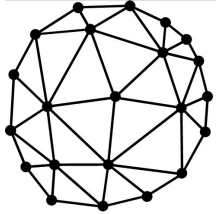
Blockchain, Bitcoin e outras aplicações para além das criptomoedas

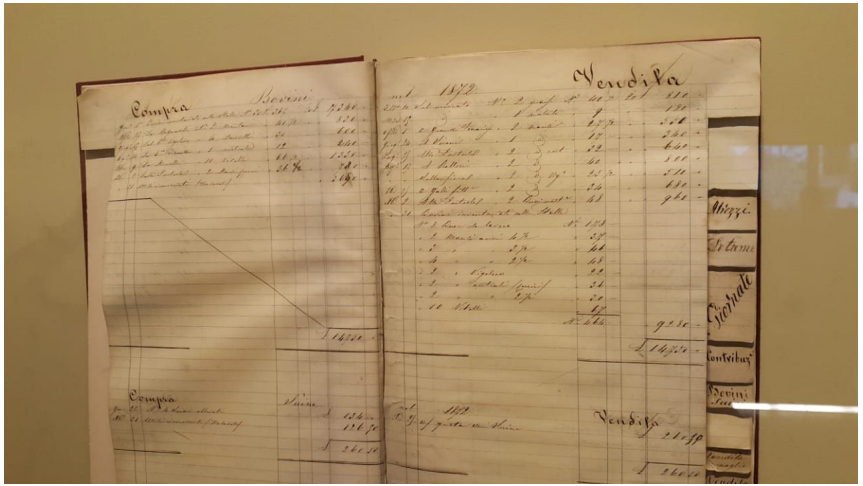
Arlindo Flavio da Conceição (arlindo.conceicao@unifesp.br)



Sobre o que vamos conversar?

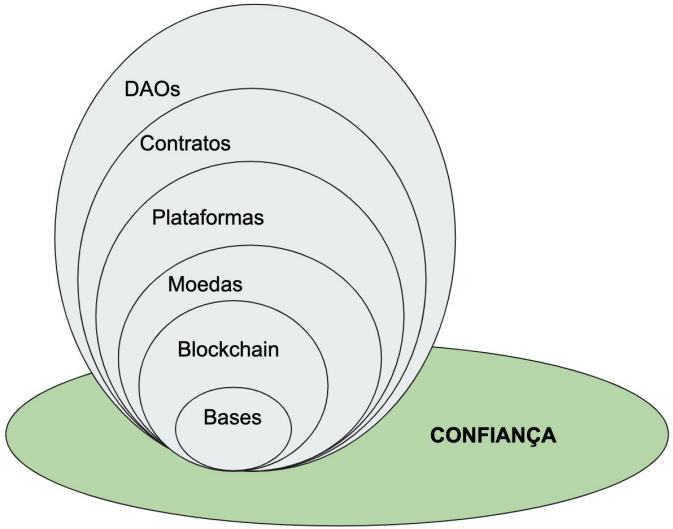
- Blockchain
- Bitcoin
  - *Advertência: Bitcoin é apenas uma aplicação...*
- Aplicações no futuro e o impacto no nosso cotidiano
- Como se aprofundar no assunto?

