



# Disciplina sobre Blockchain

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



# O que é Blockchain?

# O que é Blockchain?

Livro-razão distribuído





## Definindo Blockchain...

- É um algoritmo? Não só.
- É uma estrutura de dados? Não apenas.
- É uma moeda digital? Não somente.
- É um protocolo? Mais de um...
- É um livro caixa? É mais do que isso...

*"Blockchain é uma tecnologia **emergente** que oferece suporte distribuído **confiável** e **seguro** para realização de transações entre participantes que não necessariamente têm **confiança** entre si e que estão dispersos em **larga escala** numa rede P2P."*

Fabíola Greve et al., SBRC, 2019, grifos meus.



# Benefícios de Blockchain?

*Fonte: Greve 2019.*

- **Descentralização:** Sistemas e aplicações que usam a BC não precisam de uma entidade central para coordenar as ações, as tarefas são executadas de forma distribuída;
- **Disponibilidade e integridade:** Os dados e as transações são replicados para todos os participantes da BC, mantendo o sistema seguro e consistente;
- **Transparência e auditabilidade:** A cadeia de blocos que registra as transações é pública e pode ser auditada e verificada;
- **Imutabilidade e Irrefutabilidade:** os registros são imutáveis e a correção só pode ser feita a partir de novos registros. O uso de recursos criptográficos garante que os lançamentos não podem ser refutados;
- **Privacidade e Anonimidade:** As transações são anônimas, com base nos endereços dos usuários. Os servidores armazenam apenas fragmentos criptografados dos dados do usuário;
- **Desintermediação:** A BC consegue eliminar terceiros em suas transações, atuando como um conector de sistemas de forma confiável e segura;
- **Cooperação e incentivos:** Uso do modelo de teoria dos jogos como forma de incentivo.

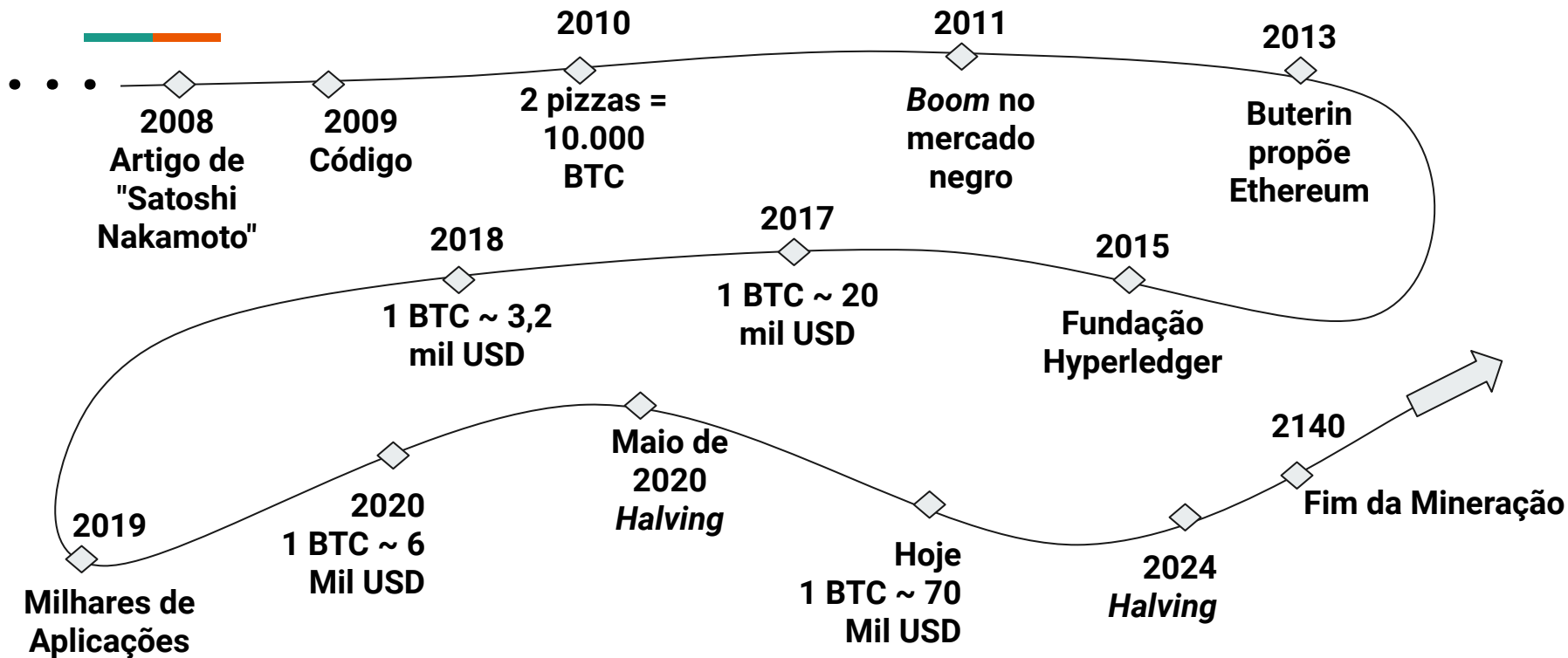


# Benefícios de Blockchain?

Fonte: Greve 2019.

- **Descentralização:** Sistemas e aplicações que usam a BC não precisam de uma entidade central para coordenar as ações, as tarefas são executadas de forma distribuída;
- **Disponibilidade e integridade:** Os dados e as transações são replicados para todos os participantes da BC, mantendo o sistema seguro e consistente;
- **Transparência e auditabilidade:** A cadeia de blocos que registra as transações é pública e pode ser auditada e verificada;
- **Imutabilidade e Irrefutabilidade:** Os registros não são mutáveis e a correção só pode ser feita a partir de novos registros. Causa desconfiança e tráfego garantindo que os lançamentos não podem ser refutados;
- **Privacidade e Anonimidade:** As transações são anônimas, com base nos endereços dos usuários. Os servidores armazenam apenas fragmentos criptografados dos dados do usuário;
- **Desintermediação:** A BC consegue eliminar terceiros em suas transações, atuando como um conector de sistemas de forma confiável e segura;
- **Cooperação e incentivos:** Uso do modelo de teoria dos jogos como forma de incentivo.

