Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

Como funcionam blockchains

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

Objetivos

- Entender as engrenagens principais que compõem um Blockchain
  - Necessário para entender o que um blockchain (não) é capaz de fazer
  - Sem entrar em soluções específicas
- Entender a (grande!) utilidade de blockchains em cenários envolvendo troca de ativos digitais em ambiente distribuído
  - Para fins de contexto, vamos falar um pouco do funcionamento do Bitcoin como “caso base”

Bitcoin

- Para entender o funcionamento do blockchain, é interessante analisá-lo no contexto de troca de ativos
  - Afinal, essa é uma de suas principais aplicações!
  - Ex.: **Bitcoin**, Ethereum, Ripple, Algorand, Solana, ...
- O que é o Bitcoin:

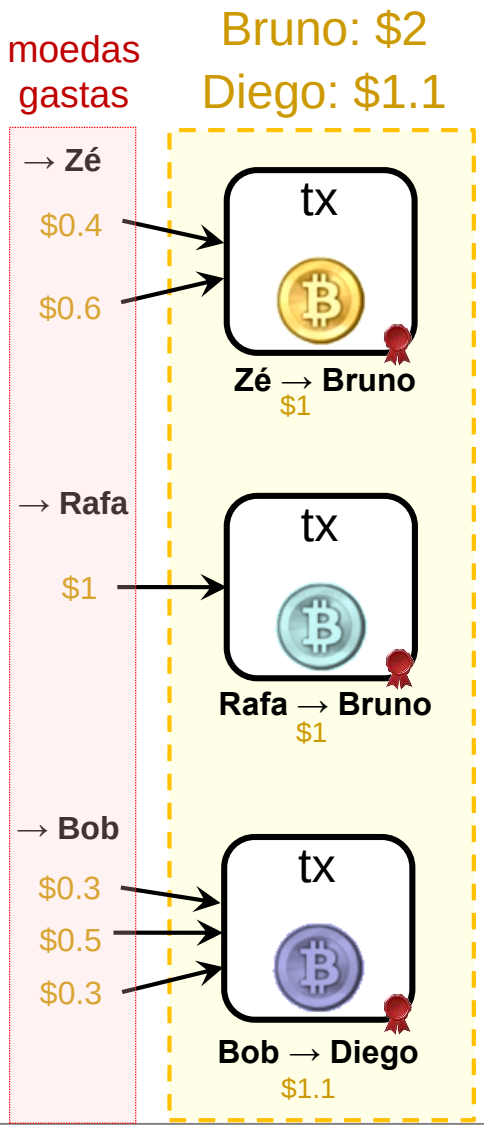
  - Livro de contabilidade (***ledger***) digital: permite verificar saldos ao analisar a **ordem de eventos** no sistema
    - **Evento** = **transação monetária** assinada por usuário
  - Permite transações **sem intermediários**: **descentralização**
    - Embora **plataformas de gerenciamento** (“Exchanges”) possam atuar como intermediários, facilitando acesso por usuários
  - **Previne fraudes**, como duplicação de moedas: embora usuários **não sejam confiáveis**

Bitcoin (cont.)

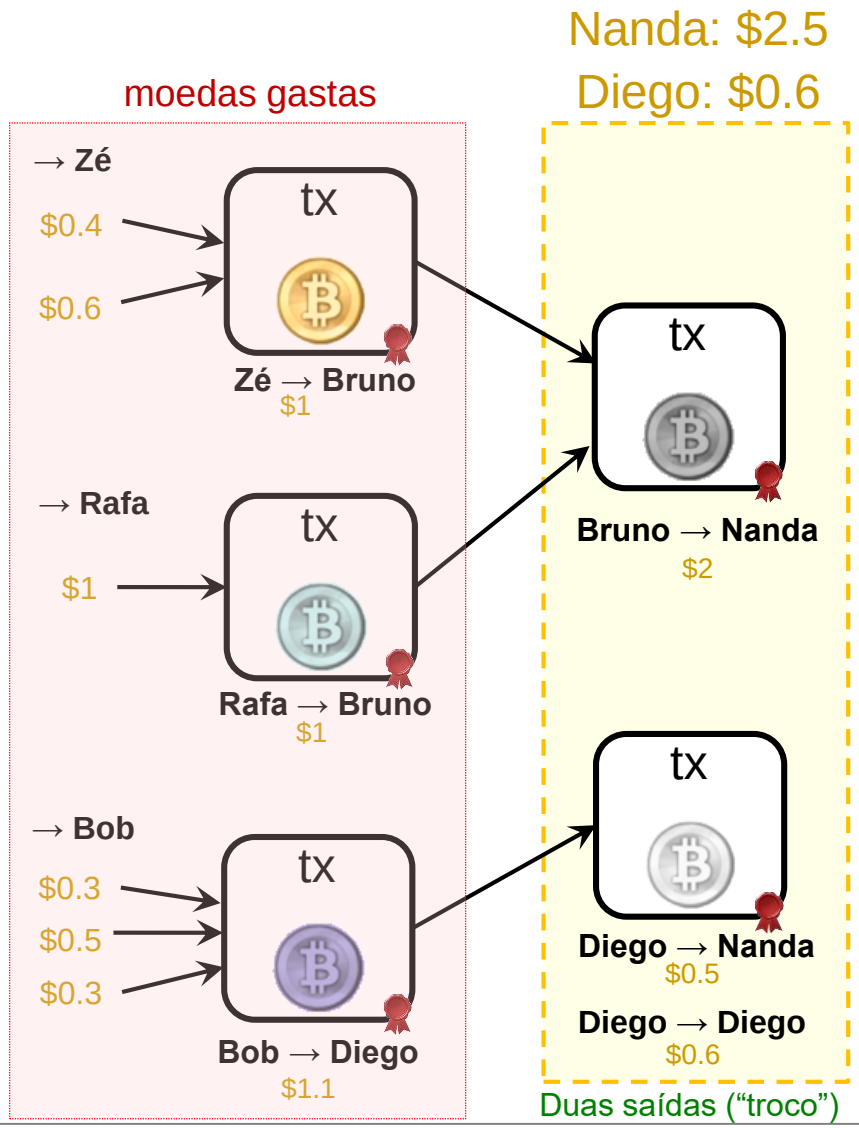
- Para entender o funcionamento do blockchain, é interessante analisá-lo no contexto de troca de ativos
  - Afinal, essa é uma de suas principais aplicações!
  - Ex.: **Bitcoin**, Ethereum, Ripple, Algorand, Solana, ...
- O que é o Bitcoin:

  - Há **incentivos** para participação: *mineração* de moedas e *taxas* pagas pelas transações
  - Permite **pseudoanonimato**: usuários são representados por suas chaves públicas (pseudônimos)
    - Chaves públicas são sequência de bits sem qualquer relação óbvia com a identidade de seus donos!
  - Uso de diferentes chaves permite algum grau de privacidade
    - Embora existam várias técnicas para ligar um usuário a suas transações (e.g., análise estatística, rastreamento de IPs, etc.)

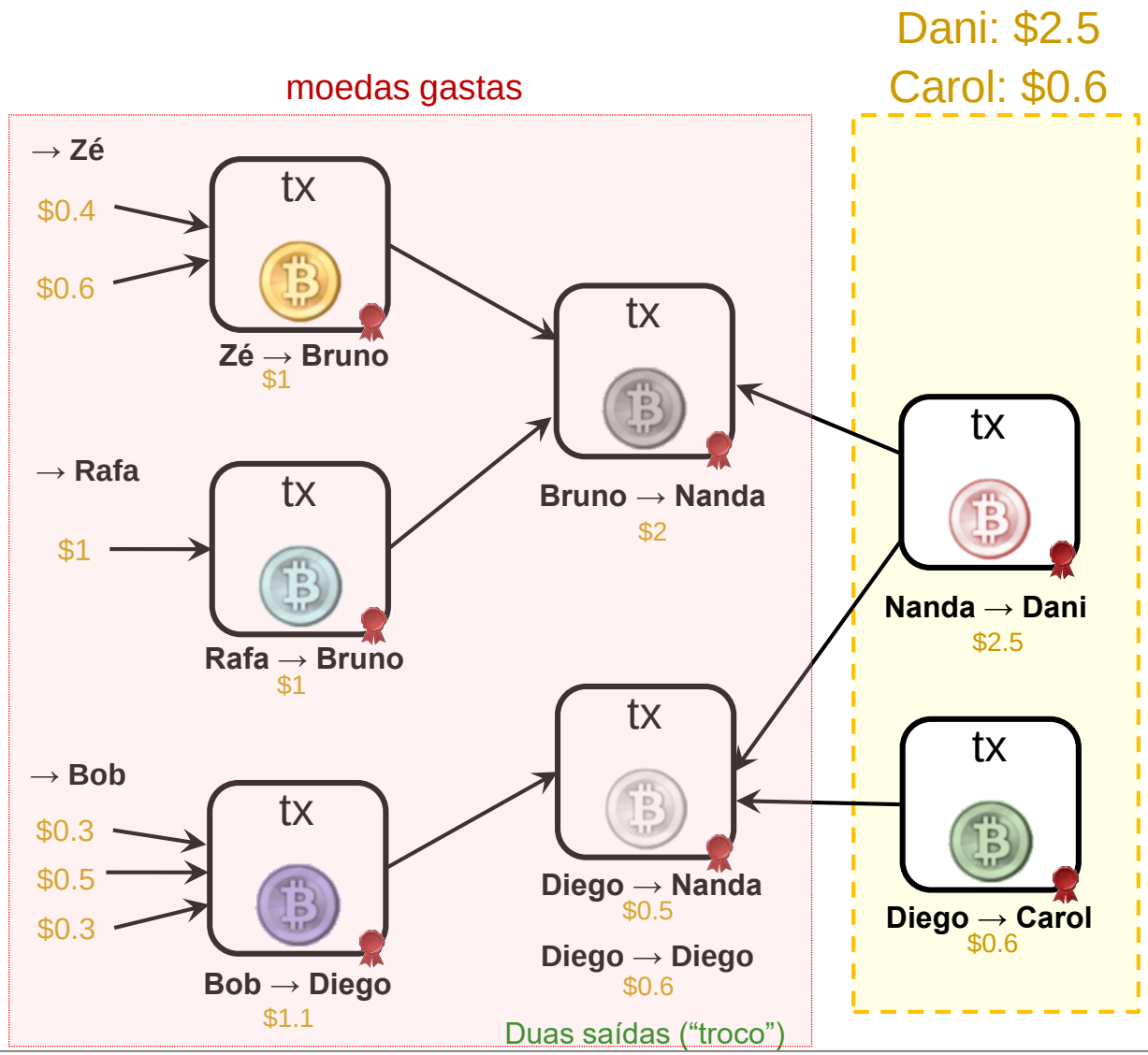
Bitcoin: transações (tx)



Bitcoin: transações (tx)

