

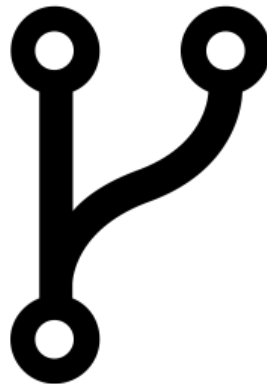
# Blockchain, Criptomoedas & Tecnologias Descentralizadas

## Blockchain sem o hype: Bifurcações (*forks*)

Prof. Dr. Marcos A. Simplicio Jr. – [mjunior@larc.usp.br](mailto:mjunior@larc.usp.br)  
Escola Politécnica, Universidade de São Paulo

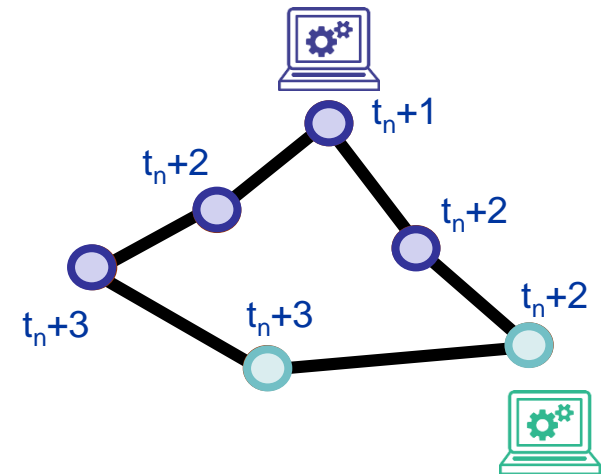
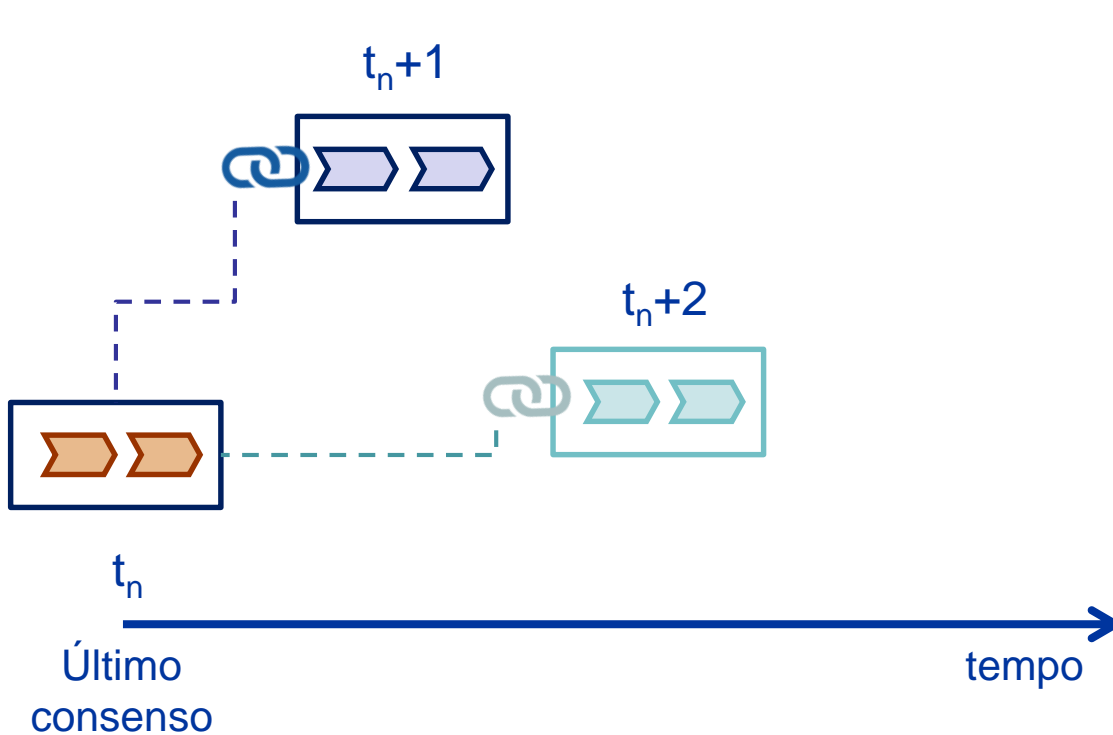
# Objetivos