# Linha do tempo (incompleta)



\* Valores e datas aproximadas



## Blockchain: pilares

1. **Peer-to-peer**: + disponibilidade e - controle
2. Mecanismos **criptográficos**
  - a. Função *Hash*
  - b. Chaves assimétricas (pública e privada) e assinatura digital
3. Mecanismo de **consenso** distribuído para uma visão consistente do sistema
4. **Software livre** para obter transparência
5. **Incentivos econômicos** para sustentabilidade



## Resumo



3

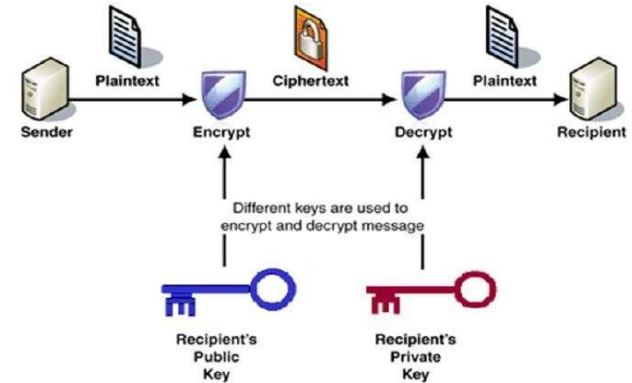


Prof. Arlindo Flavio da Conceição

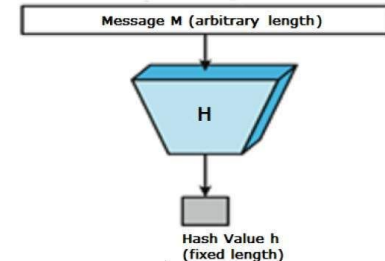
<https://www.youtube.com/watch?v=d13rjDagZ2Y> e  
<https://www.youtube.com/watch?v=prSe7RSRTyA>

# Conceitos básicos para entender Blockchain

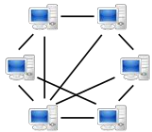
- Chaves criptográficas assimétricas
  - Pares de chaves pública (+) e privada (-)
  - Privacidade, autenticação e assinatura de mensagens



- Funções Hash:
  - $H(x) = y$
  - Dado y, qual o valor de x?
  - Fornece uma "impressão digital" de um conteúdo
  - Exemplos: MD5 and SHA256

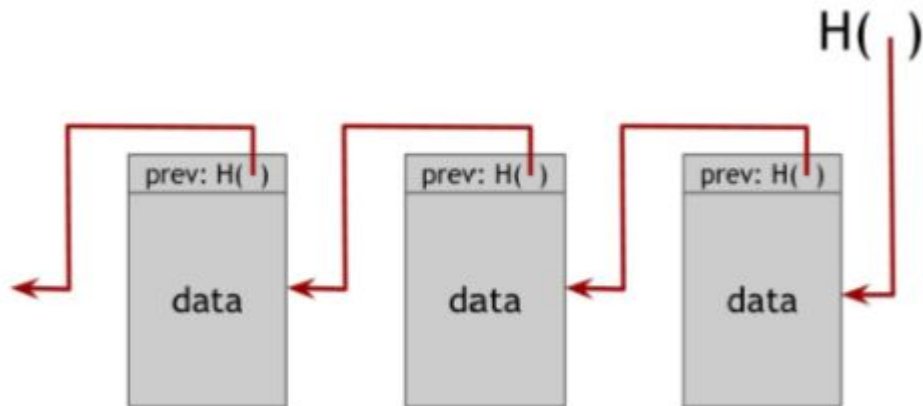


- Protocolos **Peer-to-Peer**: família Torrent
- Algoritmos de eleição e consenso distribuído
- Economia de redes de consenso distribuído



# Estrutura de dados

- Hash e cópias: imutabilidade do dado
- Disponibilidade das cópias
- Pode conter qualquer tipo de Informação, depende da aplicação.
  - Em Bitcoin, são transações
- **Importante:**
  - O que se quer registrar de forma incorruptível?
  - O que é uma transação para a sua aplicação?





## Exemplo Bitcoin...

- Bitcoin é só uma aplicação...
- Bitcoin é só uma aplicação...
- Bitcoin é só uma aplicação...
- Bitcoin é só uma aplicação...
- Bitcoin é só uma aplicação...
- Bitcoin é só uma aplicação...
- Bitcoin é só uma aplicação...
- Bitcoin é só uma aplicação...
- Bitcoin é só uma aplicação...
- É uma boa aplicação, mas é só uma aplicação...