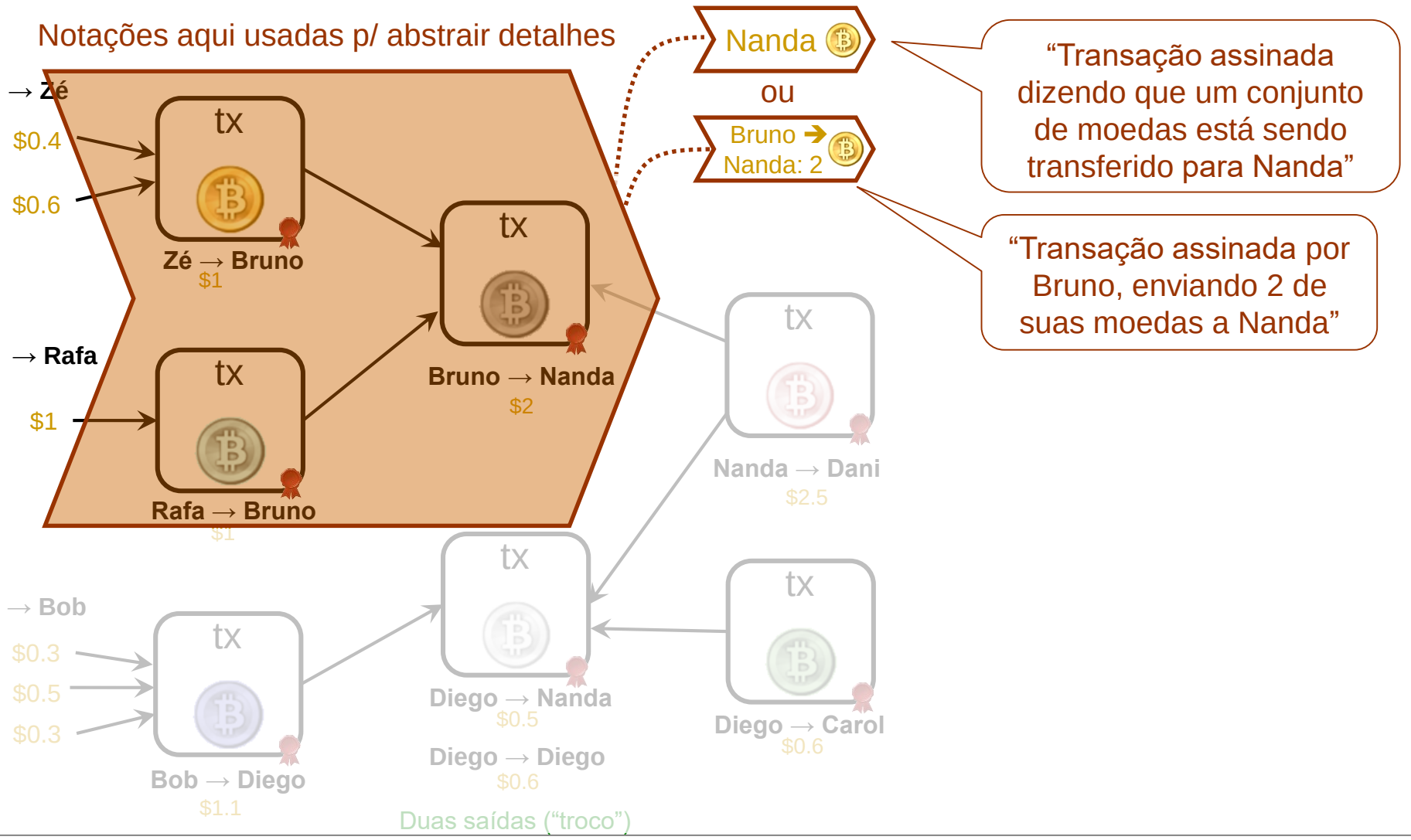


Bitcoin: transações (tx)



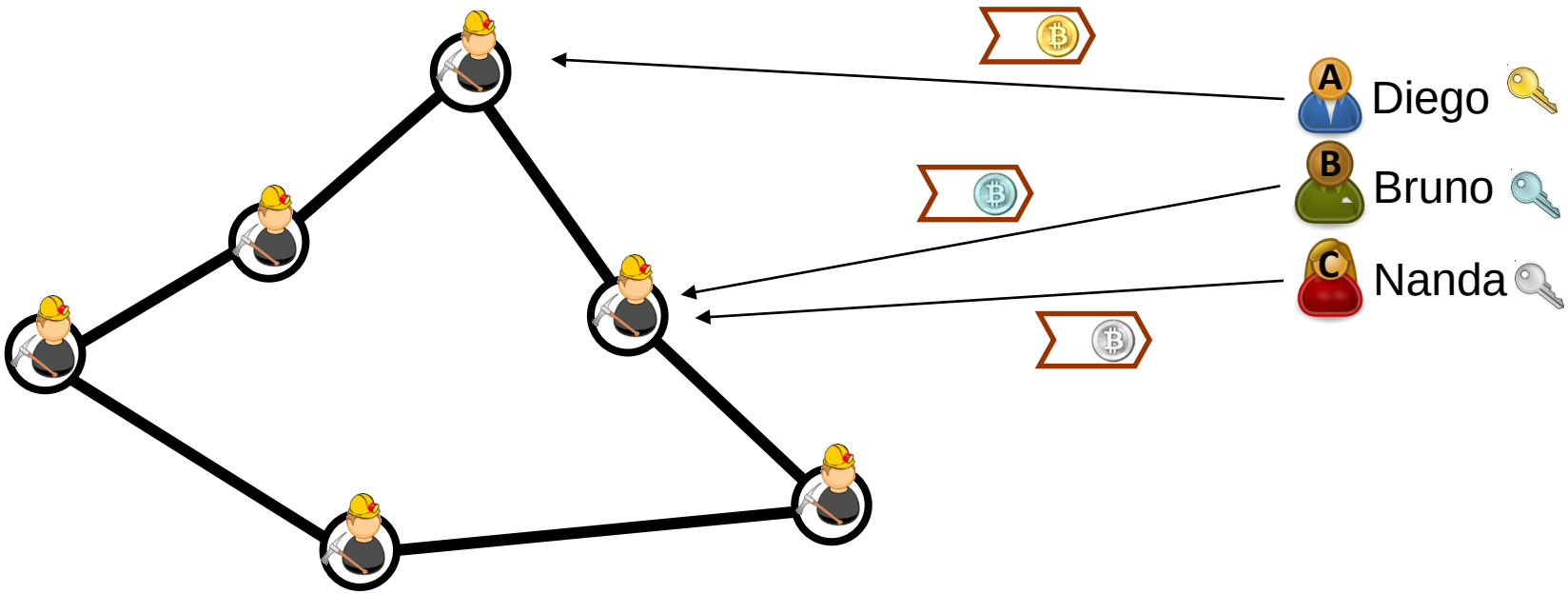
- **Início:** verificar saldos (e integridade) do blockchain do Bitcoin requer **validar todas** as transações registradas, desde a 1ª (“bloco gênesis”)
- **Depois**: basta manter base de dados com **moedas não gastas**

Bitcoin: transações (tx)



Bitcoin: visão geral da rede

- **Rede P2P aberta** à participação. Papéis principais:
  - **Usuários finais**: enviam transações assinadas para a rede
  - **Nós mineradores**: armazenam e validam transações
    - Recebem moedas pela sua participação (discussão mais adiante)

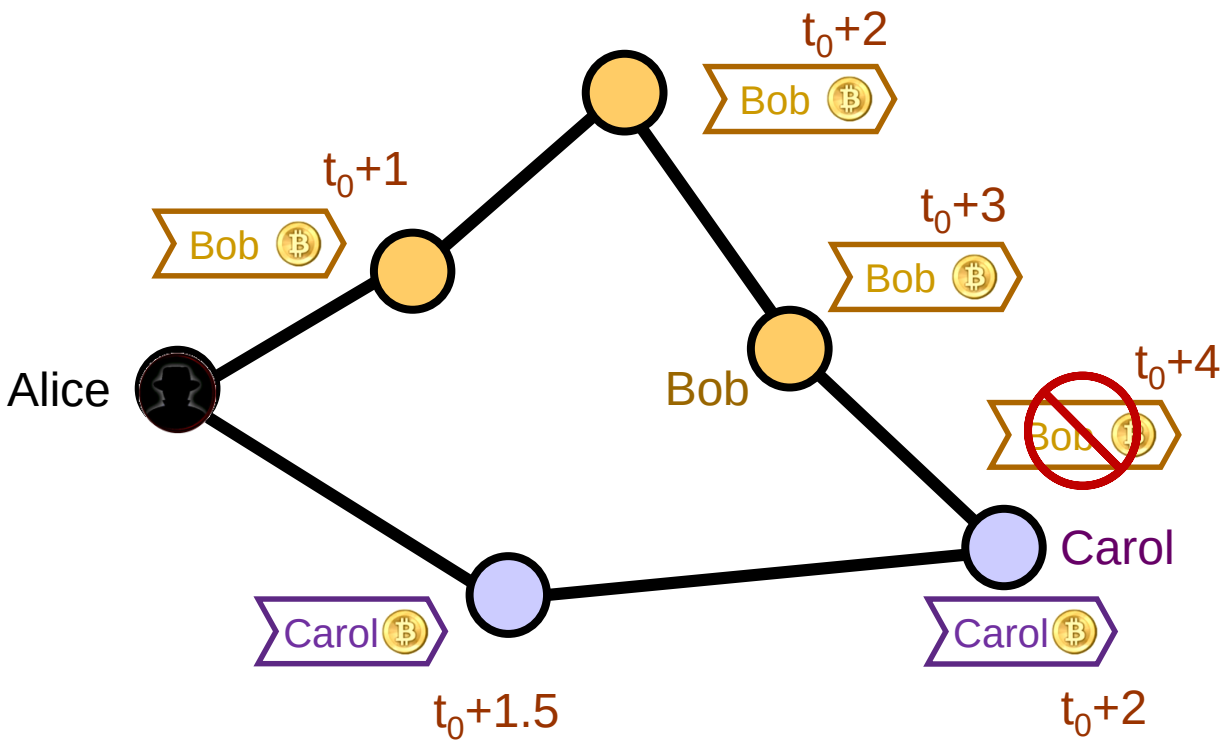


Rede P2P de nós mineradores

Usuários finais

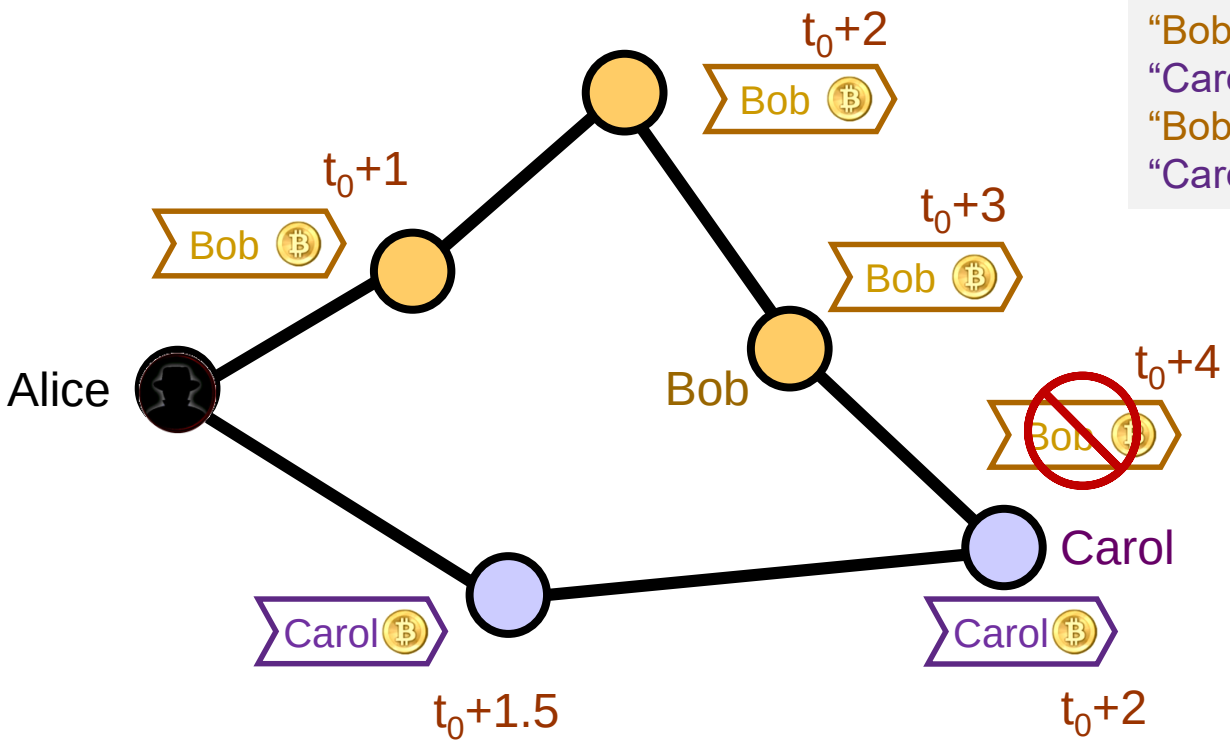
Bitcoin: por que blockchain?

- **Problema alvo:** *Double spending* (ou “gasto duplo”)
  - Pergunta: Bob ou Carol é @ nov@ don@ da moeda?



Bitcoin: por que blockchain?