- Entender como blockchains são atualizados
  - E o que acontece quando nem todos os nós concordam com as atualizações: *soft forks* e *hard forks*



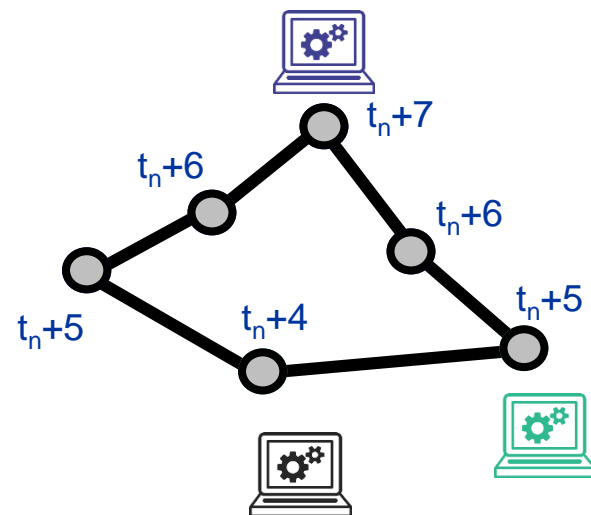
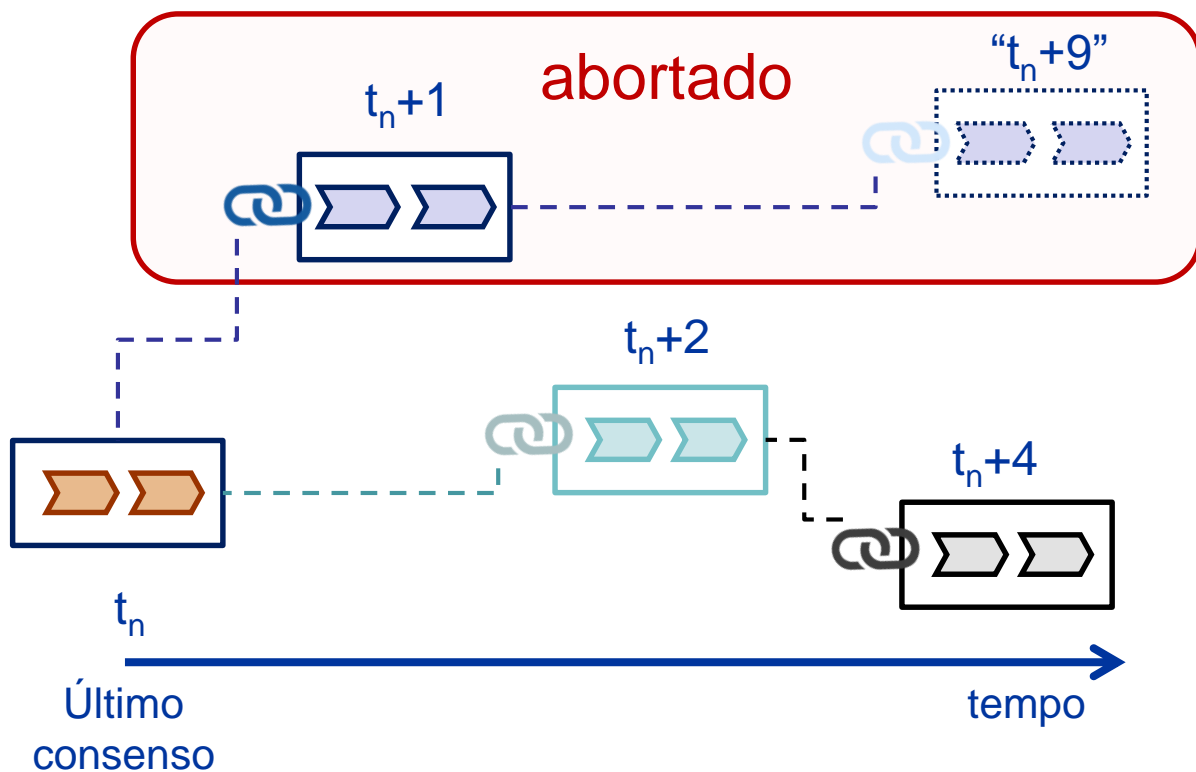
# Relembrando: *forks*

- Bifurcação: situação em que rede não está em consenso:
  - Diferentes visões da realidade: pode ser apenas evento temporário