# Rede Bitcoin

- Criado em 2008 por "Satoshi Nakamoto"
- Valor máximo:  
+/- 20K USD
- Valor atual:  
+/- 6K USD
- Excelente leitura:  
<https://bitcoin.org/bitcoin.pdf>

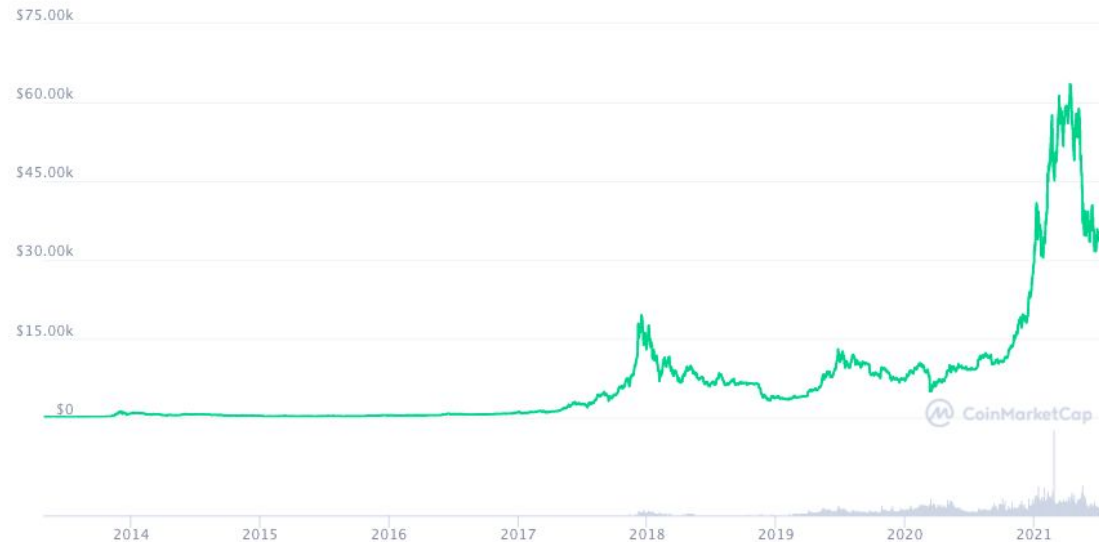
## Bitcoin Charts



Fonte: <https://coinmarketcap.com/currencies/bitcoin/> (Jun 2018)

# Rede Bitcoin

- Criado em 2008 por "Satoshi Nakamoto"
- Valor máximo: +/- 60K USD
- Valor atual: +/- 32K USD
- Excelente leitura: <https://bitcoin.org/bitcoin.pdf>



Fonte: <https://coinmarketcap.com/currencies/bitcoin/> (Jul 2021)

# Rede Bitcoin

- Criado em 2008 por "Satoshi Nakamoto"
- Valor máximo: +/- 60K USD
- Valor atual: +/- 50K USD
- Excelente leitura: <https://bitcoin.org/bitcoin.pdf>



Fonte: <https://coinmarketcap.com/currencies/bitcoin/> (Out 2021)

# Rede Bitcoin

- Criado em 2008 por "Satoshi Nakamoto"
- Valor máximo: +/- 60K USD
- Valor atual: +/- 50K USD
- Excelente leitura: <https://bitcoin.org/bitcoin.pdf>



Fonte: <https://coinmarketcap.com/currencies/bitcoin/> (Out 2023)



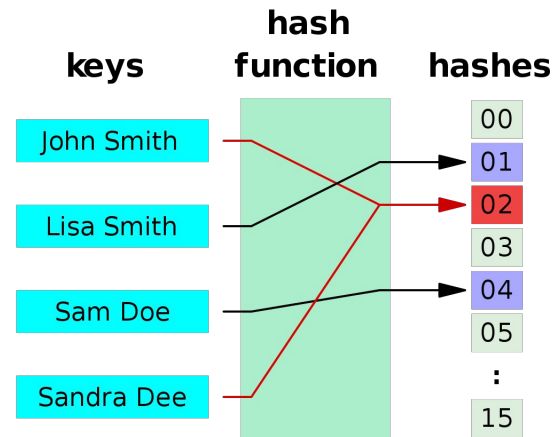
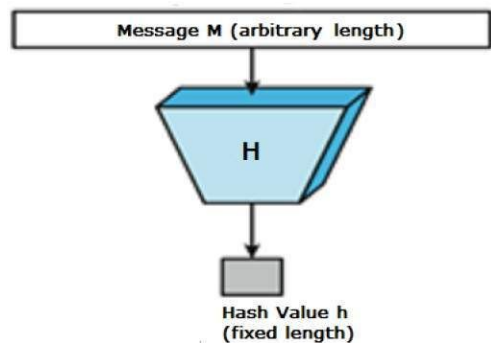


# Controvérsias

- As criptomoedas deveriam ser reguladas por governos?
- Lavagem de dinheiro?
- Esquema de pirâmide?
- Entre outros assuntos controversos...

# Funções de Hash

- Entrada de tamanho arbitrário
- Saída de tamanho fixo
- Saída determinística
- Uniformemente distribuído
- Baixa colisão
- Um único bit altera completamente o resultado
- Não volta



## Funções de Hash: exemplo usando MD5

```
[Arlindos-MacBook-Air:bin arlindo$ cat entrada.txt
-Arlindo Flavio da Conceição

[Arlindos-MacBook-Air:bin arlindo$ md5 entrada.txt
MD5 (entrada.txt) = 4fad2a15e18e64b404401bb541e52400
[Arlindos-MacBook-Air:bin arlindo$ vi entrada.txt
[Arlindos-MacBook-Air:bin arlindo$ cat entrada.txt
-Arlindo Flavio da Conceição.

[Arlindos-MacBook-Air:bin arlindo$ md5 entrada.txt
MD5 (entrada.txt) = b0753fdb4522fad30e511190a9ac6f25
Arlindos-MacBook-Air:bin arlindo$ █
```



## Funções de Hash

- Garante a imutabilidade
- O algoritmo mais usado é o *Secure Hash Algorithm* (SHA), desenvolvido pela National Security Agency (NSA)
- Bitcoin usa SHA-256 (uma variação de SHA-2) para:
  - Criar um endereço a partir da chave pública
  - Prova de trabalho
  - Cadeia de blocos

