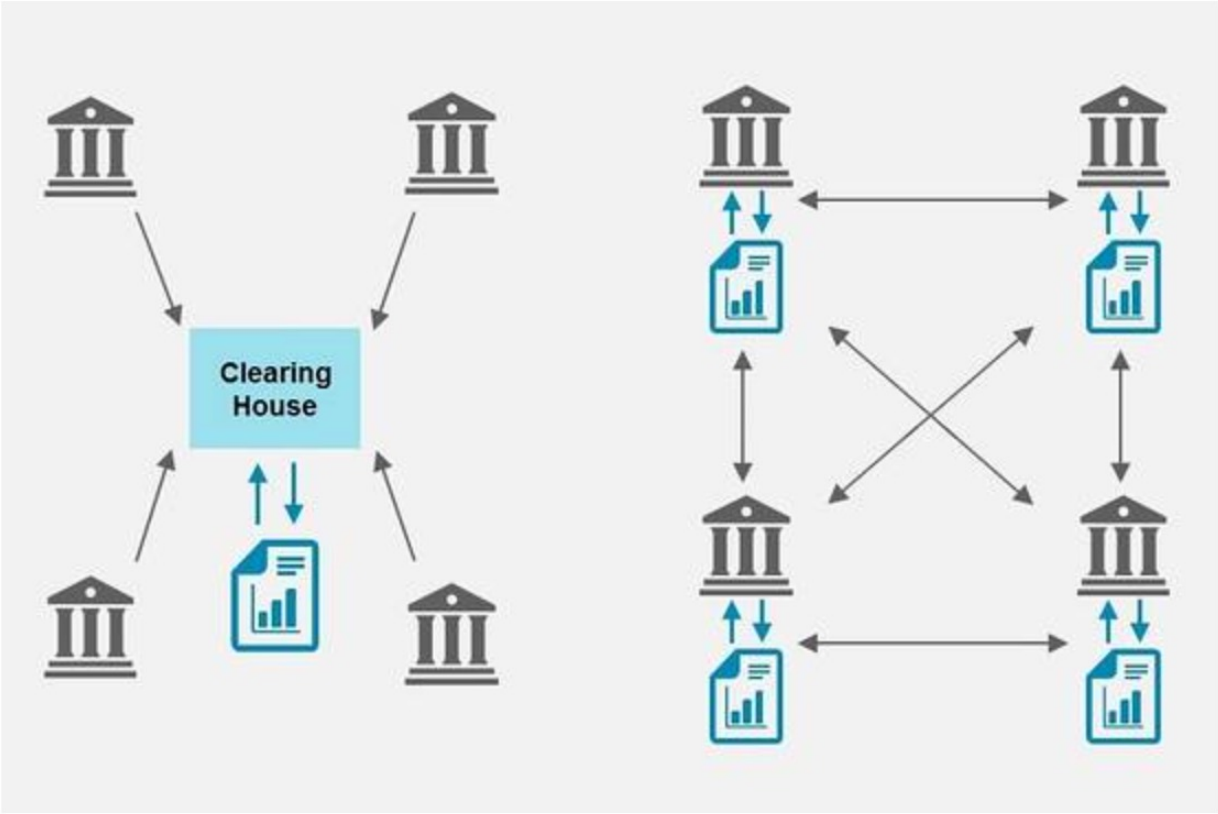
E com a blockchain?



E com a blockchain?

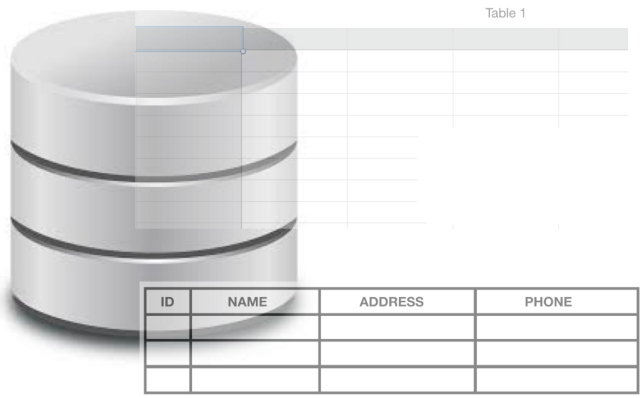
No Trusted Third Party!

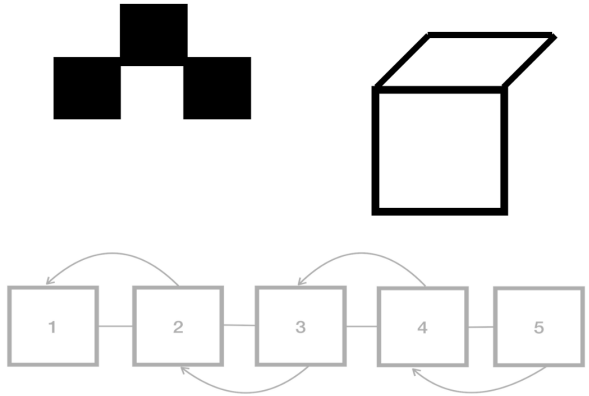
Fonte: https://smartenupinstitute.com/



Em resumo, o que é blockchain?

- É um banco de dados
- Armazena dados usando uma estrutura chamada blocos
- BD armazena dados em tabelas





HACKERNOON

Sumário

- O que é blockchain?
- Por que blockchain?
- Tipos de implementação
- Primeira aplicação da blockchain: criptomoeda
- Principais componentes
  - Funções Hash
  - Livro-contábil imutável
  - Mineração
  - Protocolo de consenso

Por que blockchain?