# Relembrando: *forks*

- Bifurcação: situação em que rede não está em consenso:
  - Diferentes visões da realidade: pode ser apenas evento temporário, desaparecendo à medida que consenso é atingido






# Atualizações: mudando regras

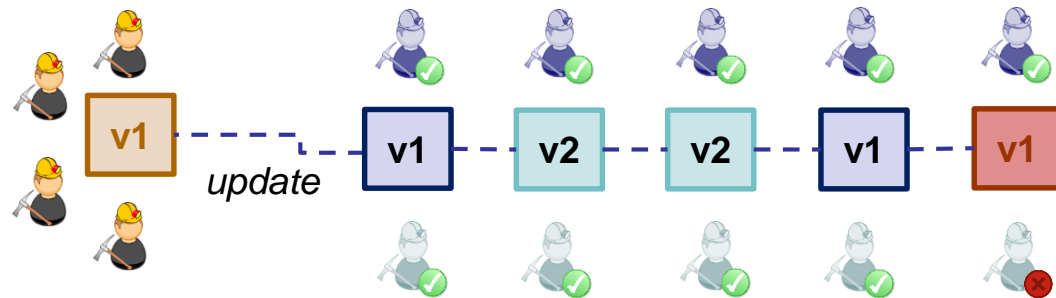
- Governança: mudanças necessárias para fins de
  - **Desempenho**: tamanho máx. bloco, mecanismo de consenso, ...
  - **Segurança**: correção de bugs, algoritmos criptográficos, lista de nós em federação (blockchain consorciado), ...
  - **Funcionalidade**: novos tipos de operação (e.g., suporte a NFTs, ou contratos inteligentes), ...
- Gestão da rede é distribuída: atualização requer que nós atualizem software
  - E nem todos os nós podem concordar com a mudança...
  - Bifurcações (“soft forks” e “hard forks”)



# Soft e Hard forks




- Causados por atualização nas regras do blockchain
- Em suma, termos tentam capturar 2 aspectos:
  1. **Retro-compatibilidade:** nós que se atualizam conseguem entender nós que (ainda) não o tenham feito?

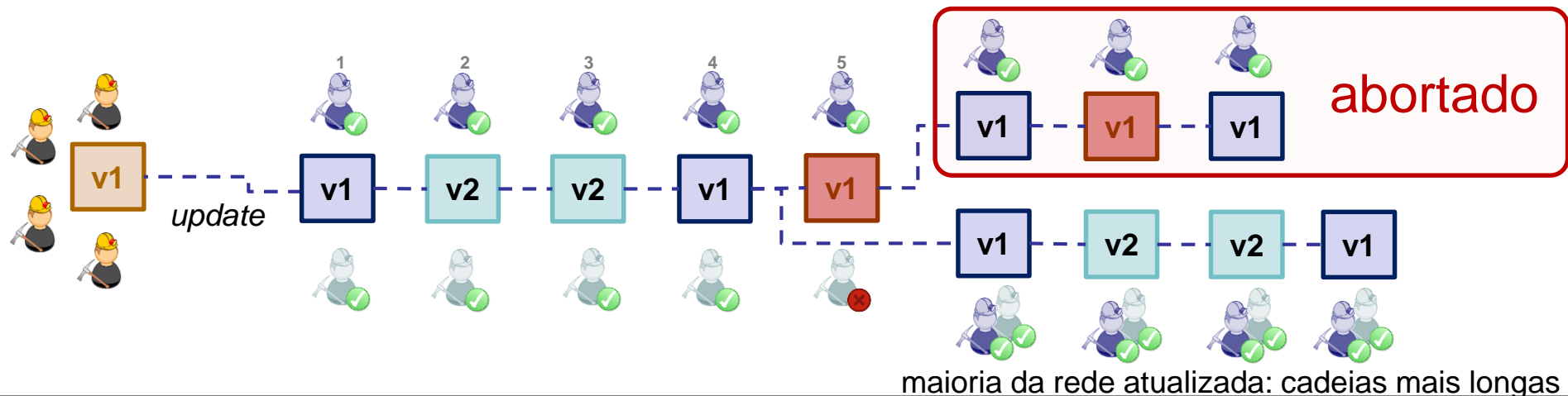
- v1** Blocos na v1, com regras compatíveis com v2, gerados por nós desatualizados 
- v1** Blocos na v1, com regras que violam v2, gerados por nós desatualizados 
- v2** Blocos na v2, gerados por nós atualizados 



# Soft e Hard forks

- Causados por atualização nas regras do blockchain
- Em suma, termos tentam capturar 2 aspectos:
  1. **Retro-compatibilidade:** nós que se atualizam conseguem entender nós que (ainda) não o tenham feito?