Blockchain: um livro razão descentralizado

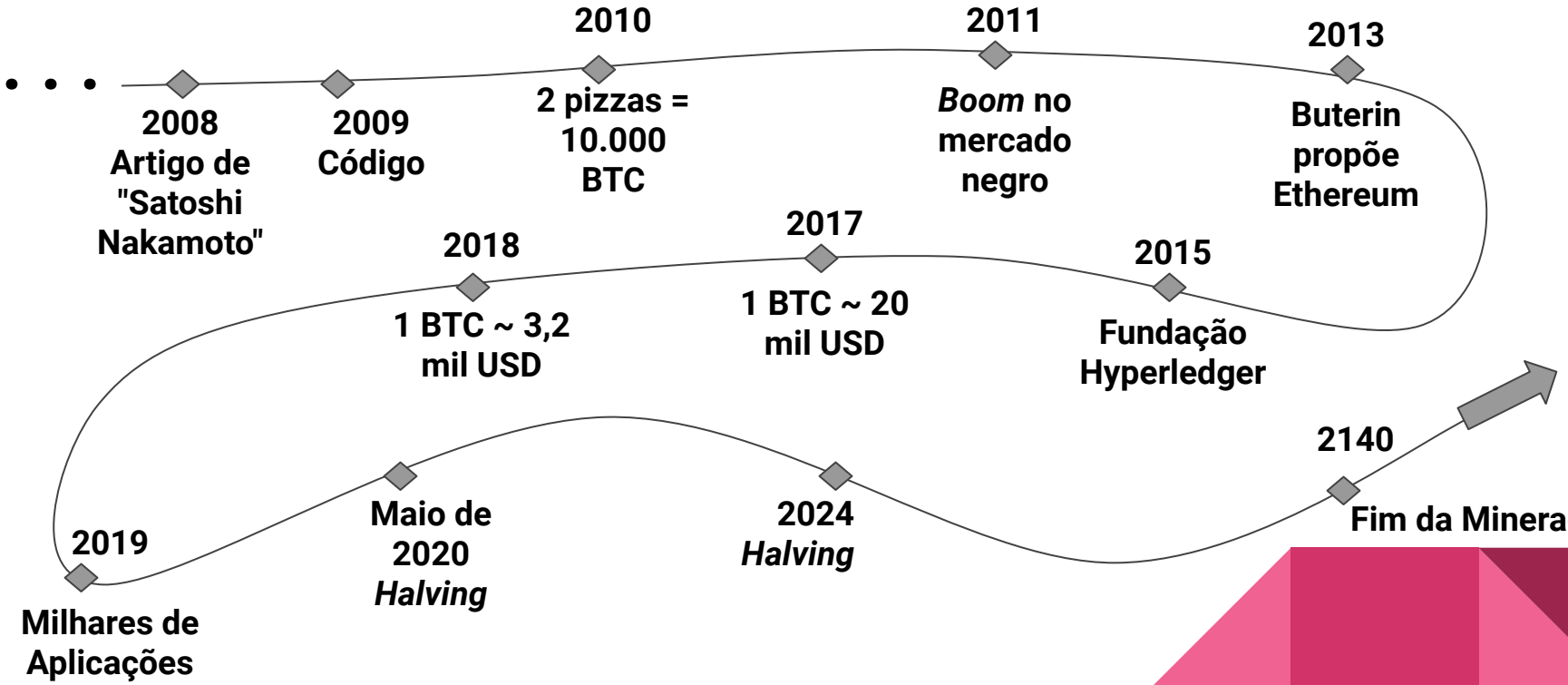


Blockchain: confiança

- Descentralizado
- Seguro
- Imutável
- Anonimizado
- Desintermediação
- Auditável
- **Confiável**

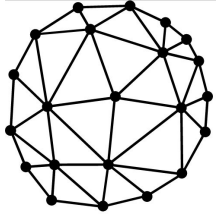


Linha do tempo (incompleta)



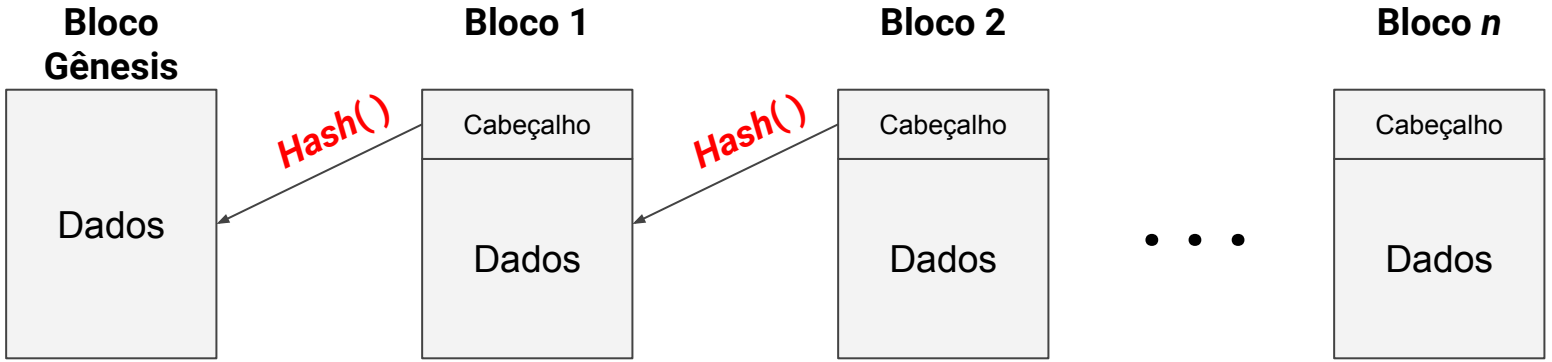
* Valores e datas aproximadas

Blockchain: como funciona?