Custo

- Serviços de transferência de valores
- Impostos envolvidos

Tempo

- Alto tempo de processamento
- Transferências internacionais levam dias
- Lentidão

A pressa é inimiga da perfeição! Conheça o mov...
medium.com

Segurança

- Todos os participantes seguem um padrão de segurança

- Unimed, Lojas Americanas, Submarino sofreram ataques
- Enquanto outras mais seguras não
- Falta um padrão de segurança

- Segurança não fica atrelada a a um servidor centralizado

- Mecanismos de comunicação segura

Tolerância a falhas

- A base de dados é replicada, isto é, “espelhada”
- Atualização constante
- A replicação protege o ledger das(os):
  - Falhas
  - Ataques
- Seria muito útil para sistemas de saúde como o Connect SUS
  - Ficou inoperante por um período em virtude das falhas
  - Dados da vacina atualizados e disponíveis “world-wide”

Sumário

- O que é blockchain?
- Por que blockchain?
- Tipos de implementação
- Primeira aplicação da blockchain: criptomoeda
- Principais componentes
  - Funções Hash
  - Livro-contábil imutável
  - Mineração
  - Protocolo de consenso

Tipos de blockchain

1) Público – **Qualquer um pode entrar** e contribuir na rede

   Exemplo: Bitcoin, Ethereum

2) Privado – **Participantes devem ser convidados** para ser membro da rede

   Exemplo: Blockchain de uma organização (cadeia de suprimentos), Enterprise Ethereum

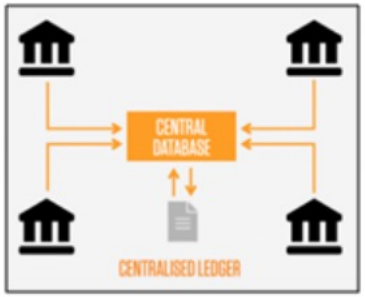
3) Permissionado – **Uma mistura das duas**: o participante pode ingressar na rede após verificação e;

   podem contribuir para certas atividades

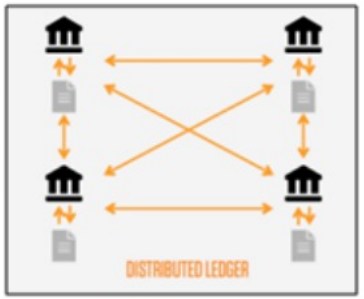
   Exemplo: Ripple

Tipos de blockchain

Centralized Ledgers
- Central trusted administrator or centralized record
- Single point of failure



Distributed Ledgers
- No central trusted administrator or centralized record
- No single point of failure



Public Permissionless
- No access restrictions
- Reliance on consensus protocols

ethereum HYPERLEDGER

Public Permissioned
- Relies on a shared distributed ledger
- Free access and participation
- Restricted access to transaction information for individual users

ethereum ripple HYPERLEDGER

Private Permissioned
- Access restricted to specific, approved parties
- Operated by a single organization or limited consortium
- Likely to include validation by trusted nodes

ethereum HYPERLEDGER r3·c·rda

Source: Capco; Beacon Research & Analysis

DLT e Blockchain

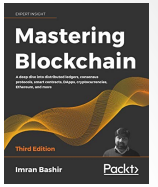
- Analogia com a classe e o objeto

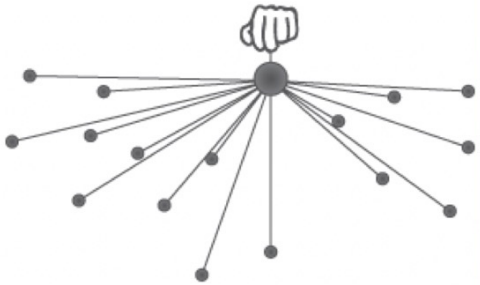
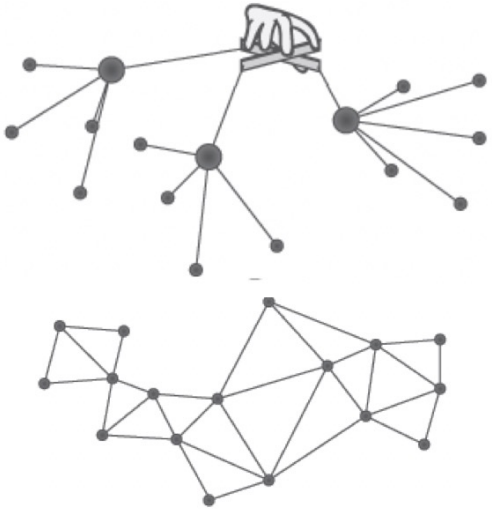
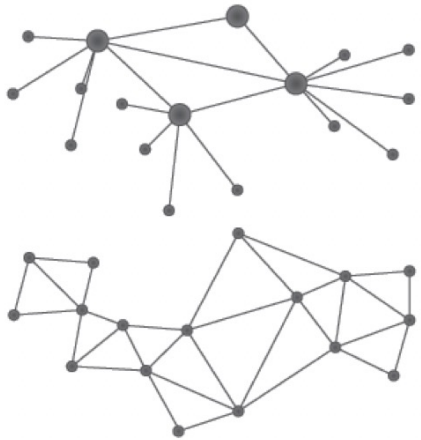
- DLT é simplesmente uma **base descentralizada** que é gerenciada por **vários participantes** em vários **nodos**

  Exemplo: Blockchain do Bitcoin, Blockchain do Ethereum, Tangle

- É uma implementação de DLT
  - Estrutura do bloco
  - Sequência de bloco
  - Protocolo de consenso

Blockchain é decentralizado

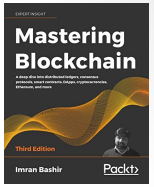


Centralized	Distributed	Decentralized
		

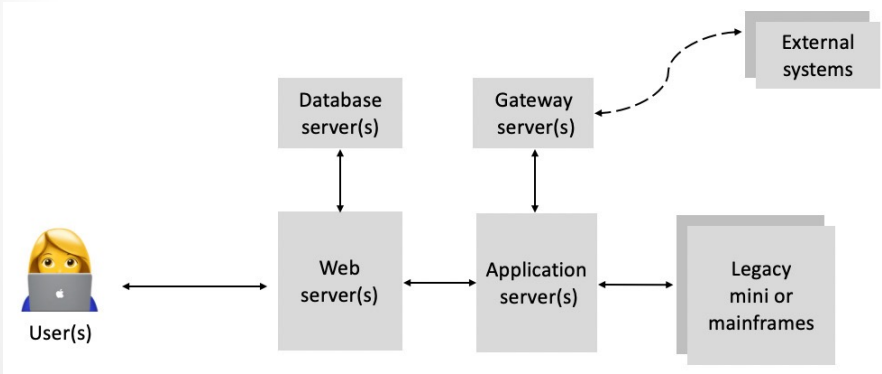
- Consenso alcançado por protocolos de consenso
- S/ *intermediary 3rd party*