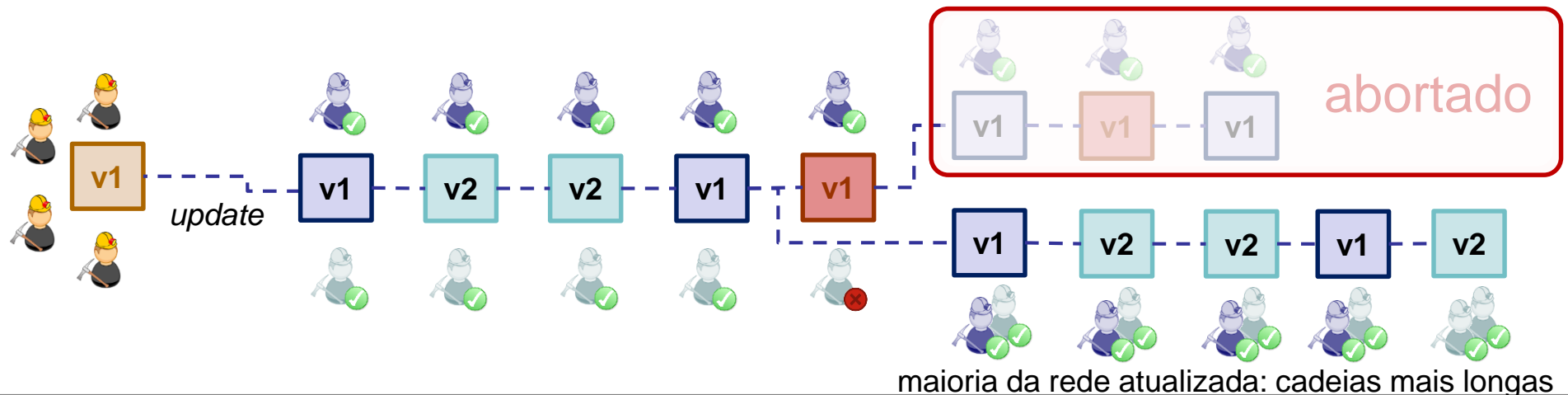
- v1** Blocos na v1, com regras compatíveis com v2, gerados por nós desatualizados 
- v1** Blocos na v1, com regras que violam v2, gerados por nós desatualizados 
- v2** Blocos na v2, gerados por nós atualizados 



# Soft e Hard forks

- Causados por atualização nas regras do blockchain
- Em suma, termos tentam capturar 2 aspectos:
  1. **Retro-compatibilidade:** nós que se atualizam conseguem entender nós que (ainda) não o tenham feito?

- v1** Blocos na v1, com regras compatíveis com v2, gerados por nós desatualizados
- v1** Blocos na v1, com regras que violam v2, gerados por nós desatualizados
- v2** Blocos na v2, gerados por nós atualizados