# Mineração: resolver um problema matemático

## *Encontrar o nonce mantém a rede no ar...*

- Um novo coordenador é eleito aproximadamente a cada 10 minutos
- O coordenador é aquele que primeiro resolve:

$$H(\textit{nonce} \parallel \textit{prev} \parallel \textit{mrkl\_root} \parallel \textit{timestamp} \parallel \textit{target}) < \textit{target}$$

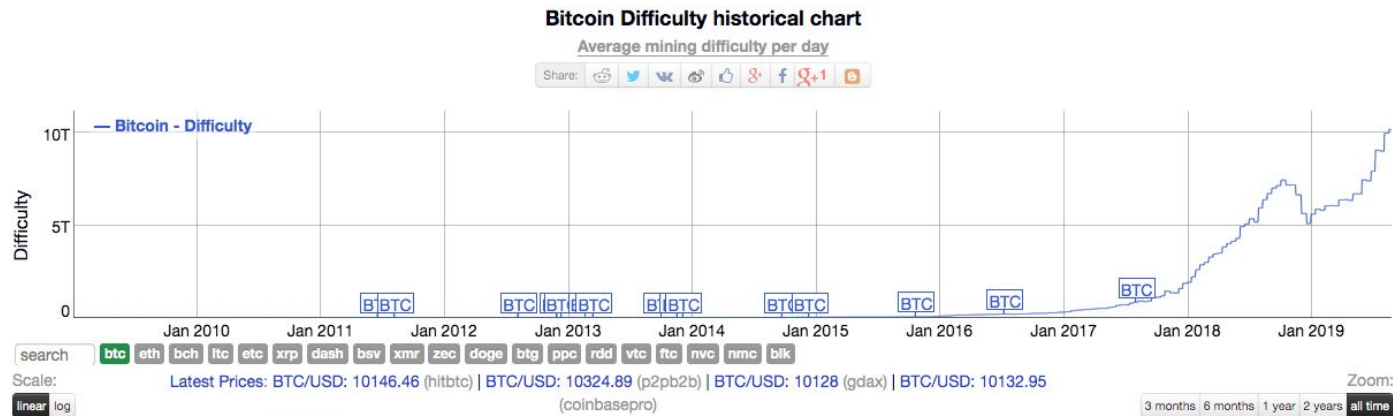
- **target** é uma faixa no espaço de solução:

256 bits

- A cada 2016 blocos, o **target** é ajustado da seguinte forma:  
$$\textit{next\_target} = \textit{previous\_target} * (\textit{tempo para encontrar os últimos 2016 blocks em minutos}) / (2016 * 10)$$
- Evolução: <http://bitcoin.sipa.be/speed-lin-ever.png>



# Dificuldade



<https://bitinfocharts.com/comparison/bitcoin-difficulty.html>



# Halving

- Último em maio de 2020
- <https://www.bitcoinblockhalf.com>



# Criptografia

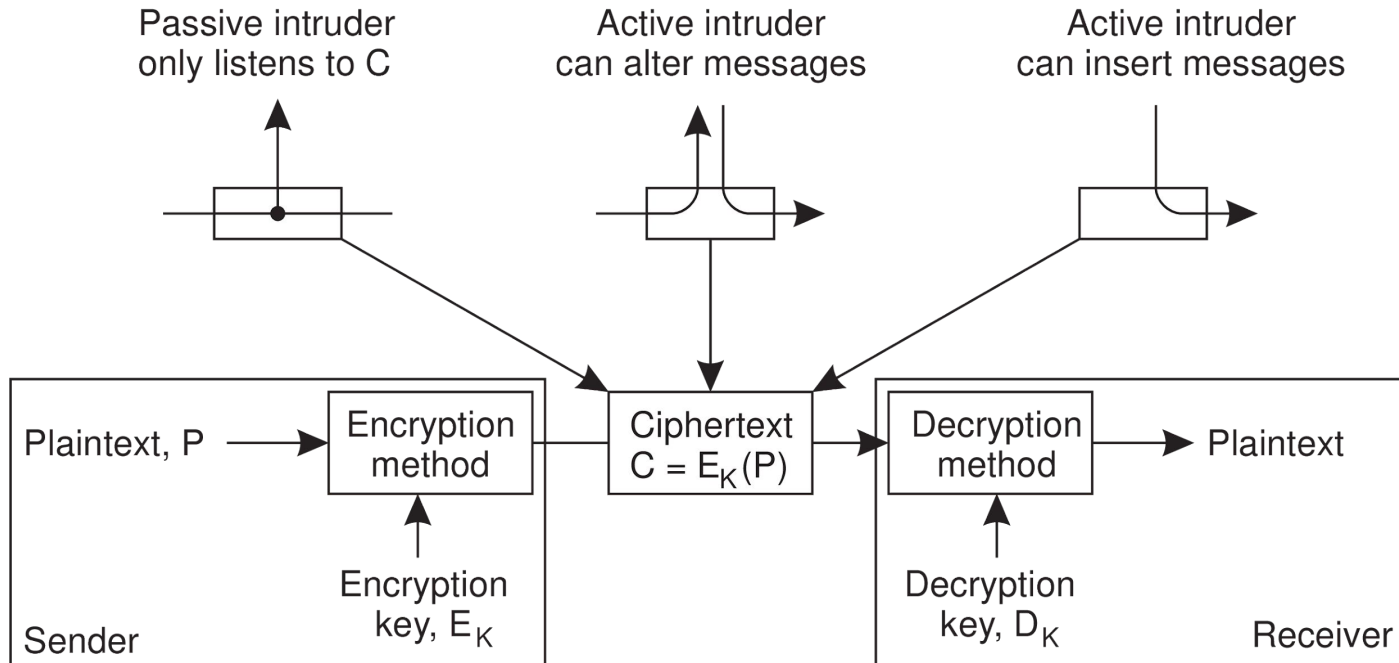




# Criptografia

- Simétrica
  - Mesma chave para codificar e para decodificar
- Assimétrica
  - Chaves diferentes para codificar e para decodificar
  - Pública e Privada
  - Codifica com a pública e decodifica com a privada ou codifica com a privada e decodifica com a pública
- Referência: Tanenbaum e Steen