Notice no hand
means no central controller / authority

Blockchain é decentralizado

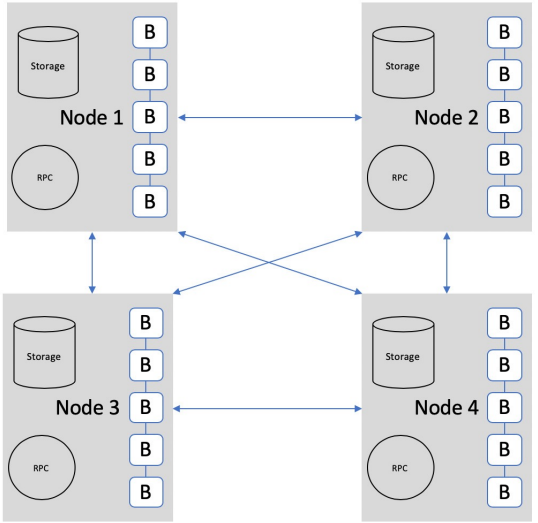


Distribuído



- No distribuído, há um controlador

Descentralizado



Sumário

- O que é blockchain?
- Por que blockchain?
- Tipos de implementação
- Primeira aplicação da blockchain: criptomoeda
- Principais componentes
  - Funções Hash
  - Livro-contábil imutável
  - Mineração
  - Protocolo de consenso

Bitcoin: Breakout To The Upside Is Most Likely (Technical Analysis)

Jul. 18, 2023 6:56 AM ET | **Bitcoin USD (BTC-USD)** | ETH-USD, SOL-USD |
11 Comments | 6 Likes

Em destaque

PayPal CEO Dan Shulman says cryptos will 'redefine the financial world' - CTech

Mar. 15, 2022 3:08 PM ET | **PayPal Holdings, Inc. (PYPL)**, **BTC-USD**, **ETH-USD** | SQ, V, MA ... | By: Max Gottlich, SA News Editor | 8 Comments

Sean Gallup/Getty Images News

Flutuação do Bitcoin

Valorização do Ethereum

Apple? Google?

PÁGINA INICIAL > AAPL • NASDAQ

Apple

$ 195,62 ↑56,41% +70,55 Acumulado do ano

28 de jul., 15:56:11 UTC-4 · USD · NASDAQ · Exoneração de responsabilidade

1 dia | 5 dias | 1 mês | 6 meses | YTD | 1 ano | 5 anos | MÁX. | Eventos principais

PÁGINA INICIAL > GOOGL • NASDAQ

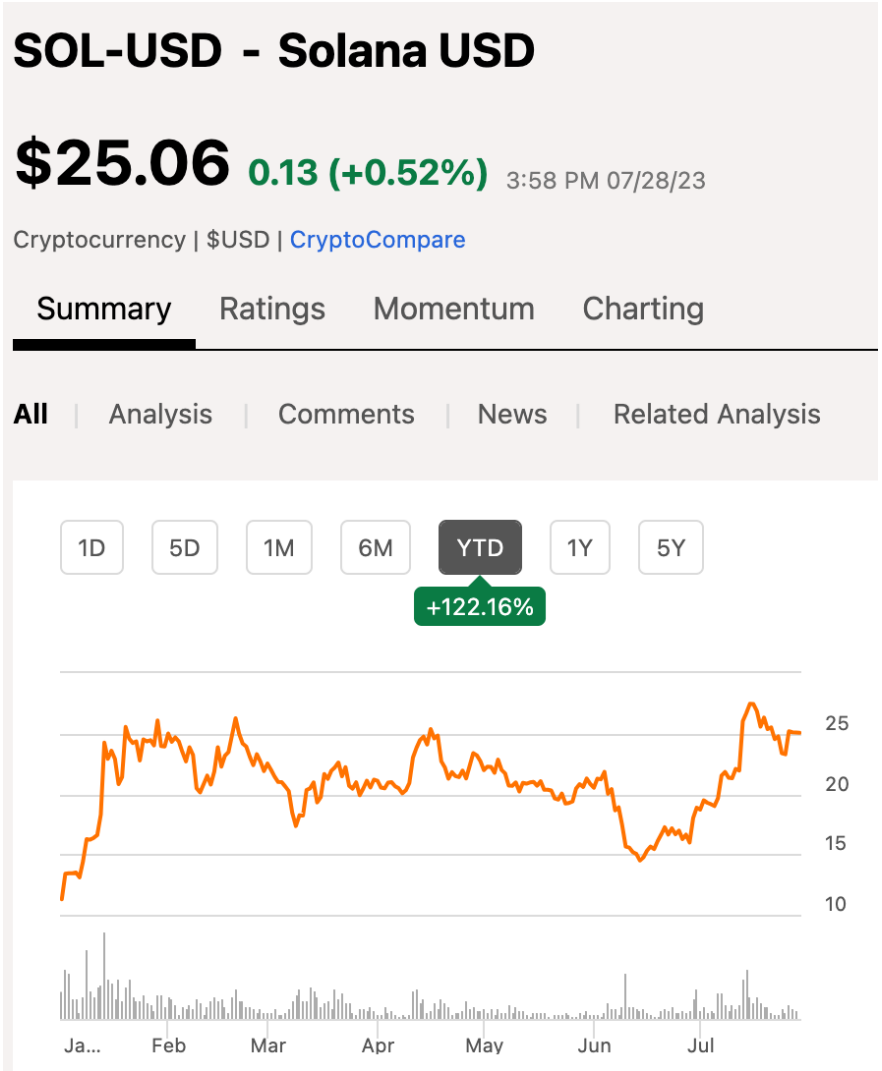
Alphabet Inc.