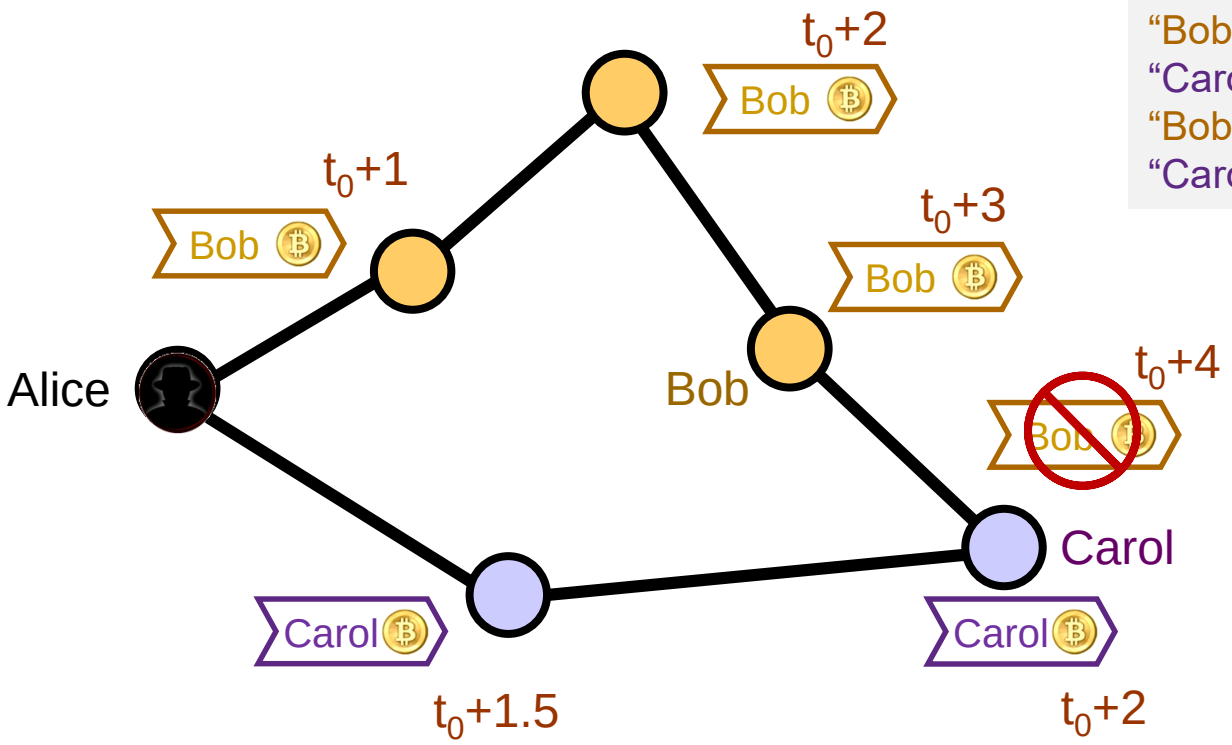
- **Problema alvo:** *Double spending* (ou “gasto duplo”)
  - Pergunta: Bob ou Carol é @ nov@ don@ da moeda?



“Bob: transação foi gerada primeiro”
“Carol: ela recebeu moeda antes”
“Bob: maioria da rede”
“Carol: mais próxima de Alice na rede”

Bitcoin: por que blockchain?

- **Problema alvo:** *Double spending* (ou “gasto duplo”)
  - Pergunta: Bob ou Carol é @ nov@ don@ da moeda?

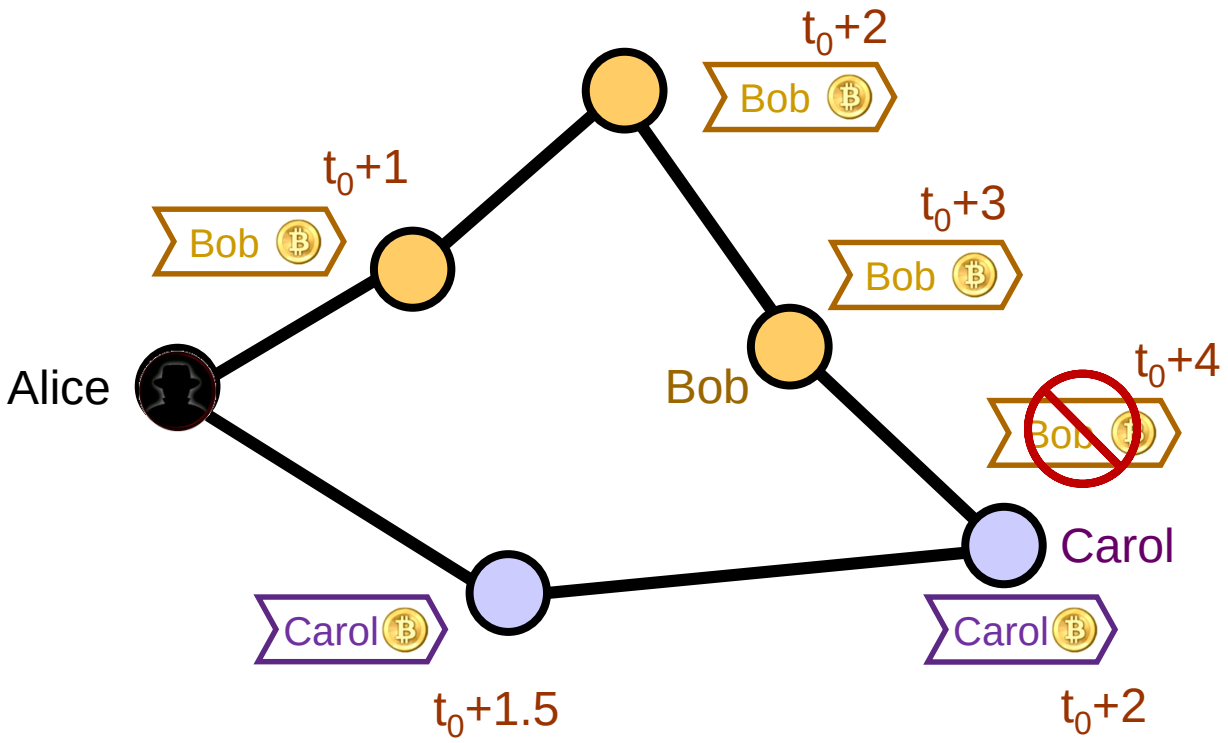


“Bob: transação foi gerada primeiro”
“Carol: ela recebeu moeda antes”
“Bob: maioria da rede”
“Carol: mais próxima de Alice na rede”

Nós não têm visão global da rede em sistemas descentralizados!

Bitcoin: por que blockchain?

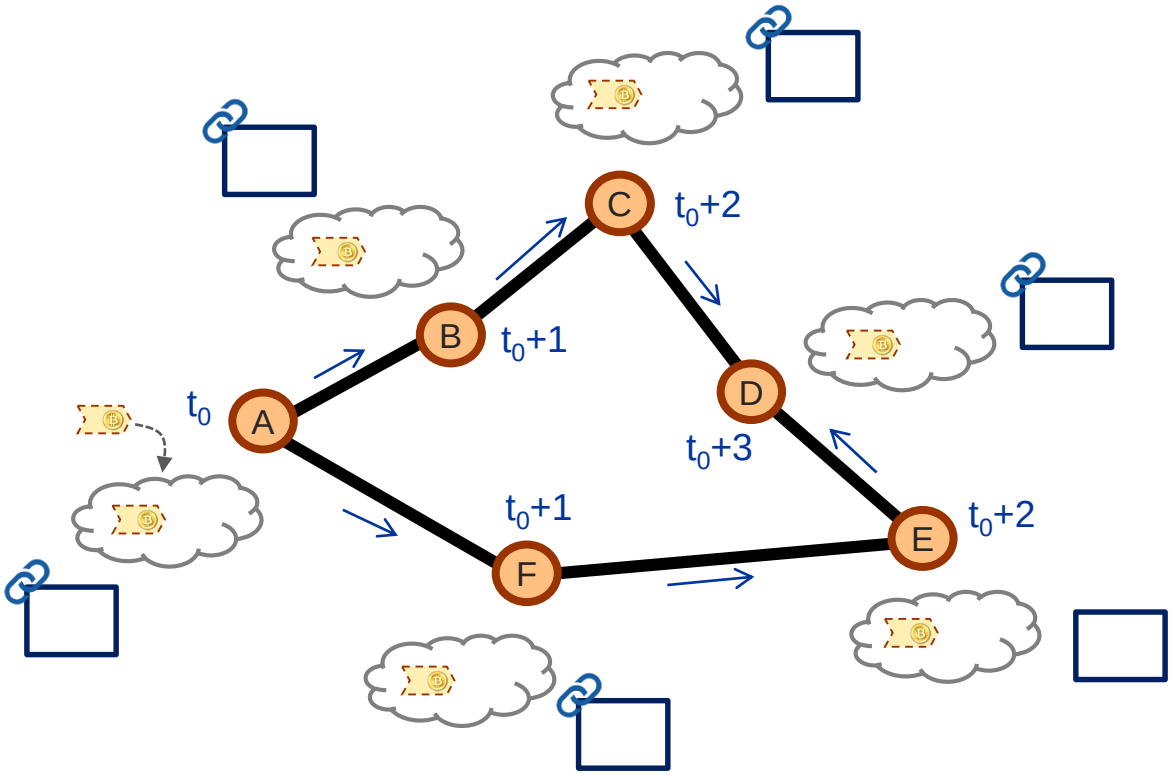
- **Problema alvo:** *Double spending* (ou “gasto duplo”)
  - Rede deve entrar em acordo sobre **ordem de eventos**: só a “1ª transação” é válida, pois a “2ª transação” não tem fundos!
  - Apenas após **consenso**, Carol/Bob entrega produto a Alice



Conflito: Bob ou Carol é @ nov@ don@ da moeda?

Blockchain: processando eventos

- Eventos processados em **duas fases**:
  - **Fase 1**: nós informam sobre evento (broadcast via **gossip**)
  - Nós receptores adicionam evento a sua lista de não validados



Início dos tempos: nenhum evento (validado ou não)

Com broadcast: nós vão descobrindo eventos a serem validados

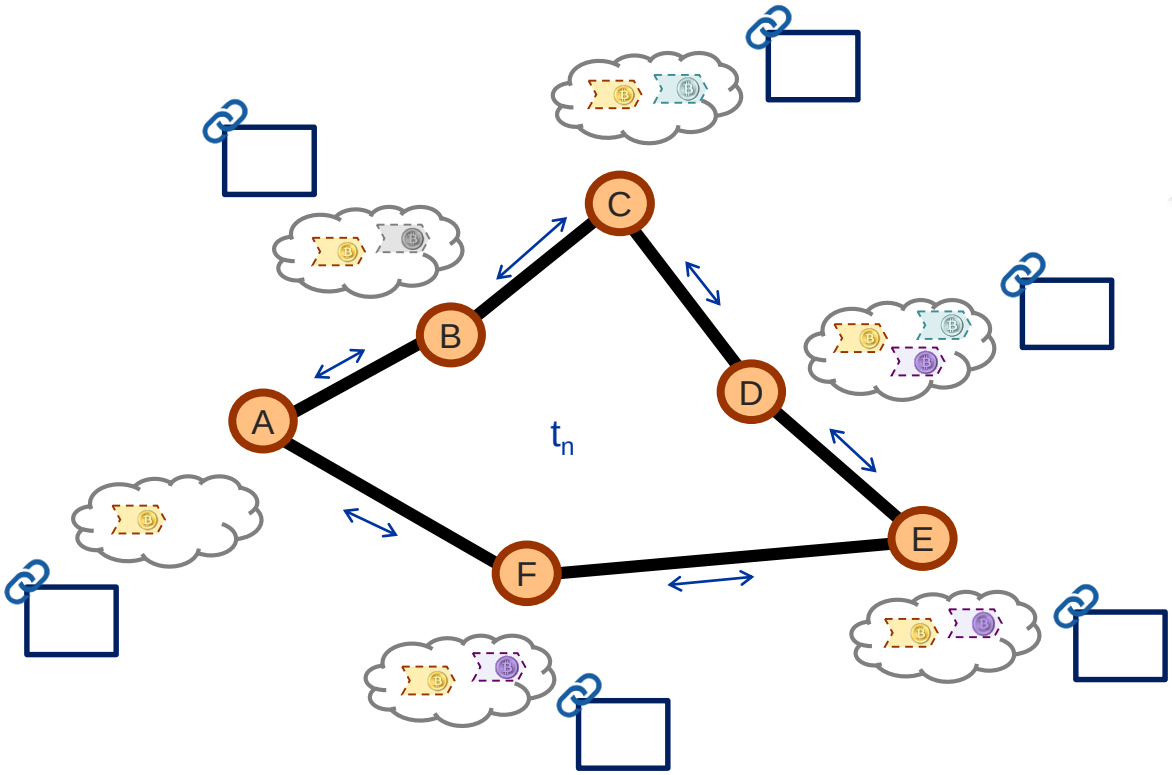
Legenda

Transações ainda não validadas (“*mempool*”)

Transações já validadas (blockchain)

Blockchain: processando eventos

- Eventos processados em **duas fases**:
  - **Fase 1**: nós informam sobre evento (broadcast via **gossip**)
  - Nós receptores adicionam evento a sua lista de não validados



Processo assíncrono e não coordenado: listas podem ter conteúdos diferentes a cada instante!