- Pilares de Blockchain
  - ***Peer-to-peer*** para maior disponibilidade e menor poder de controle
  - Mecanismos **criptográficos**
    - Função *Hash,* chaves assimétricas (pública e privada) e assinatura digital
  - Mecanismo de **consenso** distribuído para que haja uma visão consistente do sistema
  - **Software livre** para obter transparência
  - **Incentivos econômicos** para garantir sustentabilidade

Blockchain: estrutura básica



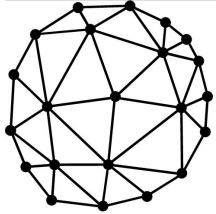
- A cadeia de blocos cresce ao longo do tempo
- **Imutável**, rastreável e auditável
- Cabeçalhos e Dados
  - O que podem ser os dados?

Bitcoin: um exemplo de aplicação

- É a mais antiga e bem sucedida moeda digital

Fonte: https://coinmarketcap.com/currencies/bitcoin/

Como funciona o Bitcoin?

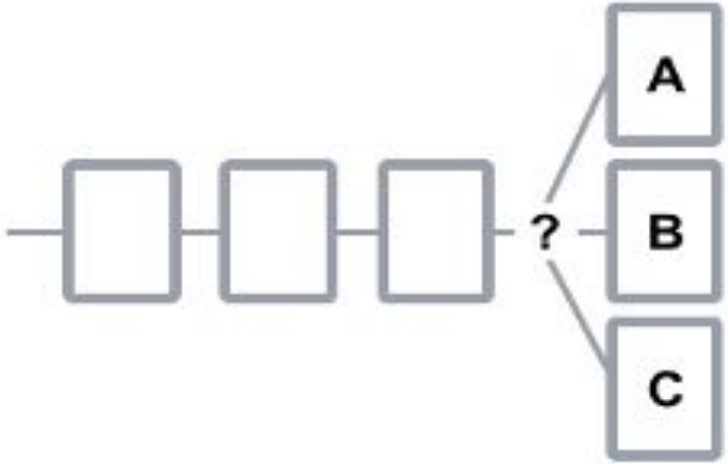


- Transações são continuamente lançadas na rede de nós
- Prova de trabalho (consenso no Bitcoin, ou eleição)
  - Nós **mineradores** tentam resolver um problema matemático
  - Quem resolver primeiro fecha um bloco de transações
    - Um novo bloco aproximadamente a cada 10 min.
    - Este nó recebe 12,5 BTC e taxas de validação.
- O novo bloco é distribuído aos nós da rede, os nós verificam os dados e incrementam a cadeia de blocos

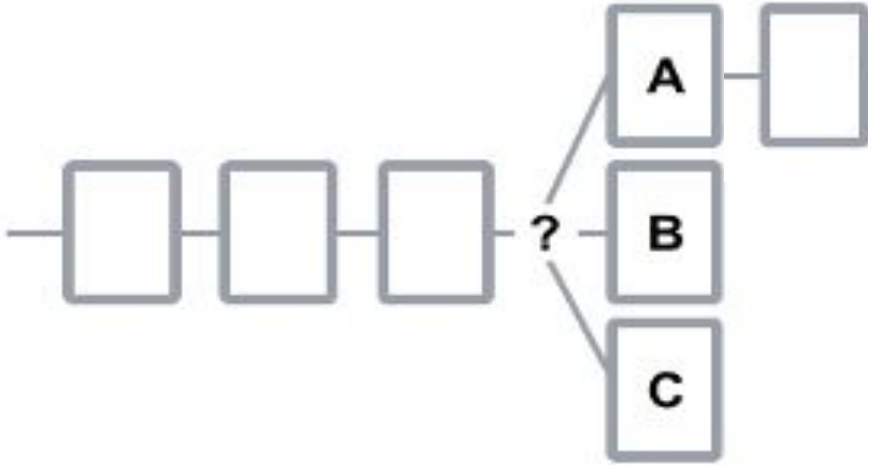
A cadeia de blocos de Bitcoin

- Lembrete: é uma rede com cerca de 10 mil nós.
- Um novo bloco aproximadamente a cada 10 minutos
- O que aconteceria se dois ou três mineradores fechassem blocos quase ao mesmo tempo?