$ 132,53 ↑48,71% +43,41 Acumulado do ano

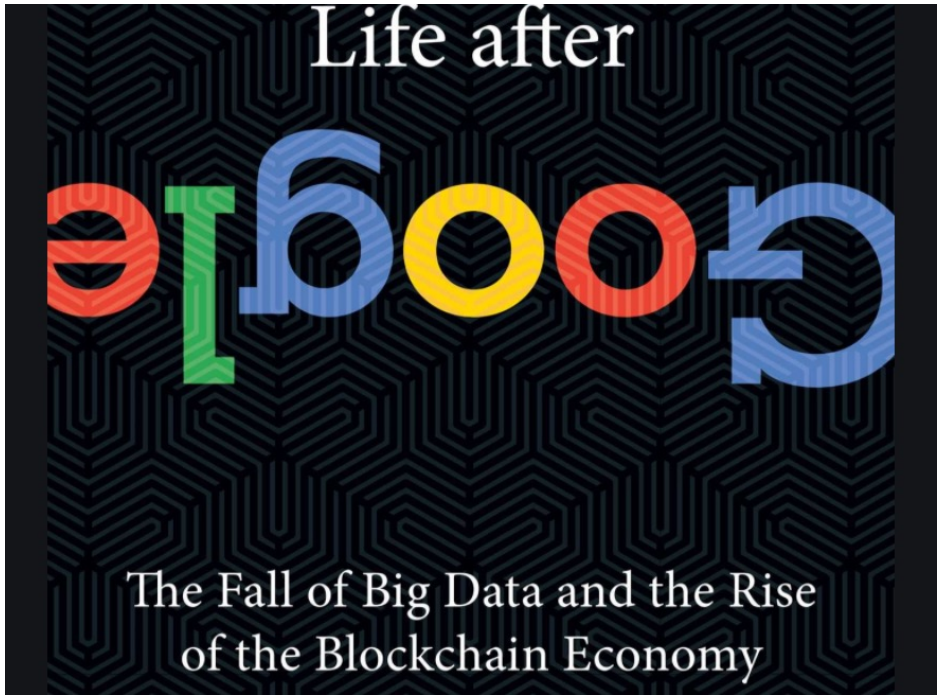
28 de jul., 15:56:47 UTC-4 · USD · NASDAQ · Exoneração de responsabilidade

1 dia | 5 dias | 1 mês | 6 meses | YTD | 1 ano | 5 anos | MÁX. | Eventos principais

E a SOL?


SOL-USD - Solana USD
$25.06 0.13 (+0.52%) 3:58 PM 07/28/23
Cryptocurrency | $USD | CryptoCompare
Summary Ratings Momentum Charting
All | Analysis | Comments | News | Related Analysis
1D 5D 1M 6M YTD 1Y 5Y
+122.16%
25
20
15
10
Ja... Feb Mar Apr May Jun Jul

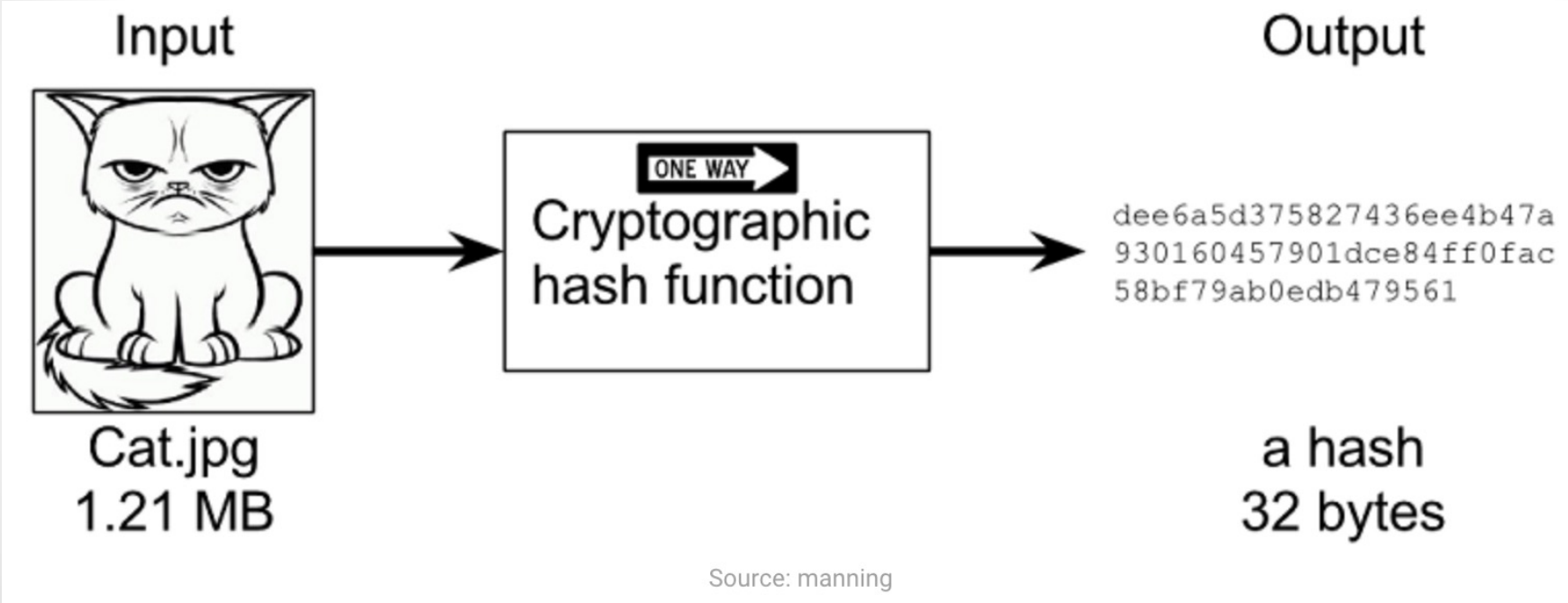
Uma discussão sobre o futuro



Sumário

- O que é blockchain?
- Por que blockchain?
- Tipos de implementação
- Primeira aplicação da blockchain: criptomoeda
- Principais componentes
  - Funções Hash
  - Livro-contábil imutável
  - Mineração
  - Protocolo de consenso