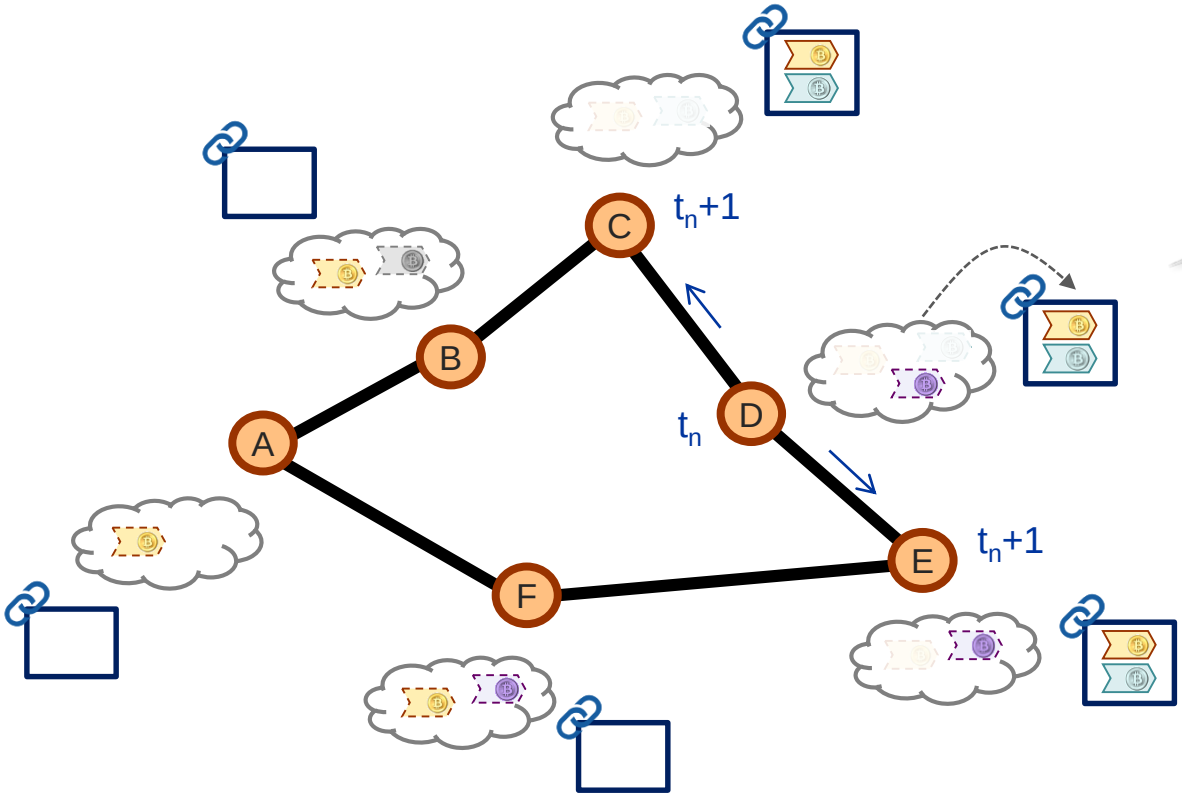
Legenda

Transações ainda não validadas (“*mempool*”)

Transações já validadas (blockchain)

Blockchain: processando eventos

- Eventos processados em **duas fases**:
  - **Fase 2**: nós validam eventos e informam rede (broadcast)
  - Eventos validados movidos para blockchain... **mas como...?**



Bitcoin: verifica assinatura e saldo

Nós receptores também validam eventos, para confirmação

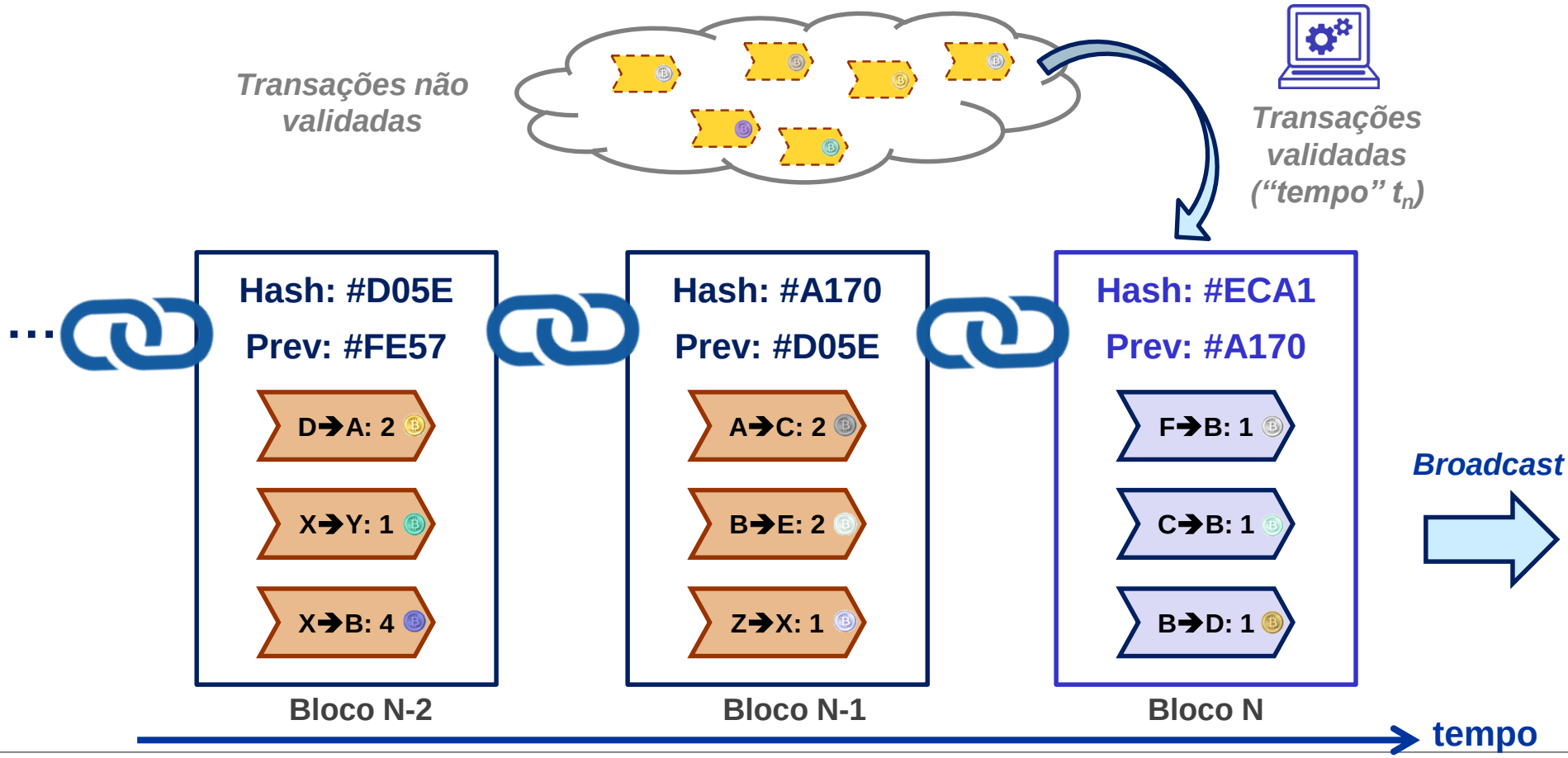
Legenda

Transações ainda não validadas (“*mempool*”)

Transações já validadas (blockchain)

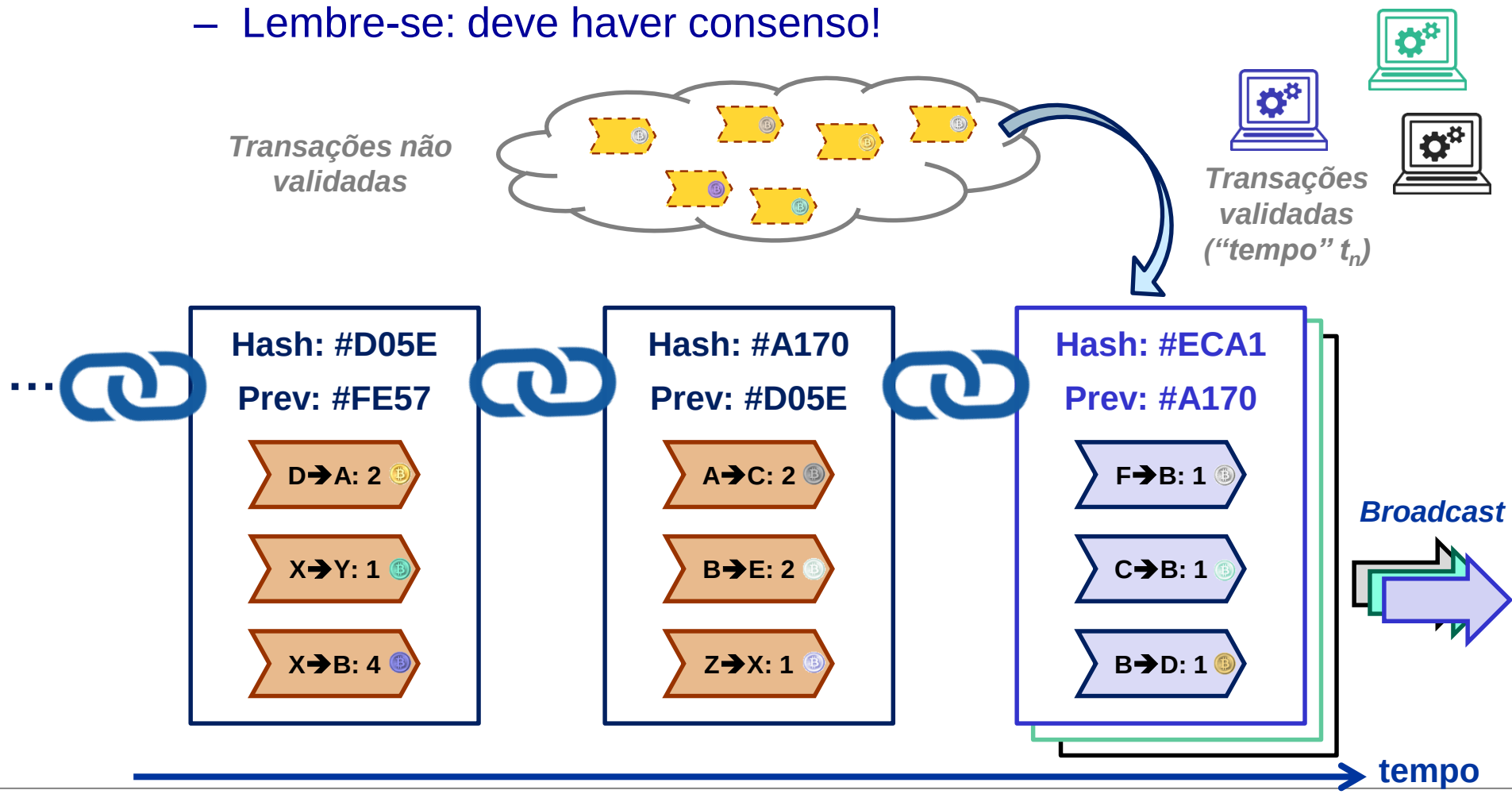
Blockchain: encadeando eventos

- Objetivo: definir uma ordem para eventos registrados
  - **Blocos**: contêm conjuntos de transações