# Ataques...





## Notação

+ Público

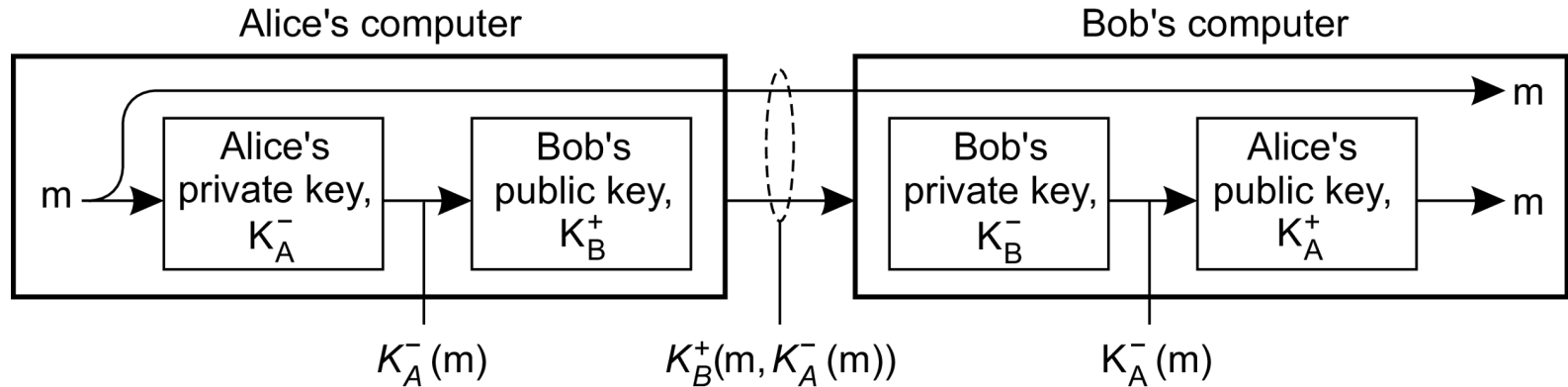
- Privado

ALICE -> Legítimo

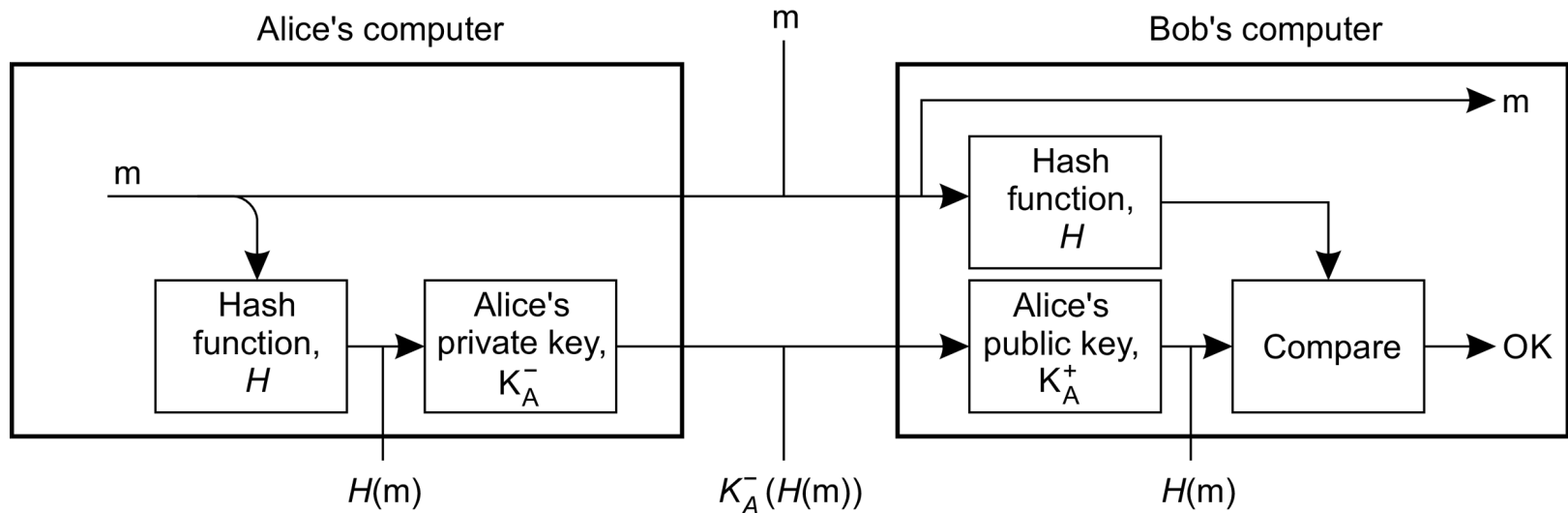
BOB -> Legítimo

TRUDY -> Invasor

# Assinatura de mensagens



## Assinatura de mensagens usando Hash

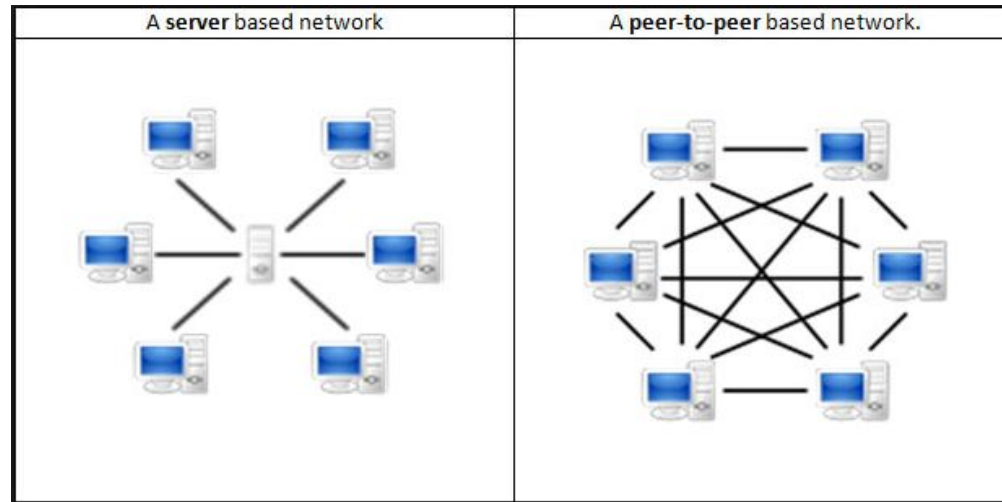




## Exemplo: uso de chaves em Bitcoin

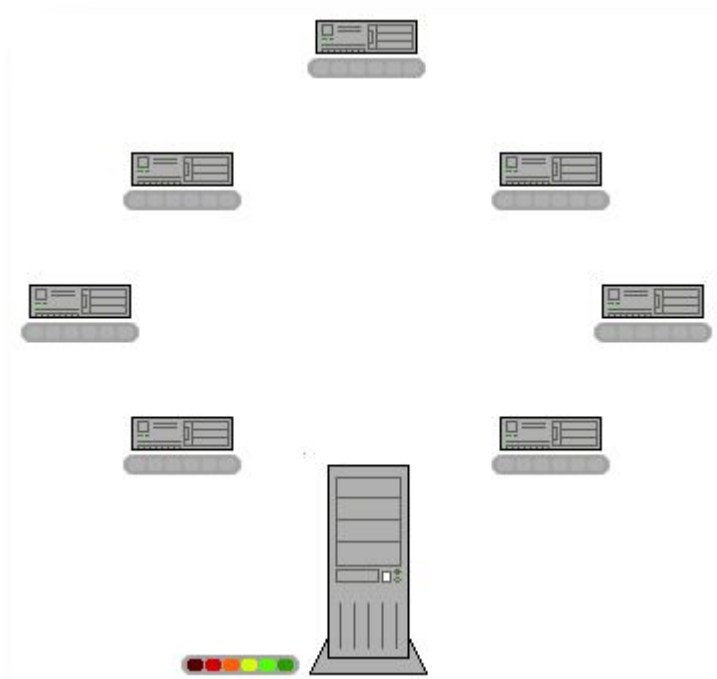
- Identidade do usuário
- Confirmação de autoria de uma mensagem por assinatura
- Transferência de um recurso
  - **Assino com a chave privada da origem e a chave pública do destino**

# Redes ponto-a-ponto ou P2P



# P2P: redução de gargalos!

- Variações do BitTorrent
- Não centralizado
- Redundância
- Disponibilidade
- Escalabilidade (por redução de gargalos)
  - Mais clientes