Componente 1: funções Hash

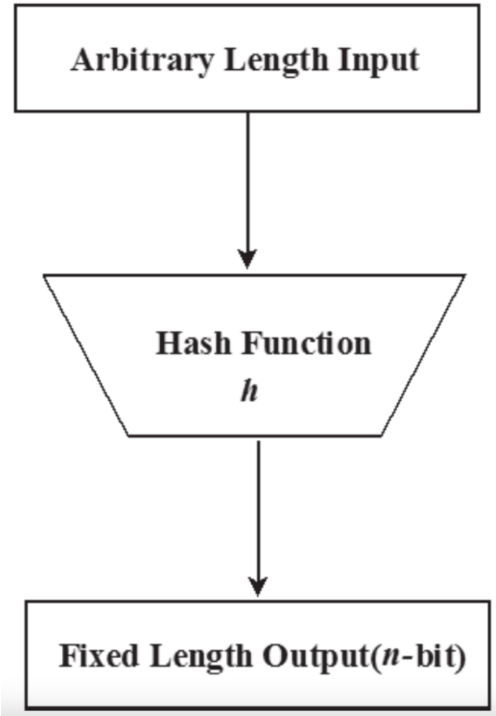


Source: manning

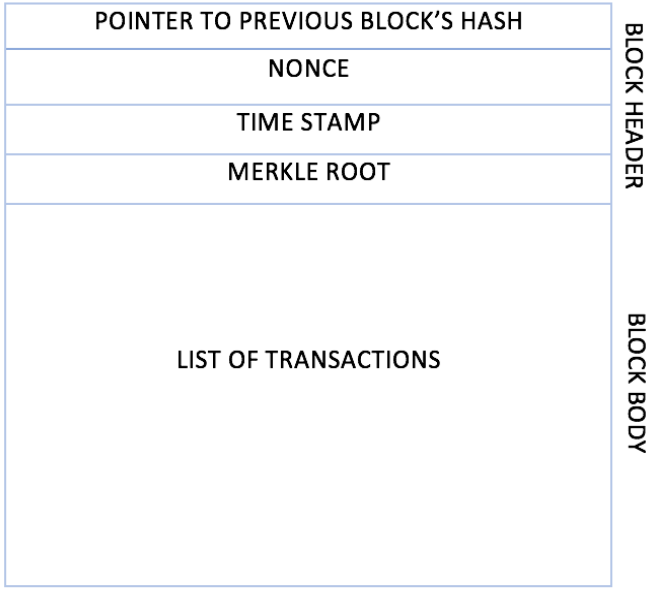
O que é uma função hash?

- Funciona como uma **impressão digital**
- **Difícil** haver **duas pessoas com a mesma digital**
- Assim como uma pessoa, um documento pode ter uma impressão digital
  - Um vídeo, uma transação e assim por diante

What is Biometrics? | Touchless Biometric ...
tbs-biometrics.com



Estrutura do bloco blockchain com Hash



- Merkle root contém o hash do bloco
- O hash é quem **assegura a imutabilidade** do bloco
- **Efeito avalanche**

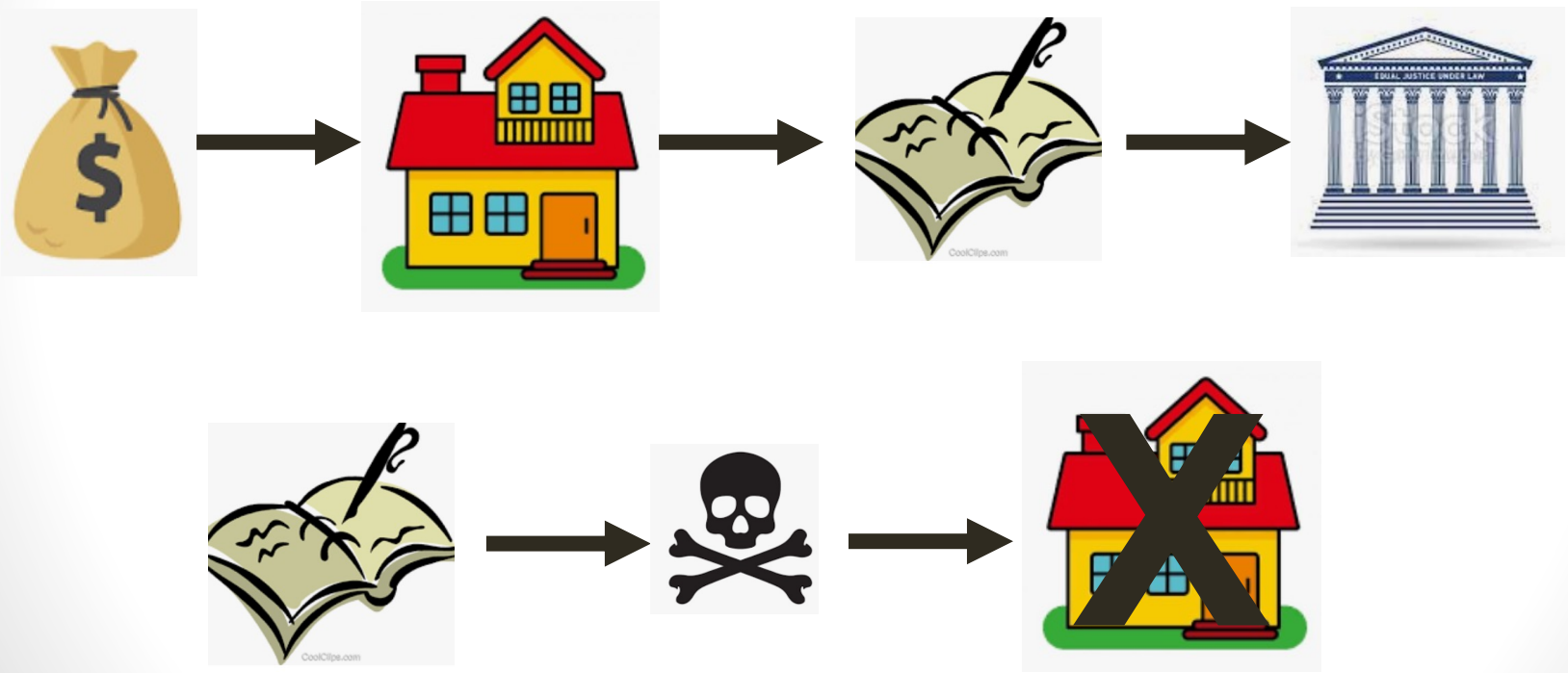
Jó Ueyama
bed0d388a0d3d8df4ed97ddcea18e89bf6e6f92050014c421db1ee0519a0d2d7