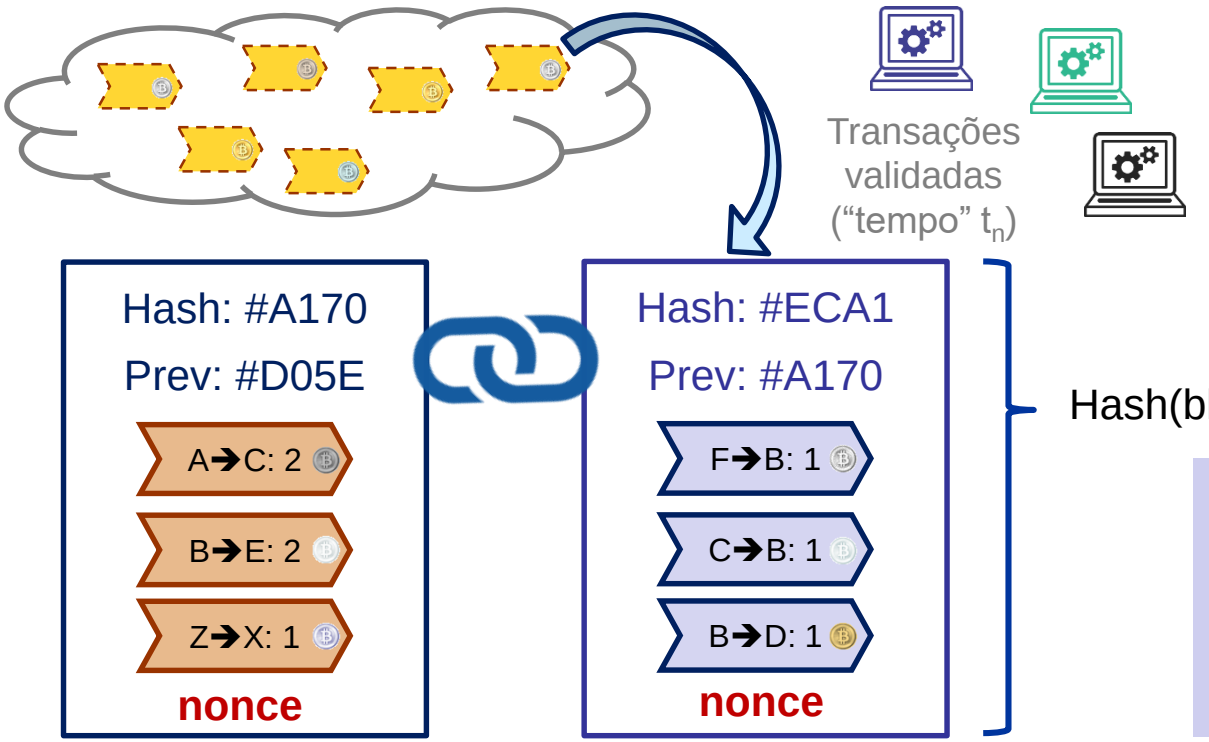
Blockchain: encadeando eventos

- Mas como decidir qual o próximo bloco “correto”?
  - Lembre-se: deve haver consenso!



Blockchain: encadeando eventos

- Consenso: proof-of-work (PoW)
  - O **primeiro que achar "nonce"** que satisfaz certas condições faz broadcast para a rede toda
  - Nós da rede sempre incluem blocos sobre **maior cadeia** recebida



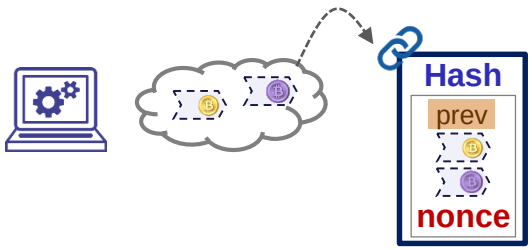
Exemplo de custo (SHA256):

Hash(bloco) < $0^{32}1^{224}$

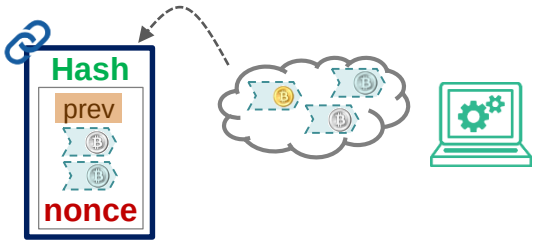
➔ em média, ~2^{32} tentativas até achar nonce

Blockchain: encadeando eventos

- Consenso: proof-of-work (PoW)
  - O **primeiro que achar "nonce"**, faz broadcast para a rede toda
  - Nós da rede sempre incluem blocos sobre **maior cadeia** recebida



Exemplo didático:
hash de 2 dígitos; alvo < 20

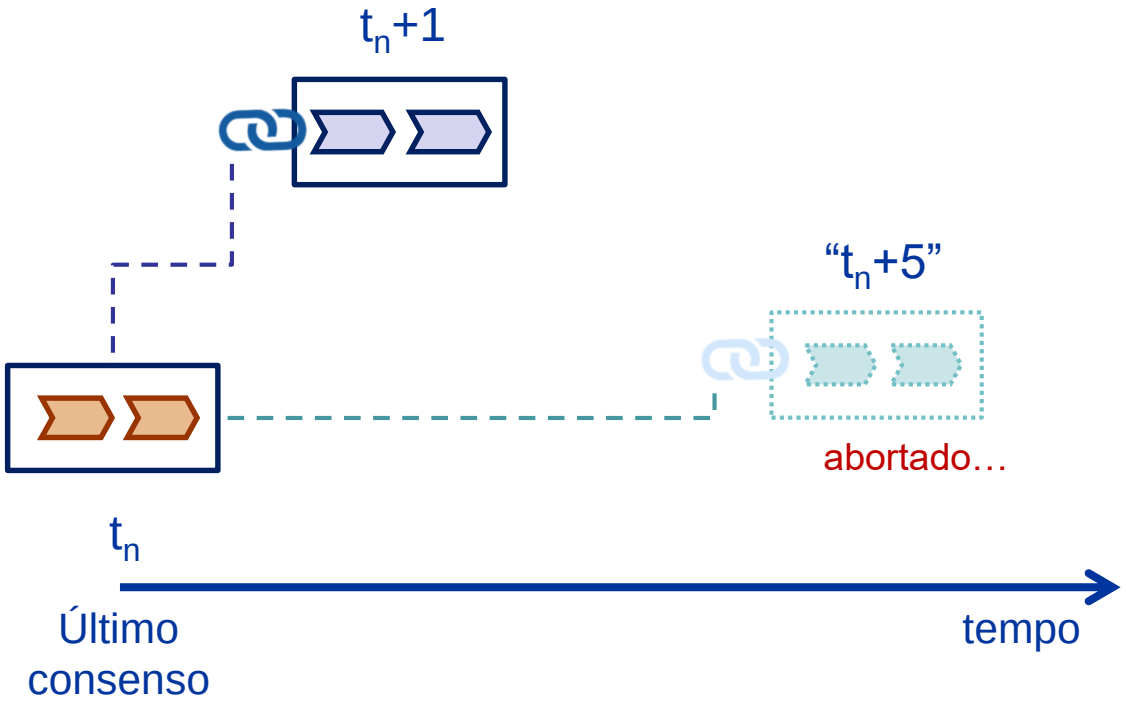


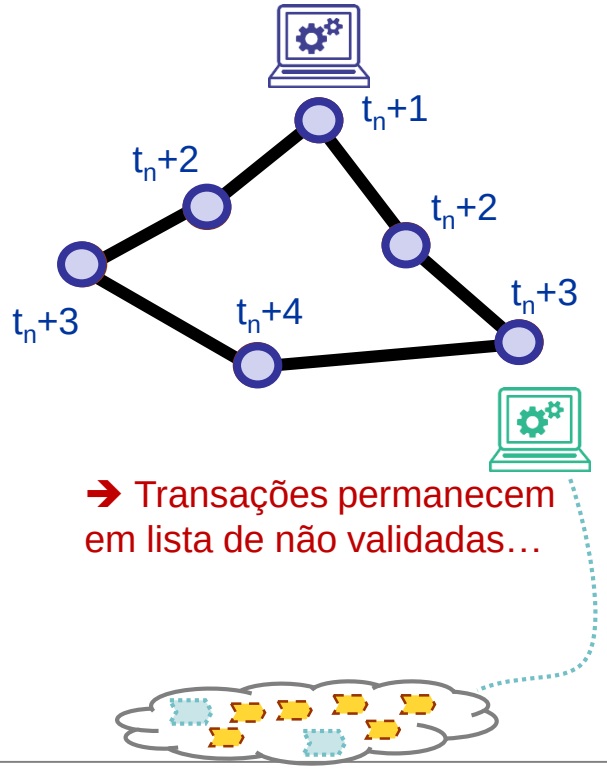
tempo

t_n	0	88			0	29
t_n+1	1	17	← broadcast		1000	54
t_n+2	2	29	propagando...		2000	91
t_n+3	4	33	propagando...		3000	38
t_n+4	8	13	propagando...		4000	54
t_n+5	16	02	propagando...	broadcast →	5000	12
	...				...	

Blockchain: encadeando eventos

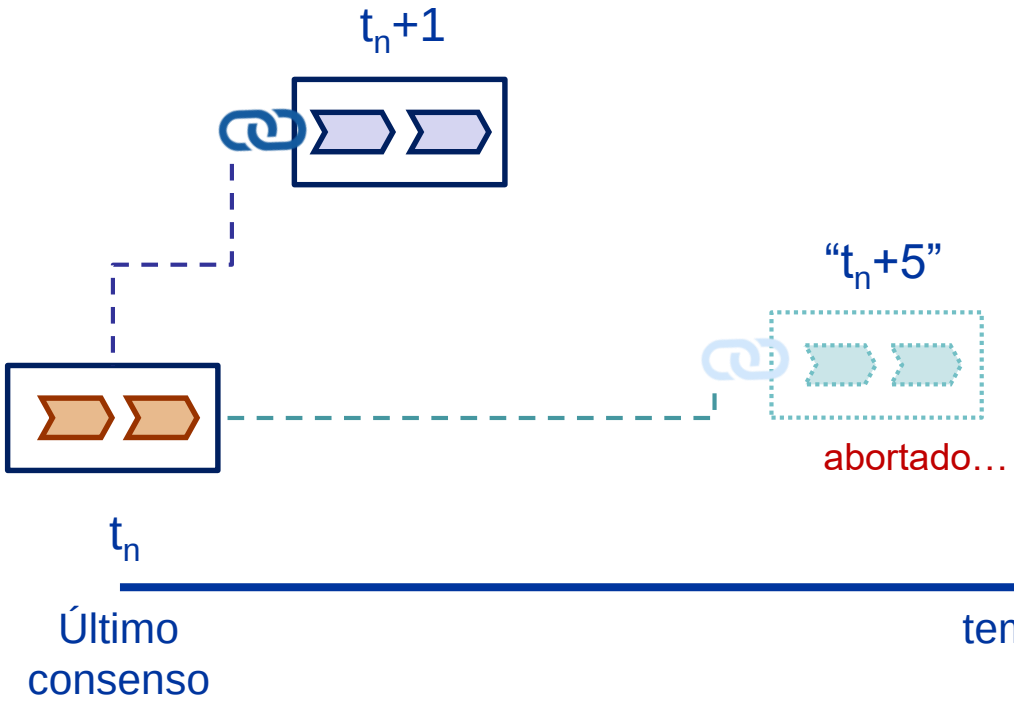
- Consenso: proof-of-work (PoW)
  - O primeiro que achar “nonce”, faz broadcast para a rede toda
  - Maior cadeia recebida ➔ consenso...