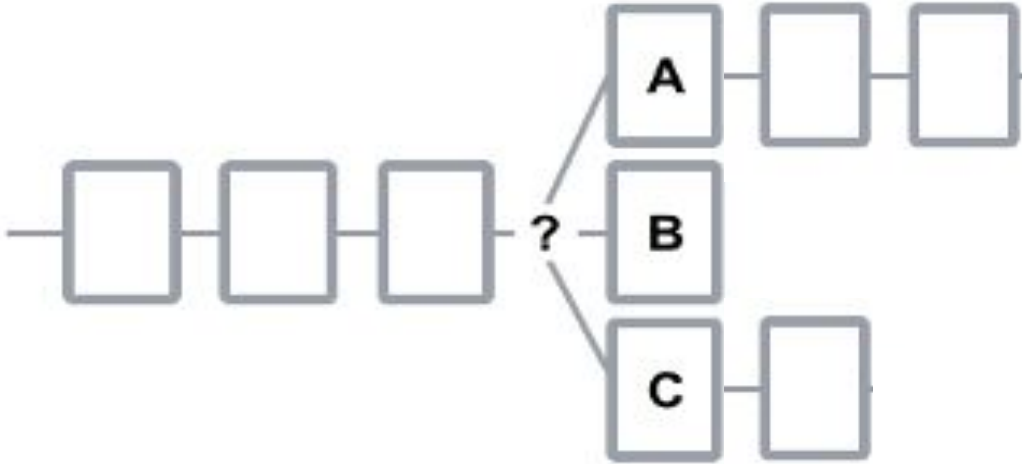
A cadeia de blocos de Bitcoin



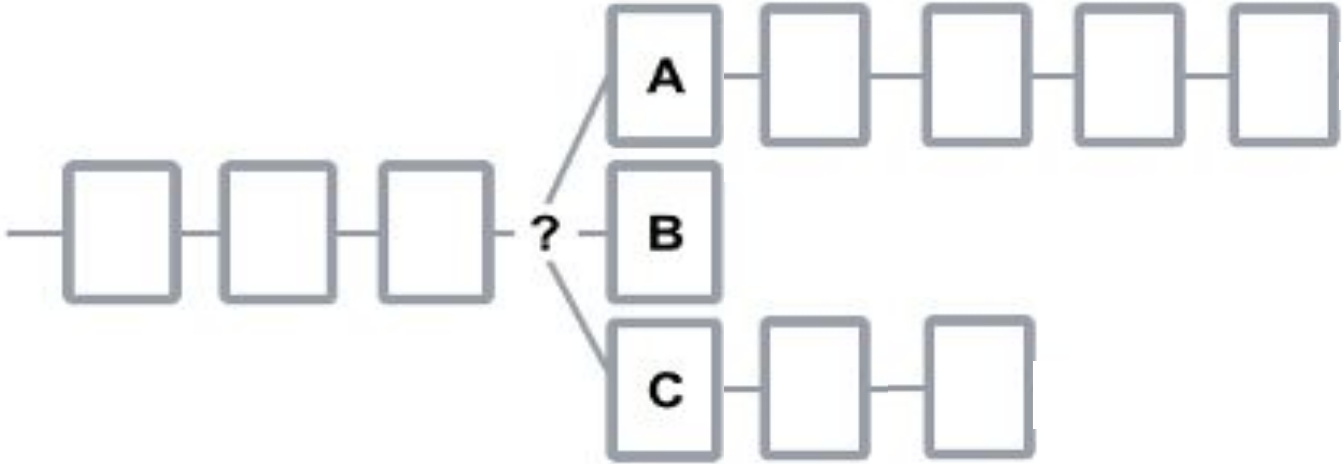
A cadeia de blocos de Bitcoin



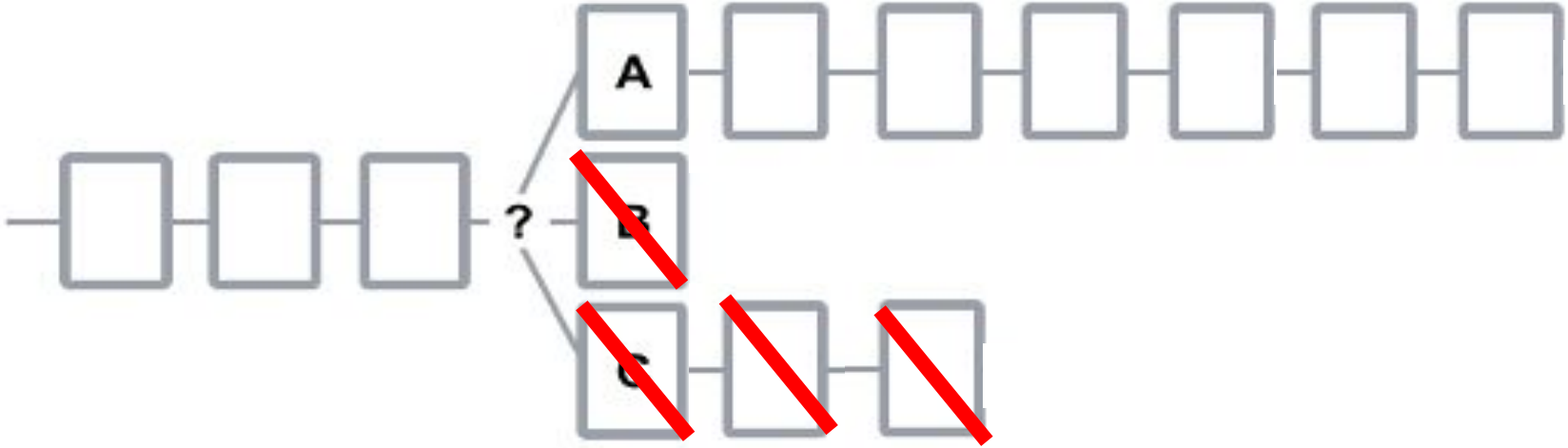
A cadeia de blocos de Bitcoin



A cadeia de blocos de Bitcoin

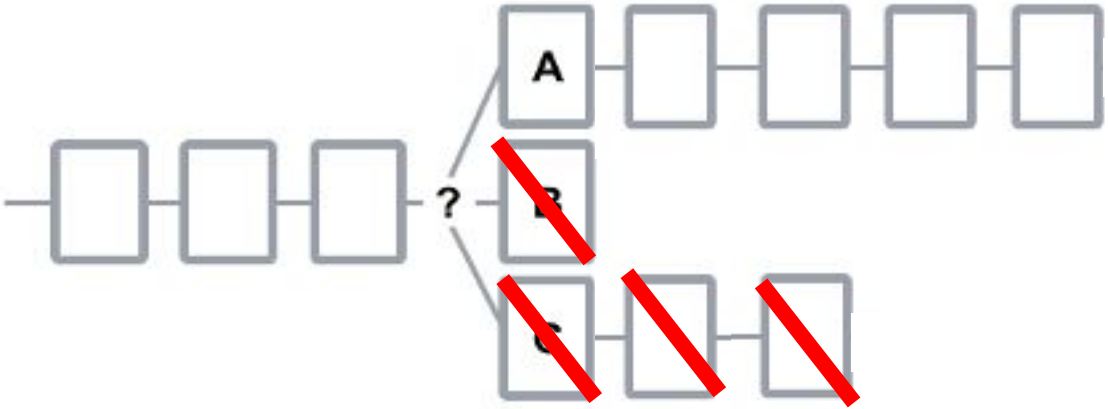


A cadeia de blocos de Bitcoin



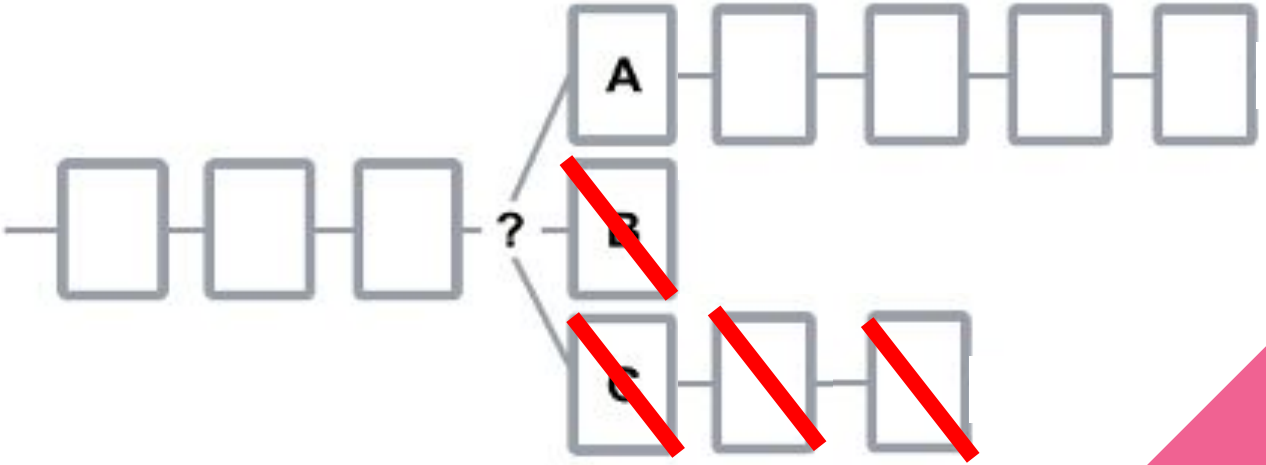
A cadeia de blocos de Bitcoin

- Apenas a cadeia mais longa é mantida
- As transações em blocos cancelados são **desconsideradas**