Jo Ueyama
d1c93206a46b1a9c9f245195807711170a187c7b387145e035df5e5050fefb5b2

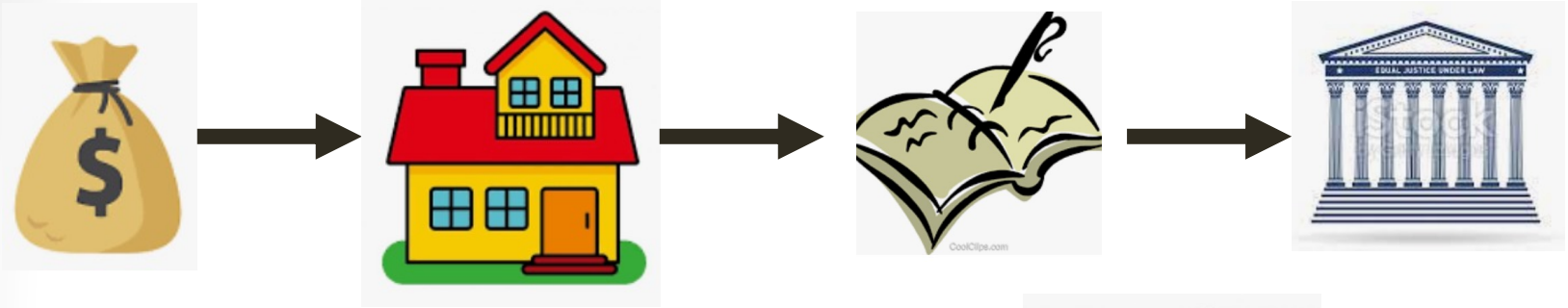
Sumário

- O que é blockchain?
- Por que blockchain?
- Tipos de implementação
- Primeira aplicação da blockchain: criptomoeda
- Principais componentes
  - Funções Hash
  - Livro-contábil imutável
  - Mineração
  - Protocolo de consenso

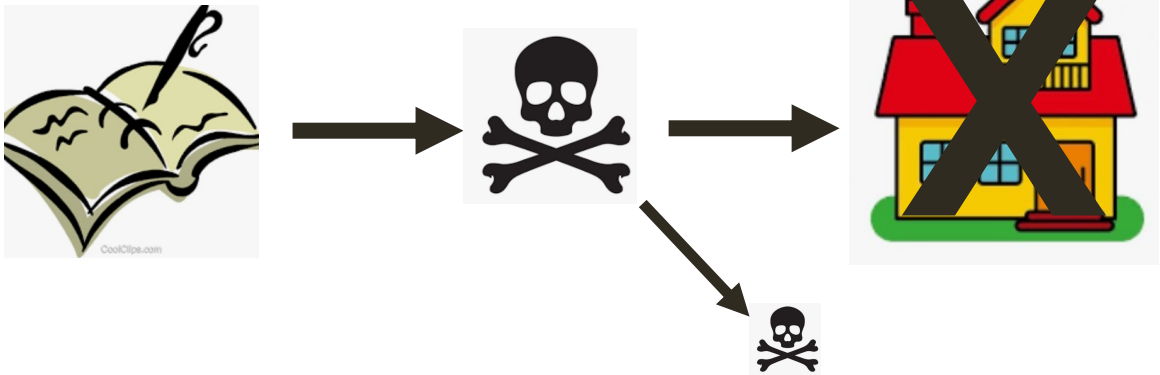
Livro-contábil imutável



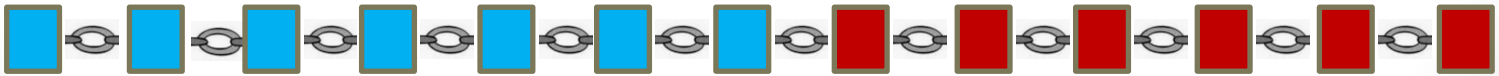
Livro-contábil imutável c/ blockchain



Ledger tradicional

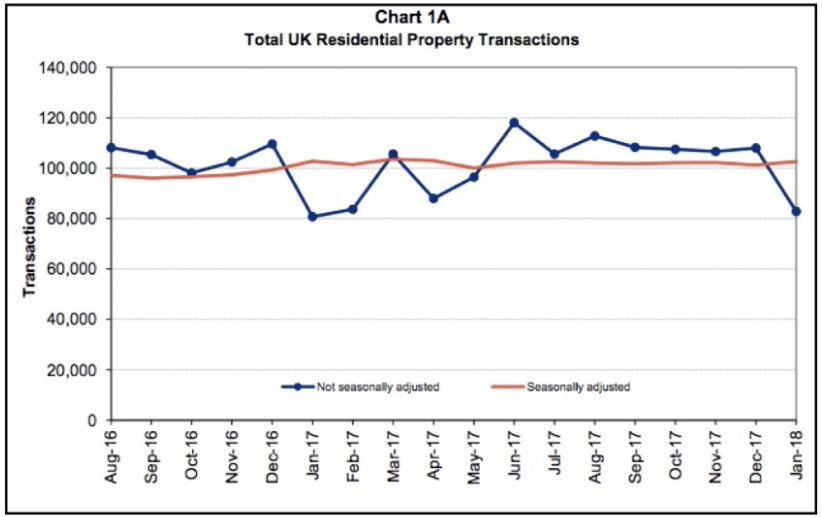


Blockchain



Livro-contábil imutável

- No cenário real: mudança de títulos residenciais acima de GBP40K
- Algo em torno de 100 transações por hora
- Suscetível a erros e fraudes