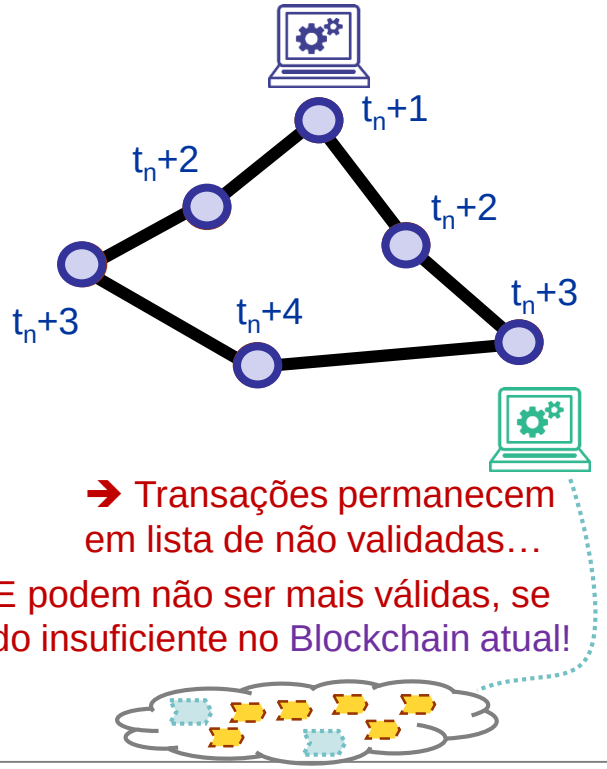




Blockchain: encadeando eventos

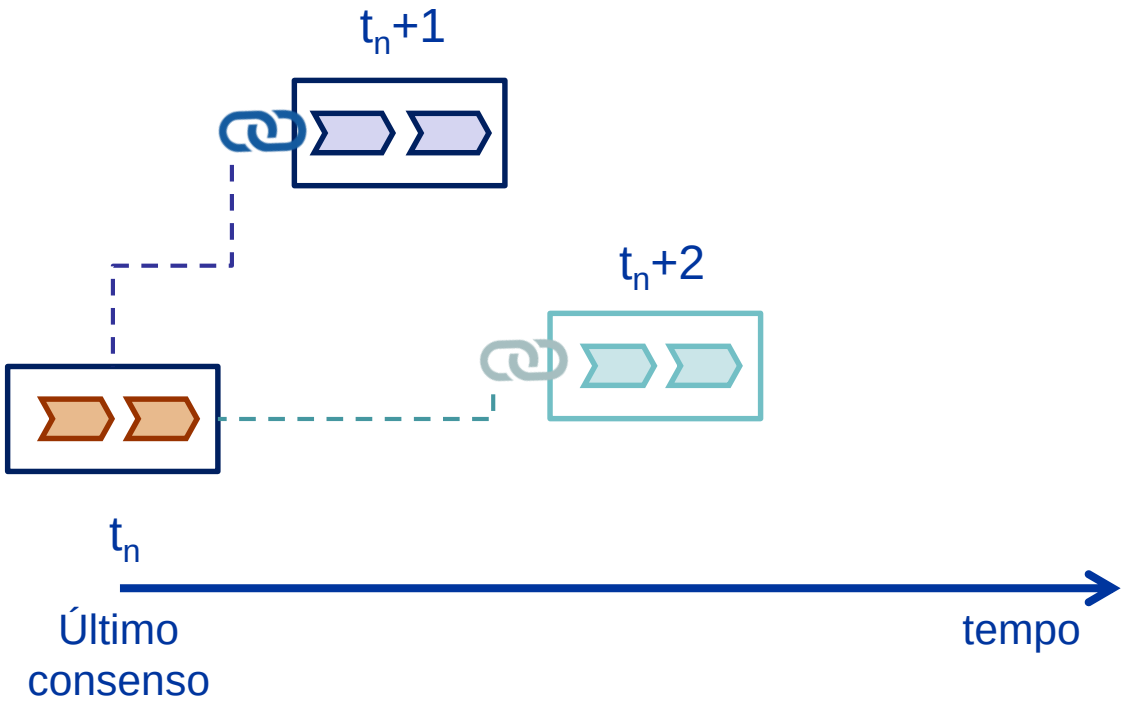
- Consenso: proof-of-work (PoW)
  - O primeiro que achar “nonce”, faz broadcast para a rede toda
  - Maior cadeia recebida ➔ consenso...

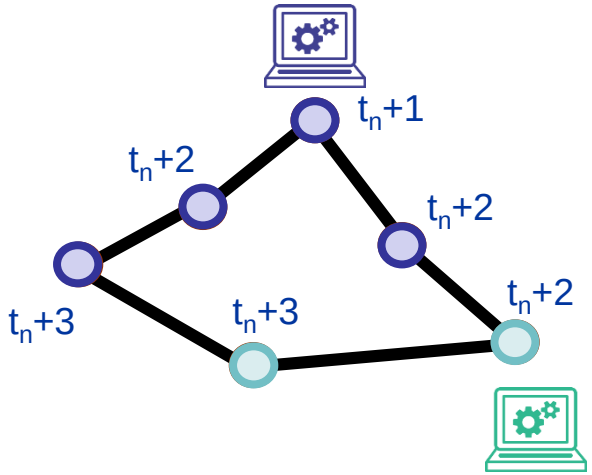




Blockchain: encadeando eventos

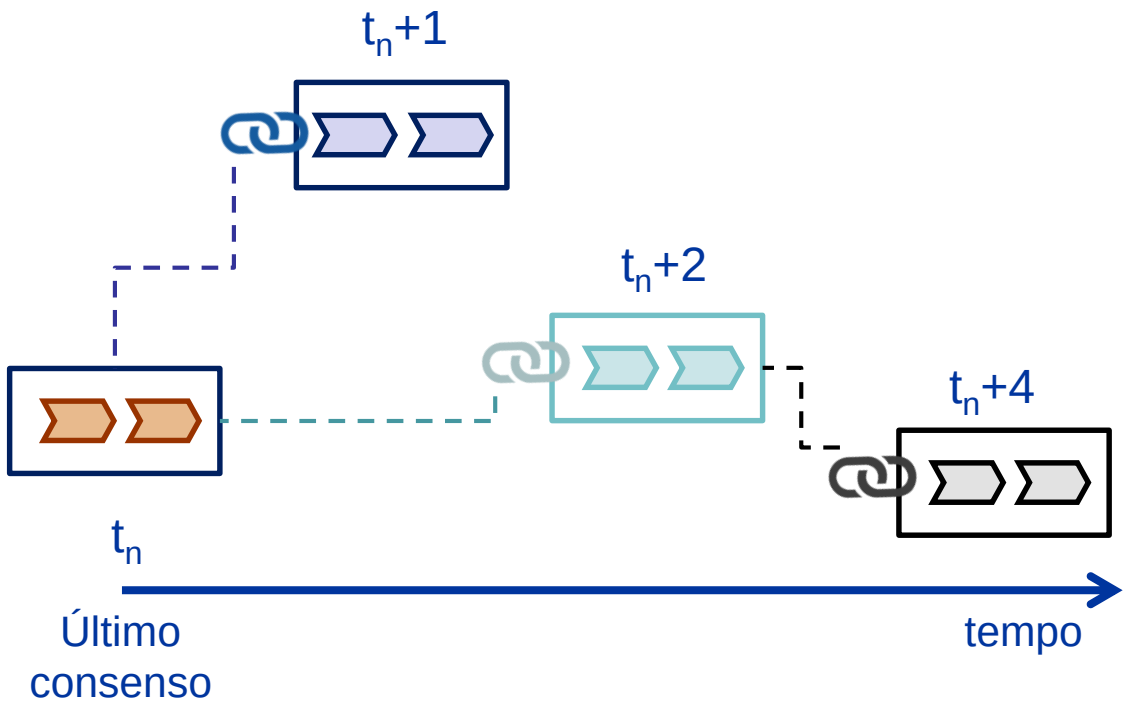
- Consenso: proof-of-work (PoW)
  - O primeiro que achar “nonce”, faz broadcast para a rede toda
  - Maior cadeia recebida ➔ consenso... **nem sempre!!!**

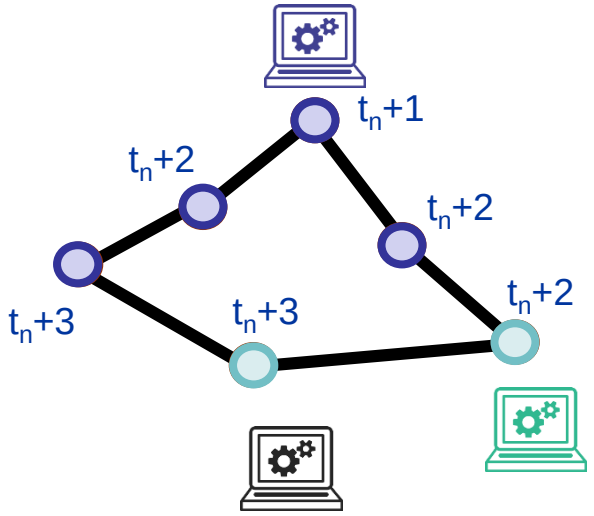




Blockchain: encadeando eventos

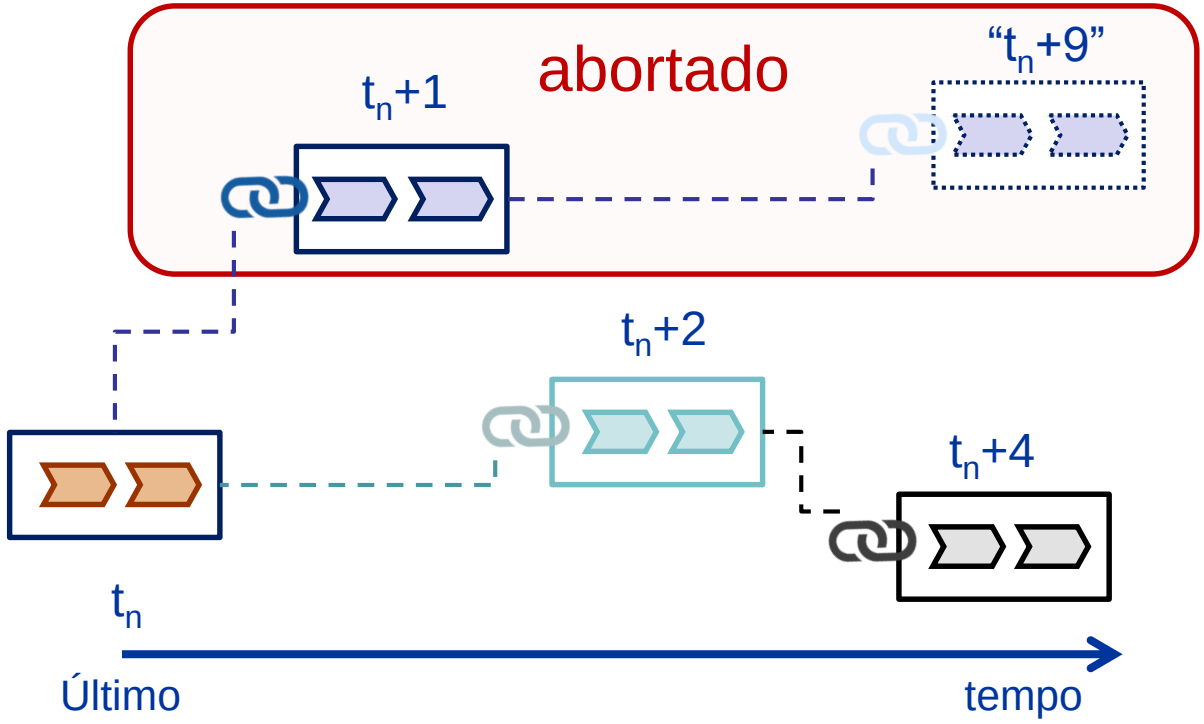
- Consenso: proof-of-work (PoW)
  - Cadeia que cresce mais rápido ganha a “corrida do consenso”
    - *Fork* (bifurcação) temporário: 2+ visões da realidade (pré-consenso)

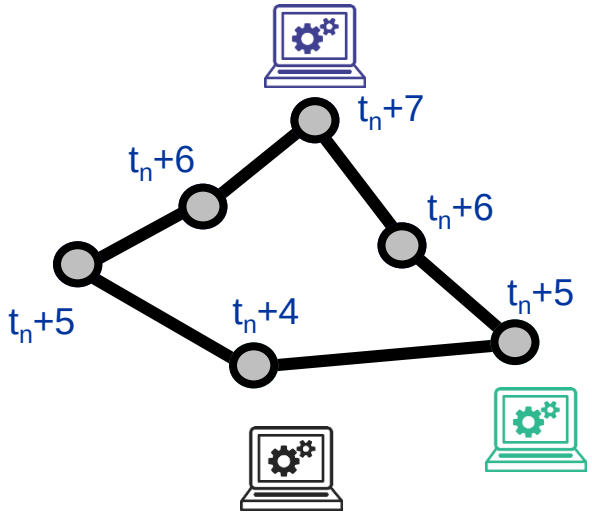




Blockchain: encadeando eventos

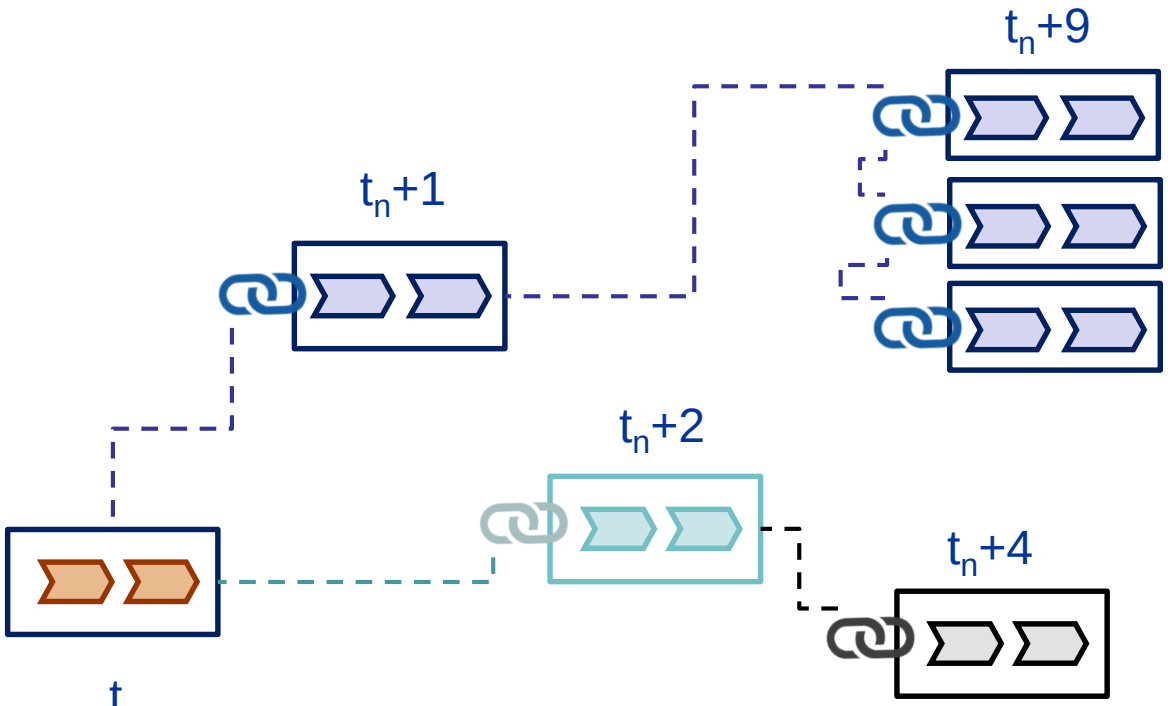
- Consenso: proof-of-work (PoW)
  - Cadeia que cresce mais rápido ganha a “corrida do consenso”
    - *Forks:* desaparecem à medida que consenso é atingido