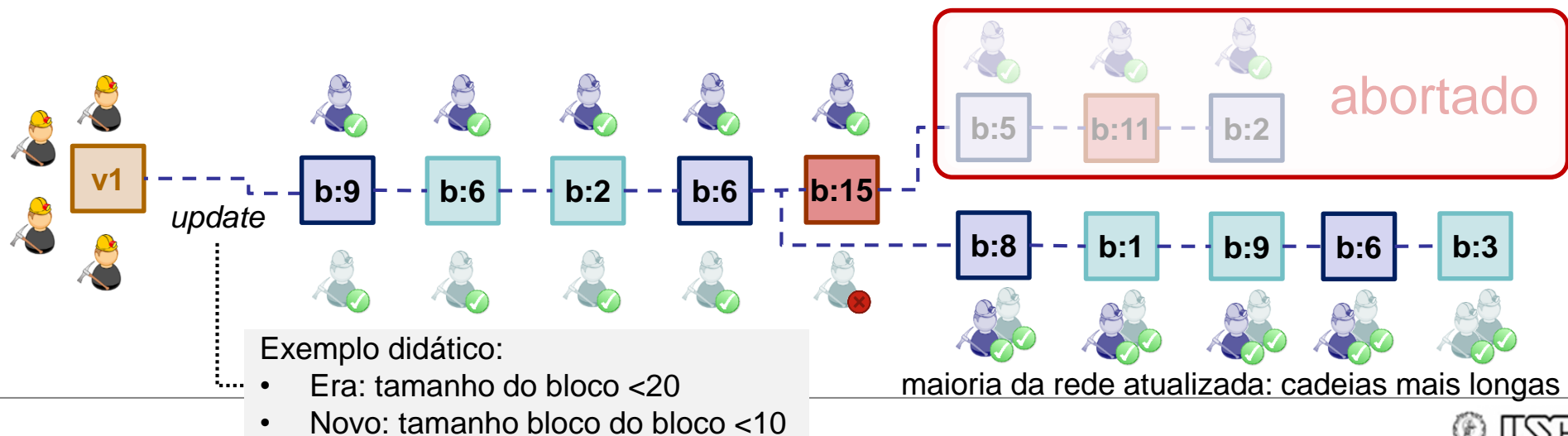




# Soft e Hard forks

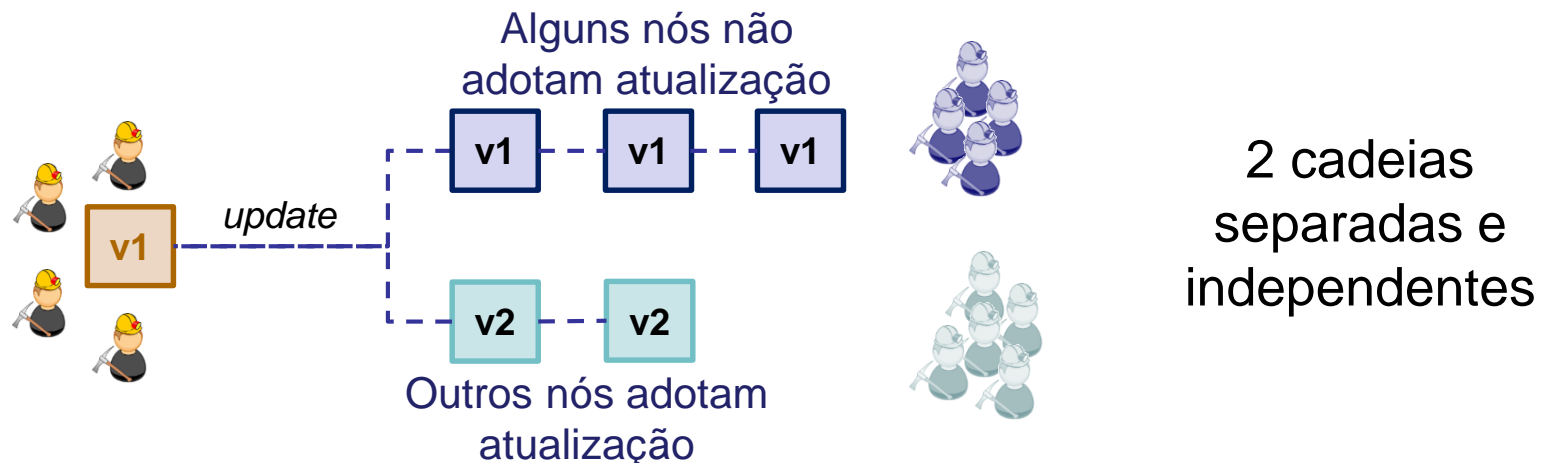
- Causados por atualização nas regras do blockchain
- Em suma, termos tentam capturar 2 aspectos:
  1. **Retro-compatibilidade:** nós que se atualizam conseguem entender nós que (ainda) não o tenham feito?

- b<10** Blocos na v1, com regras compatíveis com v2, gerados por nós desatualizados
- 10<b<20** Blocos na v1, com regras que violam v2, gerados por nós desatualizados
- b<10** Blocos na v2, gerados por nós atualizados

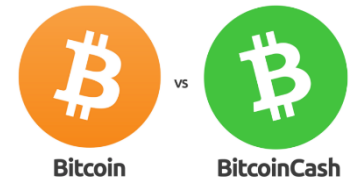


# Soft e Hard forks

- Causados por atualização nas regras do blockchain
- Em suma, termos tentam capturar 2 aspectos:
  1. **Retro-compatibilidade:** nós que se atualizam conseguem entender nós que (ainda) não o tenham feito?
  2. **Adoção:** todos os nós da rede adotam atualização, ou rede “desatualizada” continua operando separadamente?
    - Registros pré fork (ex.: moedas) são “duplicados”