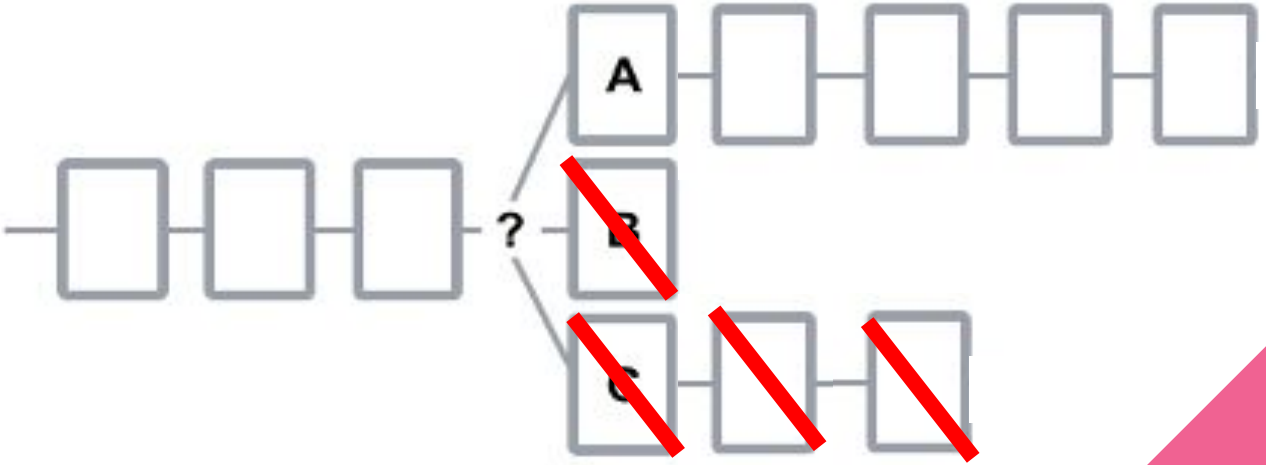
Fraudes: gasto duplo

- Verifica-se toda a cadeia válida

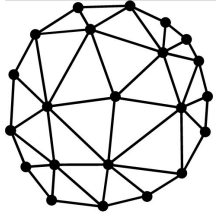


Fraudes: ataque de 51%

- Se um conjunto de mineradores conseguir dominar a rede, eles podem manipular a cadeia mais longa.

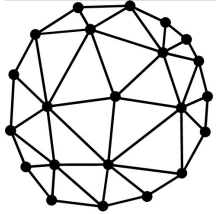


Avanços recentes



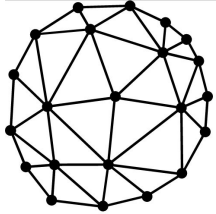
- Blockchain 2.0
  - Principal representante: Ethereum e Hyperledger
  - Contratos inteligentes
- Blockchain 3.0
  - Principais representantes: IOTA (Tangle) e Swirlds (Hashgraph)
    - Não baseados em Blockchain :-)
  - Melhor desempenho e mais segurança

Contratos Inteligentes (DApp)



- E se a Blockchain pudesse armazenar não apenas transações e dados, mas também **comportamentos e regras**?

- Um contrato inteligente é um programa de computador de uso geral que pode ser armazenado na Blockchain e executado pelos nós.
- As aplicações construídas usando Contratos Inteligentes são chamadas de **Aplicações Descentralizadas**, ou **DApps**.