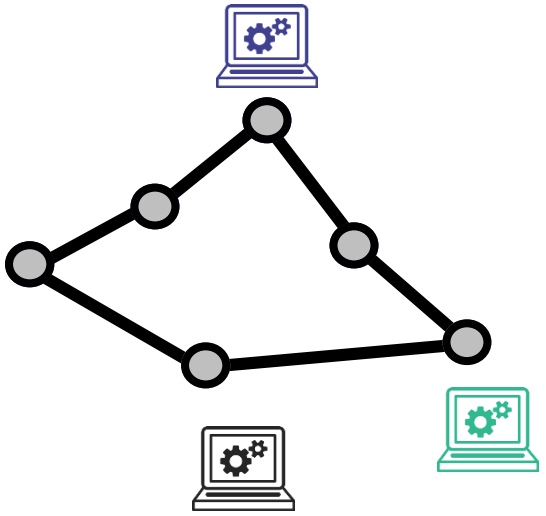




Blockchain: encadeando eventos

- Possível trapacear o consenso?
  - Se minha cadeia crescer muito rápido, posso apagar eventos!!!

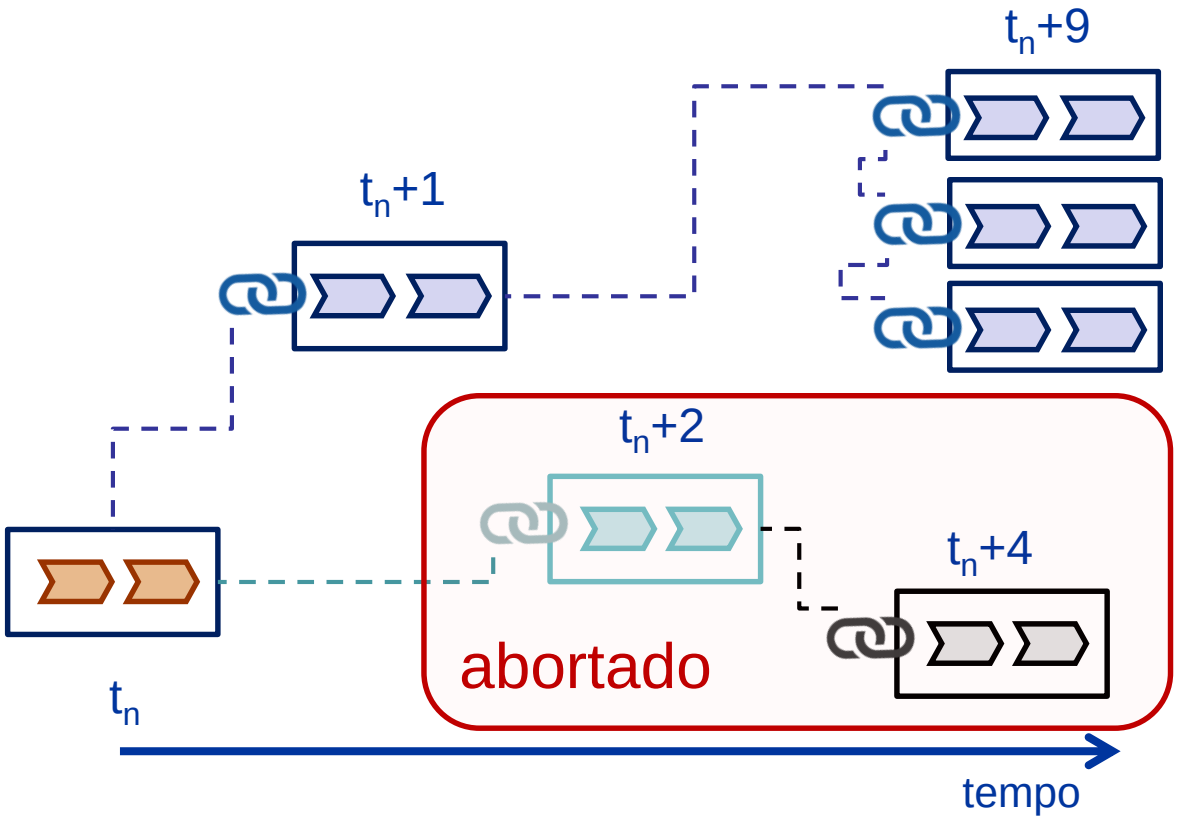


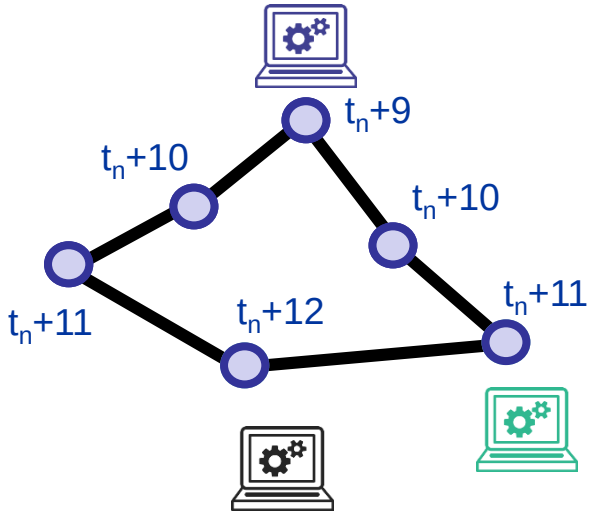


Último consenso : t_n+ 7

Blockchain: encadeando eventos

- Possível trapacear o consenso?
  - Se minha cadeia crescer muito rápido, posso apagar eventos!!!

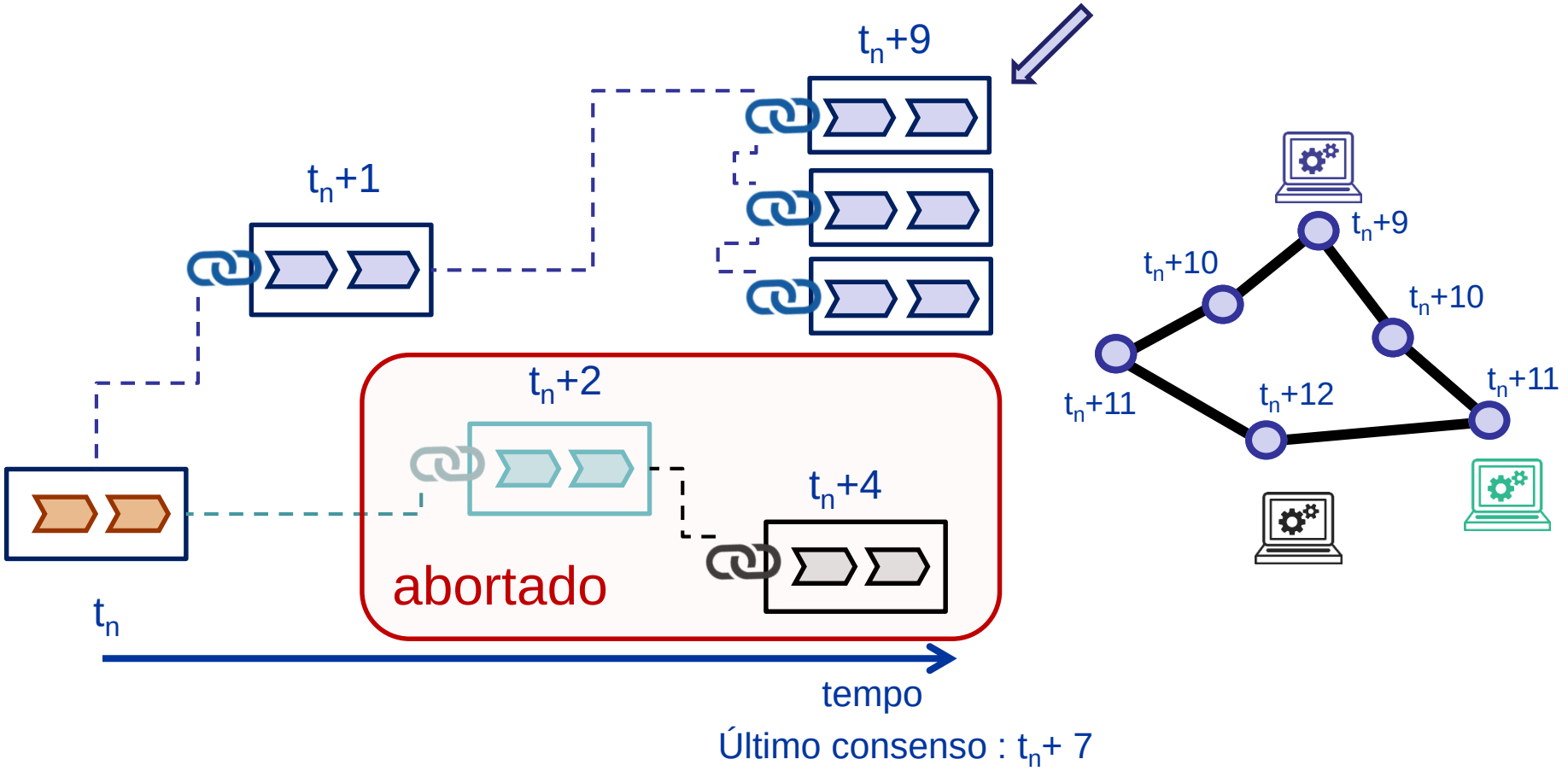




Último consenso : t_n+ 7

Blockchain: encadeando eventos

- Possível trapacear o consenso?
  - Só com poder computacional “superior ao da rede toda”...



Último consenso : t_n+ 7

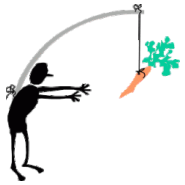
Blockchain: que tipo de eventos?