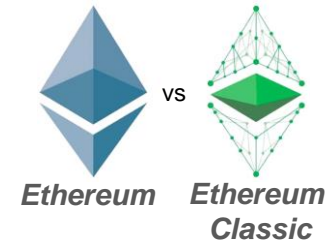
# Soft e Hard forks: exemplos



- Bitcoin original: blocos limitados a 1MiB
  - 1 bloco a cada 10 minutos => ~7 transações/s
  - Queda de desempenho (formação de filas) e aumento de taxas com o “boom de criptomoedas” em ~2015
- Propostas:
  - Segregated Witness (segwit): move assinaturas de transações p/ região separada do bloco (não conta no limite de 1 MiB)
    - Redução de ~50% no tamanho do bloco: ~14 transações/s
    - Também evita manipulações maliciosas ID das transações: hash do conteúdo, sem incluir assinaturas ECDSA (maleáveis)
  - Aumentar tamanho limite dos blocos para 8 – 32 MiB
    - Mais transações suportadas por bloco: cerca de 50 a 200 transações/s
- Fork em 2017: duplicação de moedas
  - Saldo no Bitcoin = saldo no Bitcoin Cash.



# Soft e Hard forks: exemplos



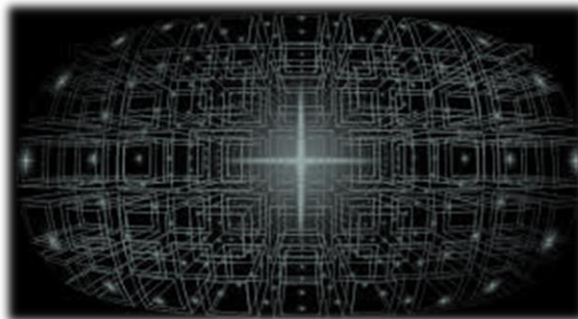
- Ethereum: o “Incidente DAO” (2016)
  - DAO: decentralized autonomous organization
    - “Crowdfunding sobre blockchain”: investidores compram tokens DAO, e votam na alocação de recursos para projetos de seu interesse
    - Lucros divididos entre stakeholders
  - Após lançamento: U\$150M em Ethers angariados...
    - ... mas contrato tinha um bug: U\$50M roubados...
- Propostas:
  - Não aceitar transações com fundos vindos do roubo (“soft”)
  - Nada: “imutabilidade”
  - “Desfazer roubo”: transações do contrato pós-roubo desfeitas
    - Fundos movidos para novo contrato, para saque por investidores
    - Votação censitária: 87% favoráveis ao “desfazer”
      - Apenas 5.5% de participação, 1/4 dos quais de 1 só endereço



Ethereum  
Classic



Ethereum



# Blockchain, Criptomoedas & Tecnologias Descentralizadas

## Blockchain sem o hype: Bifurcações (*forks*)

Prof. Dr. Marcos A. Simplicio Jr. – [mjunior@larc.usp.br](mailto:mjunior@larc.usp.br)  
Escola Politécnica, Universidade de São Paulo

# Referências

- A. Antonopoulos, G. Wood (2018): "Ethereum timeline". In Mastering Ethereum: Building Smart Contracts and DApps, page 329. O'Reilly Media; 424 pages. ISBN 9781491971918
- P. Vigna (2017). "Bitcoin Cash, Litecoin, Ether, Oh My! What's With All the Bitcoin Clones?". The Wall Street Journal, Dec 2017. URL: <https://www.wsj.com/articles/bitcoin-cash-litecoin-ether-oh-my-whats-with-all-the-bitcoin-clones-1514037600>
- J. Frankenfield, S. Anderson (2022). Segregated Witness (SegWit). Investopedia, Jan/2022. URL: <https://www.investopedia.com/terms/s/segwit-segregated-witness.asp>
- J. Frankenfield, E. Rasure, A. Courage (2022). Bitcoin Cash. Investopedia, Jul/2021. URL: <https://www.investopedia.com/terms/b/bitcoin-cash.asp>
- Cryptopedia Staff (2022). "What Was The DAO?". Cryptopedia, Mar/2022. URL: <https://www.gemini.com/cryptopedia/the-dao-hack-makerdao>