IPFS

# What's really happening when you add a file to IPFS?

community • Aug 27, 2018

**From raw data to Merkle DAGs and a few steps in between**

- Referência: <https://blog.textile.io/what-s-really-happening-when-you-add-a-file-to-ipfs-/>

# Rede p2p de Bitcoin

- +/- 10K nós

## GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Thu Jun 28 2018  
10:10:57 GMT-0300 (Horário Padrão de Brasília).

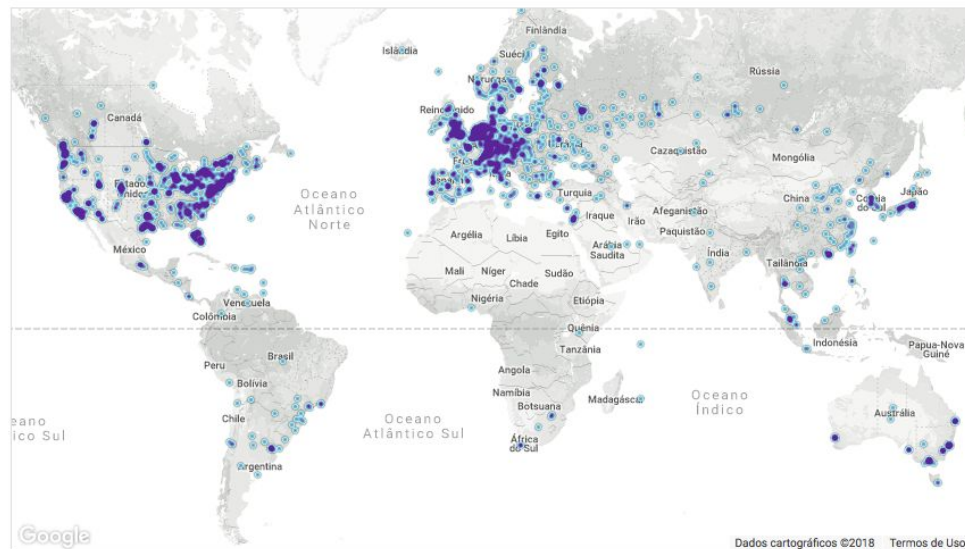
## 9640 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2419 (25.09%)
2	Germany	1775 (18.41%)
3	China	854 (8.86%)
4	France	666 (6.91%)
5	Netherlands	473 (4.91%)
6	Canada	365 (3.79%)
7	United Kingdom	310 (3.22%)
8	Russian Federation	290 (3.01%)
9	Japan	232 (2.41%)
10	Singapore	204 (2.12%)

More (103) »