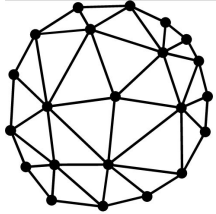


Organizações Autônomas e Descentralizadas (DAO)

- E se, usando Contratos Inteligentes, fosse possível automatizar todo o funcionamento de uma empresa ou organização social?
  Sem custos operacionais, salários ou subjetividade de decisões...

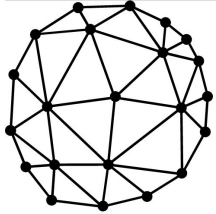
  - Exemplos?

Novas aplicações no futuro



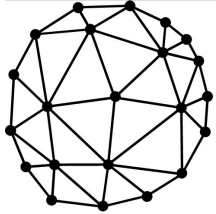
- Criptomoedas
- Cadeia de suprimentos
  - Alimentos, cadeias ecológicas, manutenção de veículos, etc.
- Recursos digitais (*digital assets*)
  - Cartórios, universidades (diplomas), ingressos, eleições, jogos, etc.
- Desintermediação
  - AirBNB, Uber, Spotify, Seguro Saúde, etc.
- Cidades Inteligentes

Proteção de Dados



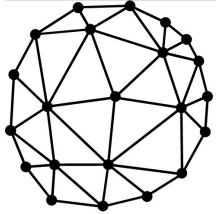
- GDPR (*General Data Protection Regulation*)
  - https://eur-lex.europa.eu/eli/reg/2016/679/oj
- LGPD (Lei Geral de Proteção de Dados)
  - Vigência a partir de agosto de 2020
  - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- Blockchain pode proteger dados de clientes
  - Registro de transações
  - Requisitos: identificação anônima e contratos de "esquecimento"

Controle Tributário

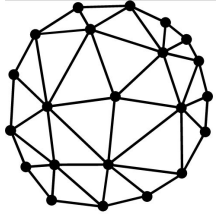


- Está em andamento a reforma tributária…
- Problemas atuais: fraudes, sonegação, rastreamento, etc.
- **E se** toda transação financeira fosse registrada de forma anônima em uma Blockchain?
- Blockchain pode proteger dados de clientes
  - Requisitos: identificação anônima e contratos de "esquecimento"

Dados de Saúde



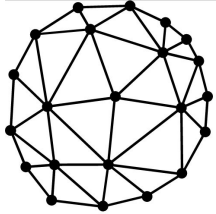
- **E se** toda ação referente a saúde fosse gravada em uma Blockchain?
- Identificação única
- Interoperabilidade de dados
- Validação de procedimentos
- Desintermediação de serviços
- Saúde coletiva
- Etc.



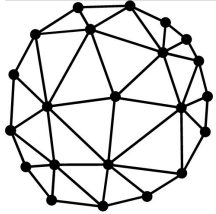
Aplicações de Blockchain em Cidades Inteligentes

- Casos de estudo: Talim, Singapura, Shenzhen, etc.
- Pagamentos eletrônicos
- Identidade única e segura dos cidadãos
  - Identidades auto-soberanas
- Interoperabilidade de dados
- Transparência de contas públicas
- Agilidade de serviços

Sobre o que nós não falamos...

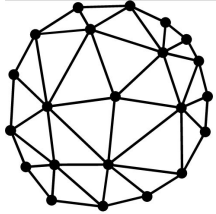


- Blockchains públicas, privadas e federadas
- Blockchain é uma excelente ferramenta mas não deve ser usada para tudo
  - Não é um banco de dados
  - Não é um servidor de transações
  - **Se você confia em todos os membros da rede você não precisa de Blockchain**
- Custos para manter uma rede Blockchain
- Novas fraudes e o uso para fins duvidosos
- Regulamentação



Para saber mais...

- Artigo de Satoshi Nakamoto
  - https://bitcoin.org/bitcoin.pdf
- Rede Ethereum
  - https://ethereum.org e https://www.coursera.org/learn/smarter-contracts
- Projeto Hyperledger
  - https://www.hyperledger.org
- Coin Telegraph
  - https://cointelegraph.com
- Podcasts, livros, coursera, etc.



Agradecimentos e perguntas...

- Obrigado ao InterSCity e ao Espaço T.A.Z.
- Contatos: Arlindo Flavio da Conceição
  arlindo.conceicao@unifesp.br
- Perguntas?