Source: https://www.gov.uk

Sumário

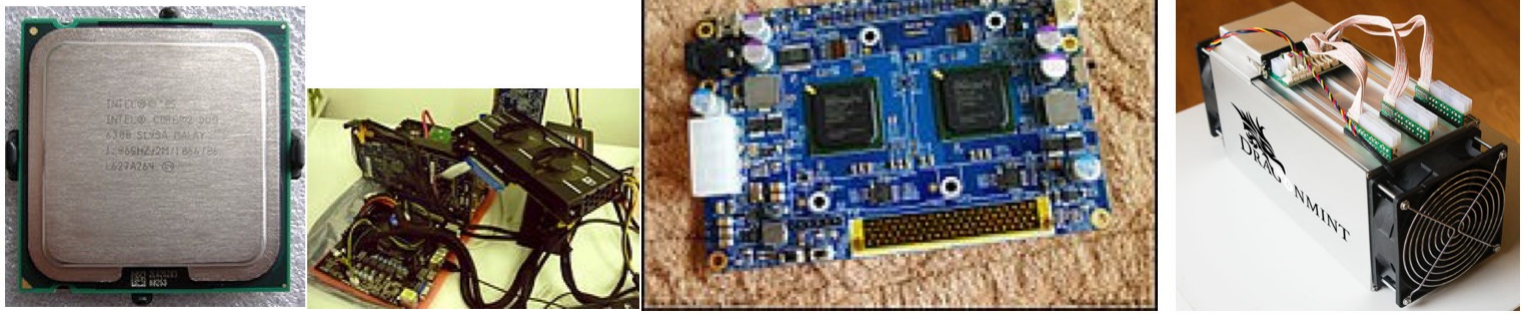
- O que é blockchain?
- Por que blockchain?
- Tipos de implementação
- Primeira aplicação da blockchain: criptomoeda
- Principais componentes
  - Funções Hash
  - Livro-contábil imutável
  - Mineração
  - Protocolo de consenso

Mineração de blocos

High Quality Padlock Solid Br...
aliexpress.com

- É como cadeados com segredo
  - É difícil de adivinhar
  - Toma bastante tempo para testar
  - 10.000 tentativas com segredo de 4 dígitos
  - Ganha quem tem maior poder computacional
    - O mesmo ocorre com a mineração
  - Mas por outro lado é fácil de testar o segredo desde que ele tenha sido fornecido
    - Trabalho de nodos pares na blockchain

Mining systems



Quatro plataformas de hardware: CPU, GPU, FPGA e um ASIC

Sumário

- O que é blockchain?
- Por que blockchain?
- Tipos de implementação
- Primeira aplicação da blockchain: criptomoeda
- Principais componentes
  - Funções Hash
  - Livro-contábil imutável
  - Mineração
  - Protocolo de consenso

Principais componentes da blockchain

- Funções Hash
- Livro-contábil imutável
- Mineração
- Protocolo de consenso

Protocolo de consenso

- É fácil atingir um acordo em cliente/servidor
  - O servidor “manda” e detém as regras
  - O cliente confia no servidor
  - P.ex., o cliente confia no Banco do Brasil

- Mas em um ambiente sem um intermediário confiável?
- Ambiente com nodos que podem estar defeituosos
- Ambiente carece de regras para se chegar a um consenso
- Alguém tem que mandar? Mas quem? O protocolo de consenso

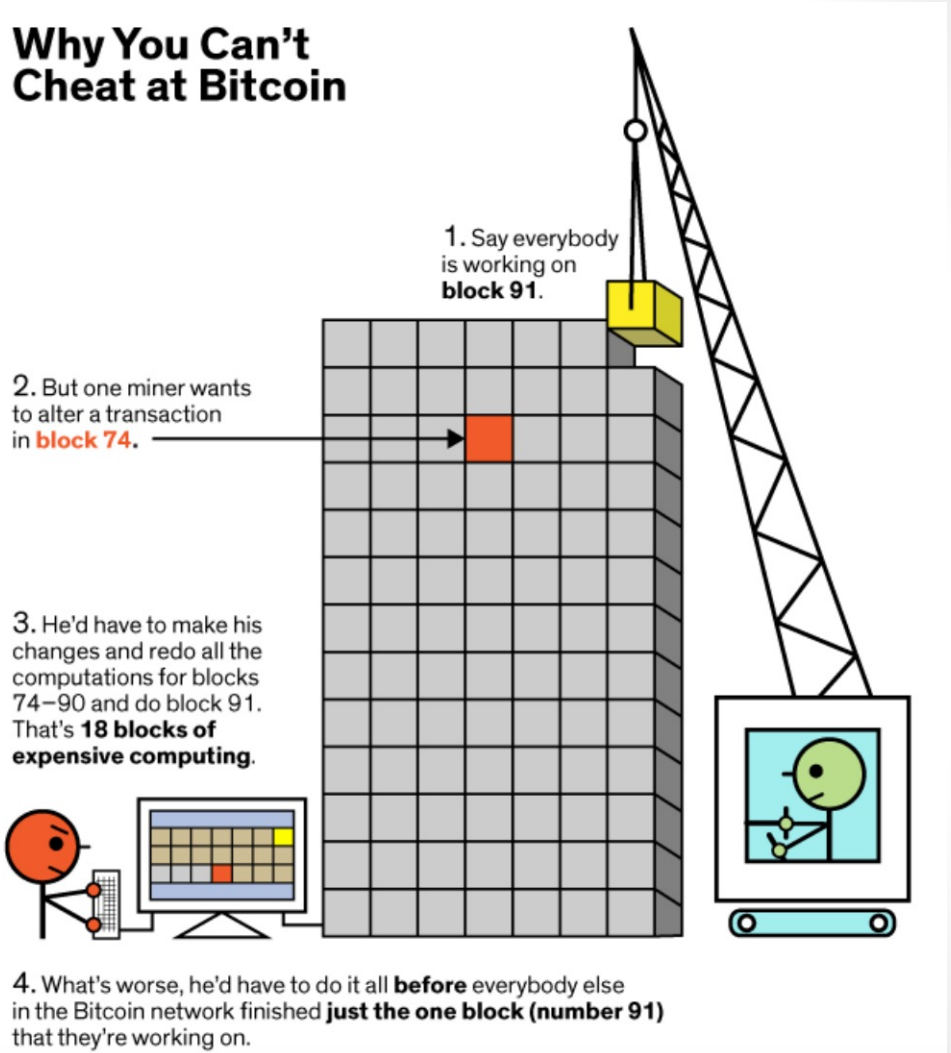
- **Protocolo que dita o acordo entre os nodos não-confiáveis sobre os dados na blockchain**
- P.ex., quem vai criar o novo bloco?