Source: <https://bitnodes.earn.com> e <https://ethstats.net>

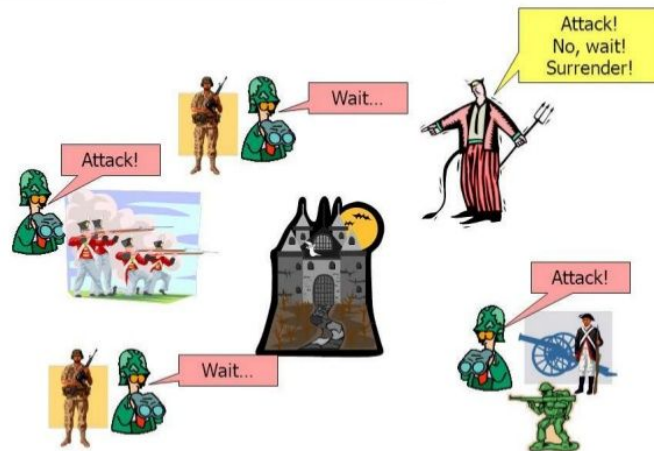
# Consenso distribuído

*Blockchain não é sobre \$\$\$*

- Generais Bizantinos
  - Todos atacam: vitória
  - Todos recuam: sobrevivência
  - Ataque parcial: aniquilação
- Protocolos
  - PoW
  - PoS e outros... Voltaremos a esse ponto.

[Apresentação SBCAS](#)

## Generais bizantinos



# Exemplo de transação em Bitcoin

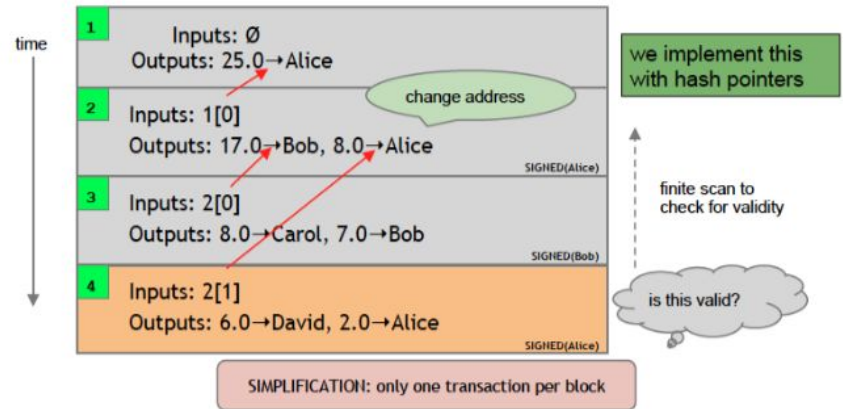
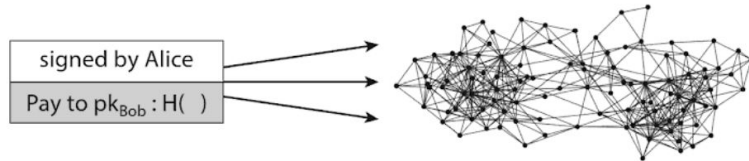
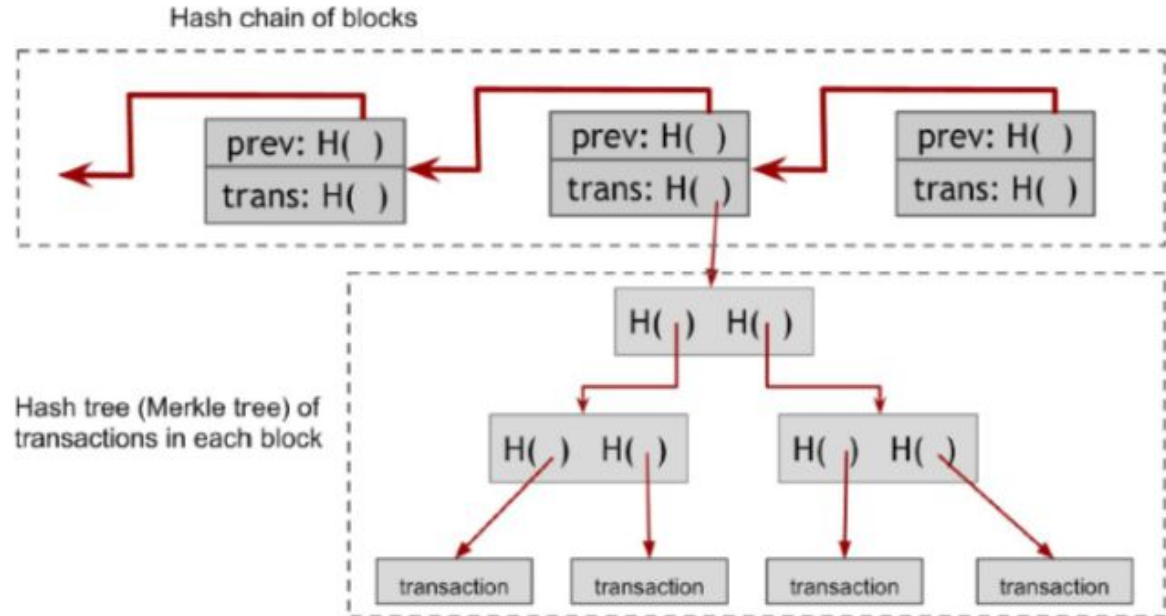


Figure 5.4. Esquema de Conjunto de Transações em Bitcoin (fonte: [Narayanan et al. 2016](#), slides: Montresor (UniTN))

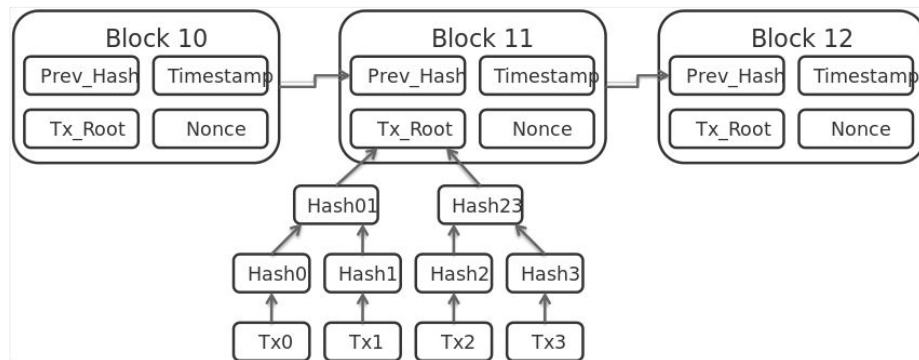
# Árvores de Merkle indexa as transações

- Apenas o *hash* da raiz é gravado no cabeçalho
- Transações são folhas
- Busca em  $O(\lg n)$



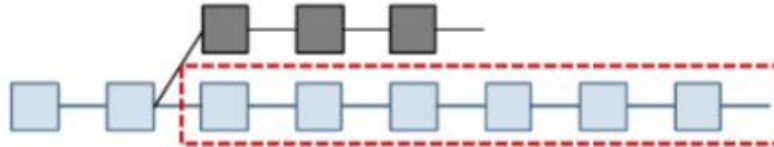
## O campo *nonce* e a eleição distribuída

- Líderes eleitos de maneira pseudo-aleatória são responsáveis por fechar um Novo bloco



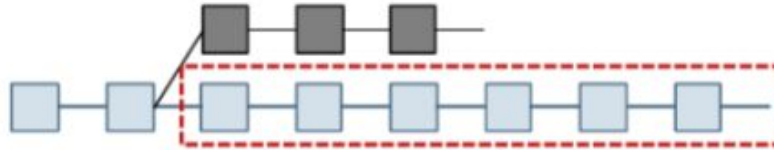
# Forks

- E se dois nós encontram o *nonce* aproximadamente ao mesmo tempo?
- Consistência eventual
- Resolve, de modo probabilístico, o Consenso Bizantino
- Ataques de "51%" consistem em forçar artificialmente a escolha de uma das bifurcações



# Duplo gasto

- Toda transação é validada
- O problema de duplo gasto é resolvido verificando **toda** a cadeia de pagamentos







# Incentivos

- Criar um bloco
  - A cada 210.000 blocos (cerca de 4 anos) esse valor é reduzido pela metade
  - Hoje são 6,25 BTCs
- O conjunto de transferências pode deixar um valor a ser pago para quem criou o bloco
- O número máximo de bitcoins em circulação é limitado.
- **Os incentivos impelem a permanecer honesto.**

# Rede Ethereum

- <https://ethereum.org>
- Público
- ETH
- Contratos inteligentes
- Próximos passos:  
[https://www.youtube.com/channel/UCNOFzGXD\\_C9YMYmnefmPH0g](https://www.youtube.com/channel/UCNOFzGXD_C9YMYmnefmPH0g)













# Criptomoedas

*Apenas uma aplicação!*

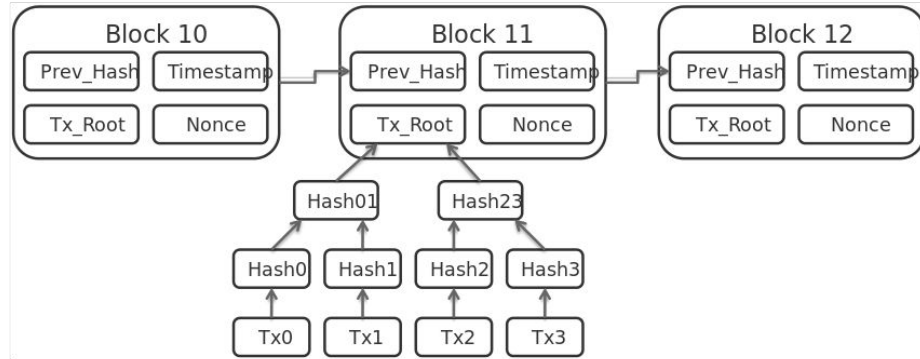
- 1596 exemplos em Junho de 2018
- Atualmente passando por duras perdas

Fonte: <https://coinmarketcap.com>

#	Name	Market Cap	Price
1	 Bitcoin	\$104.002.816.516	\$6.074,90
2	 Ethereum	\$43.569.890.988	\$434,15
3	 Ripple	\$17.941.129.471	\$0,456958
4	 Bitcoin Cash	\$12.016.176.810	\$698,28
5	 EOS	\$6.956.790.585	\$7,76
6	 Litecoin	\$4.477.275.590	\$78,31
7	 Stellar	\$3.520.918.620	\$0,187679
8	 Cardano	\$3.220.505.140	\$0,124214
9	 Tether	\$2.695.935.492	\$0,995861
10	 IOTA	\$2.675.206.173	\$0,962467

# Summary, Blockchain, a decentralized data structure

- Bitcoin example:
  - Each block contains transactions and a hash to the last block
  - Avoid modification?
  - Every +/- 10 minutes a new block is created
  - Leader gains coins
- It is public data
- It is pseudo-anonymous
- Resilient up to "51%" attack
- See data online:  
Blocks: <https://blockexplorer.com/>



- TED Talk about Blockchain: [https://www.youtube.com/watch?v=KP\\_hGPOVLpA](https://www.youtube.com/watch?v=KP_hGPOVLpA) (Recommended) (Merkle Tree)
- Curso para a UFMA: <https://www.youtube.com/watch?v=d13rjDagZ2Y> e <https://www.youtube.com/watch?v=prSe7RSRTyA>