Proof of Work (PoW)

- Adotado no Bitcoin (SHA256) e no Ethereum (KECCAK-256)
- Os nodos competem entre si para encontrar o padrão de hash
- Normalmente com cerca de 18 zeros na frente
- Este padrão é ajustado periodicamente

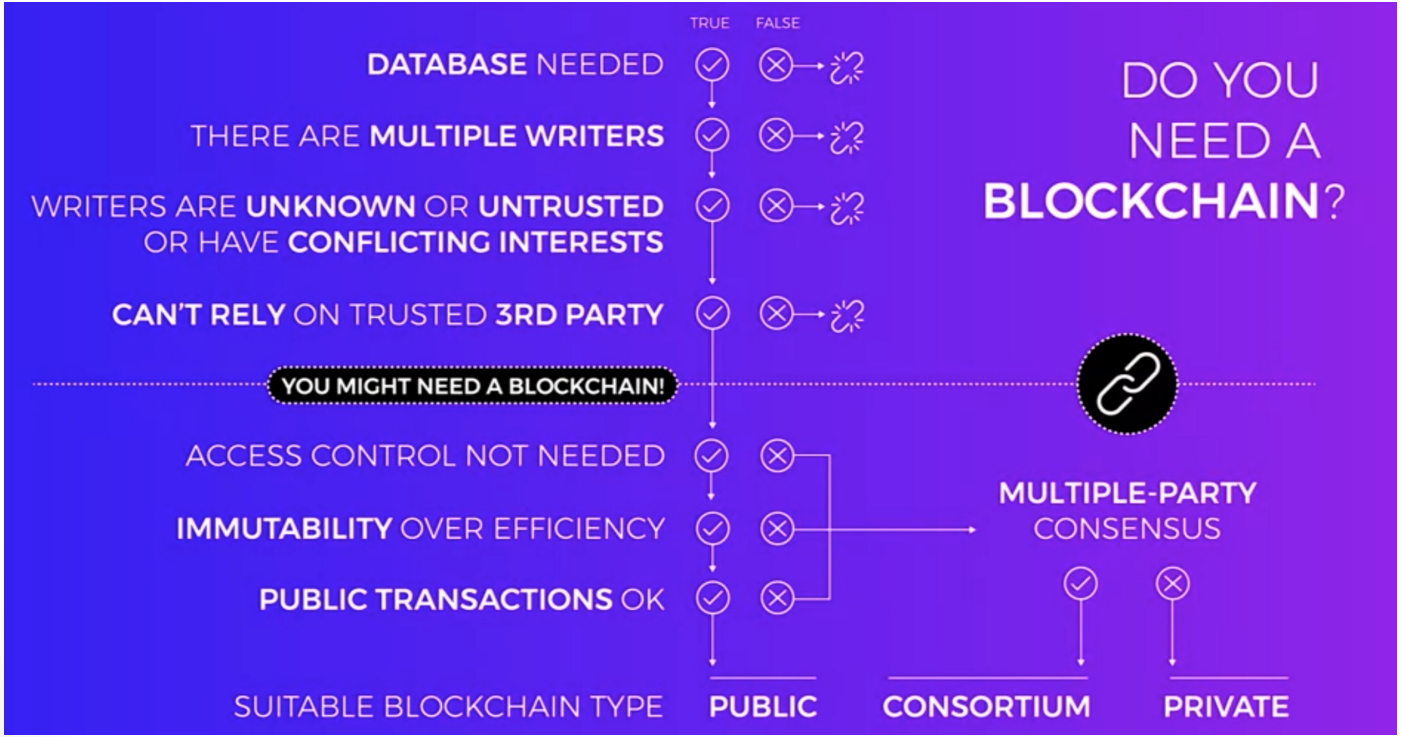
- Como o custo computacional é alto, isto seria um **desincentivo para os *hackers***

Por que é difícil atacar o Bitcoin?



www.medium.com

Blockchain é para todas os sistemas?



Fonte da ilustração: coursera

Exercícios da aula

1) Escreva um pseudo-código da mineração do blockchain para hashes começando com quatro zeros
2) Explique o porquê do Proof of Work do Bitcoin ser difícil de minerar, porém de ser fácil para verificar
3) Cite o que um mecanismo presente em um sistema decentralizado que não é encontrado em um ambiente distribuído
4) Descreva um sistema para meio-ambiente que requeira o uso da blockchain e mostre como ela é atende os requisitos citados
5) Cite duas desvantagens presentes em um sistema baseado na blockchain

Blockchain e Criptomoedas

Prof. Jó Ueyama