- Blockchain não faz validação dos eventos em si
  - Isso fica a cargo da camada de aplicação!
  - Nota: análogo a ACTs centralizadas…
- Verificabilidade: depende do sistema…

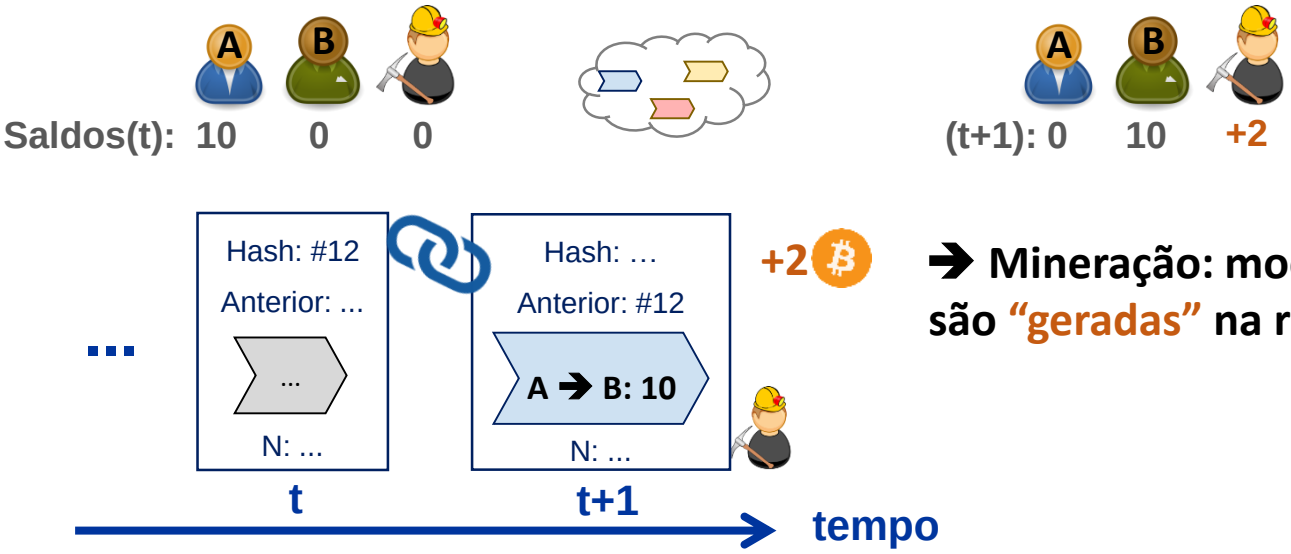
  - No Bitcoin: evento = transferência de moeda de **A** ➔ **B**
    - Verificar **assinatura de A** sobre evento
    - Verificar **saldo de A**: (1) **A** recebeu as moedas referenciadas na trasferência?; (2) **A** ainda não usou essas moedas?
      - Obs.: nó mantém base separada com “moedas não gastas”

  - Outros cenários: **pode ser complexo**…
    - **Assinatura** dos envolvidos no evento costuma ser comum
    - Interação com o mundo real (e.g., execução de um serviço, ou entrega de um produto) pode exigir auditoria no mundo real

Blockchain: incentivos?

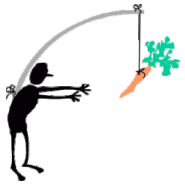


- Comumente necessário em qualquer rede P2P
  - Motivação p/ nós fornecerem recursos uns aos outros = ?
- Ex.: Bitcoin (e várias outras criptomoedas)
  - PoW: **remuneração** da rede e **taxas** para minerador

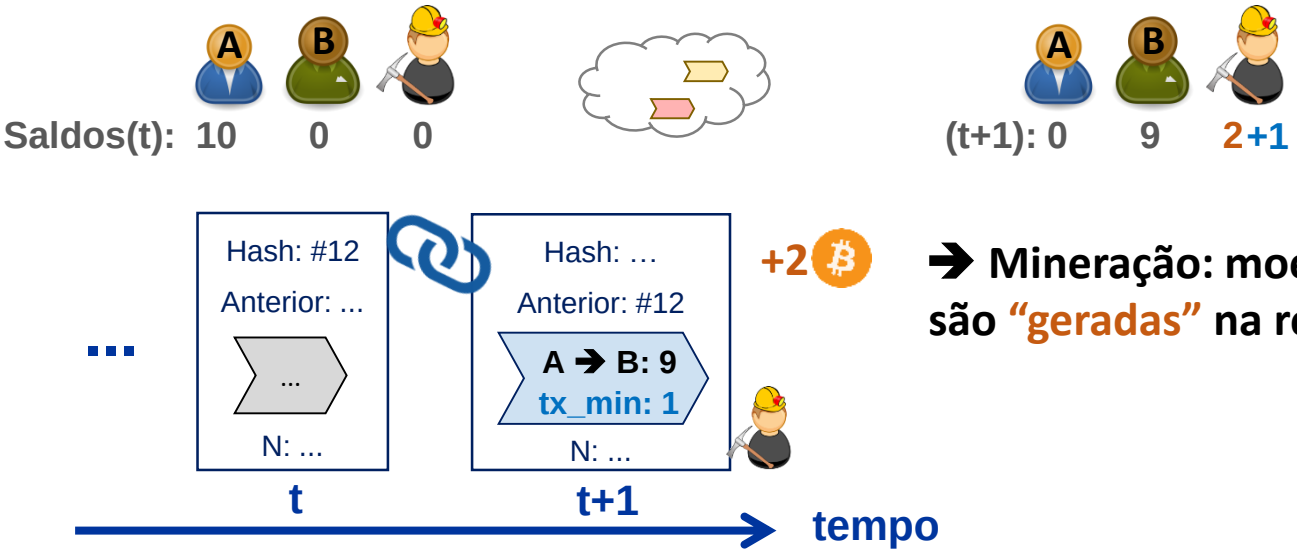


➔ **Mineração: moedas são "geradas" na rede!**

Blockchain: incentivos?



- Comumente necessário em qualquer rede P2P
  - Motivação p/ nós fornecerem recursos uns aos outros = ?
- Ex.: Bitcoin (e várias outras criptomoedas)
  - PoW: **remuneração** da rede e **taxas** para minerador



➔ **Mineração: moedas são "geradas" na rede!**

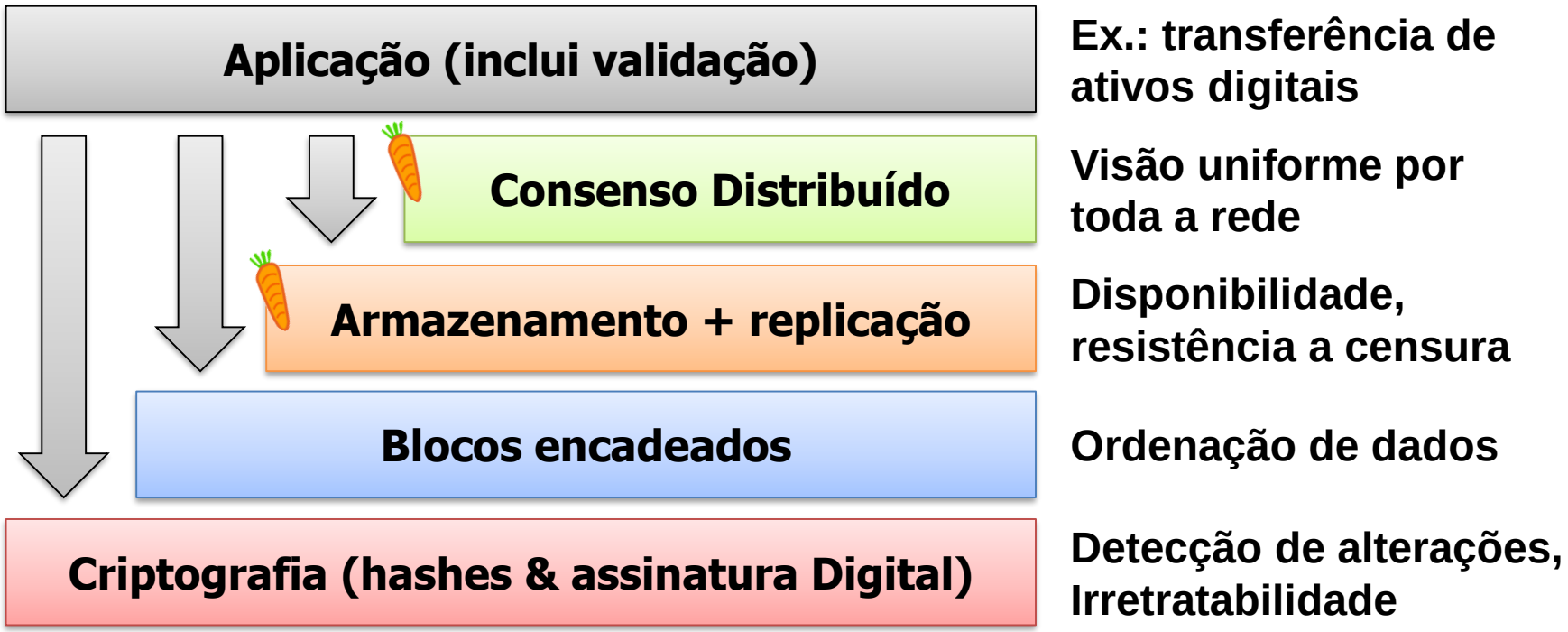
Blockchain: consenso?

- **Vários mecanismos** possíveis (tema de aula específica)
  - Dependendo do cenário, será mais ou menos custoso
  - Comumente chamados de “proof-of-something”
  - Segurança requer resiliência a conluio
    - “Ataque dos 51%”: reversão de consenso anterior se um nó (ou grupo de nós) for mais poderoso que o restante da rede
- Cenário do Bitcoin: nenhum nó conhece a rede toda, e nós são anônimos e não-confiáveis
  - **Consenso**: proof-of-work
    - Processo **custoso computacionalmente** e **demorado**:
    - Recomenda-se aguardar a validação de alguns (e.g., 8) blocos antes de aceitar transações como “parte do consenso” (forks temporários…)
    - Mais info: https://www.blockchain.com/pt/explorer

Blockchain: resumo

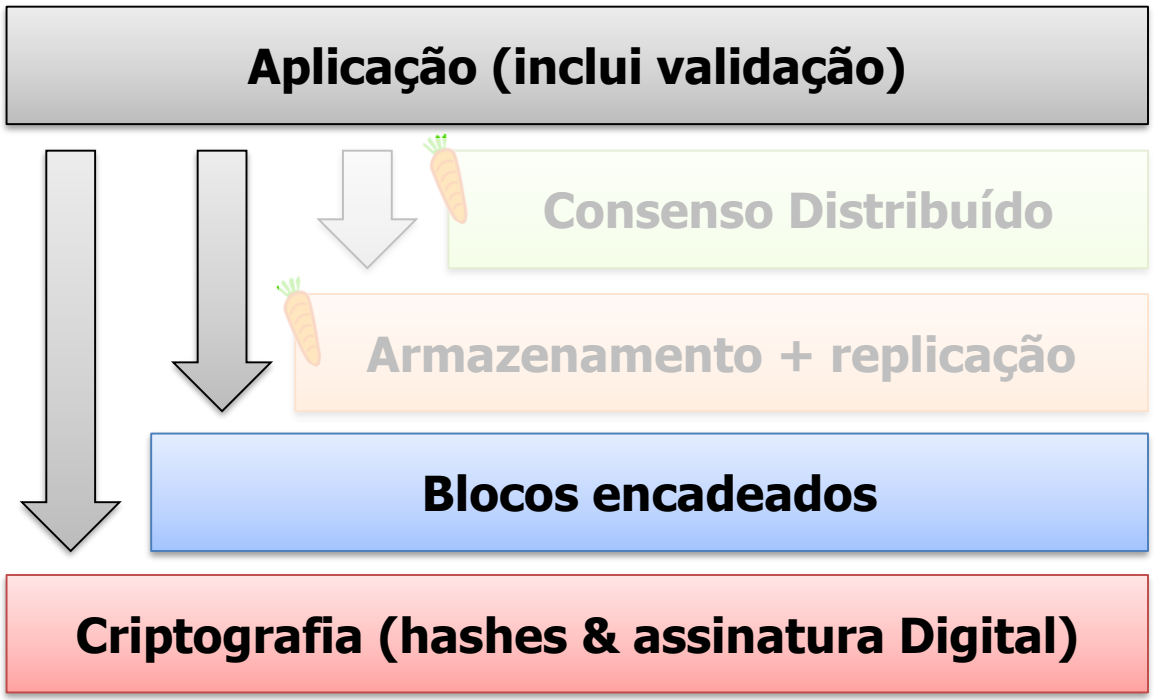
- Do ponto de vista funcional:
  - Mecanismo distribuído para **ordenação de eventos**
    - Não necessariamente corresponde à ordem do mundo real
  - Requer **consenso** entre as partes, para que todos concordem **com a ordem** armazenada
    - Consenso nada tem a ver com conteúdo (tarefa da aplicação)
- Do ponto de vista estrutural, combina
  - Cadeia de **blocos encadeados** como estrutura de dados:
    - Cada bloco contém o hash de seu antecessor
  - **Mecanismo de replicação e consenso**
    - Todos os nós armazenam uma cópia dos blocos
    - Todos os nós concordam com a ordem dos blocos na cadeia

Blockchain: módulos



- : operação do módulo costuma envolver incentivos
- **Importante**: algumas aplicações precisam apenas de alguns desses módulos!

Blockchain: log transparente



Ex.: transferência de ativos digitais

Visão uniforme por toda a rede

Disponibilidade, resistência a censura

Ordenação de dados

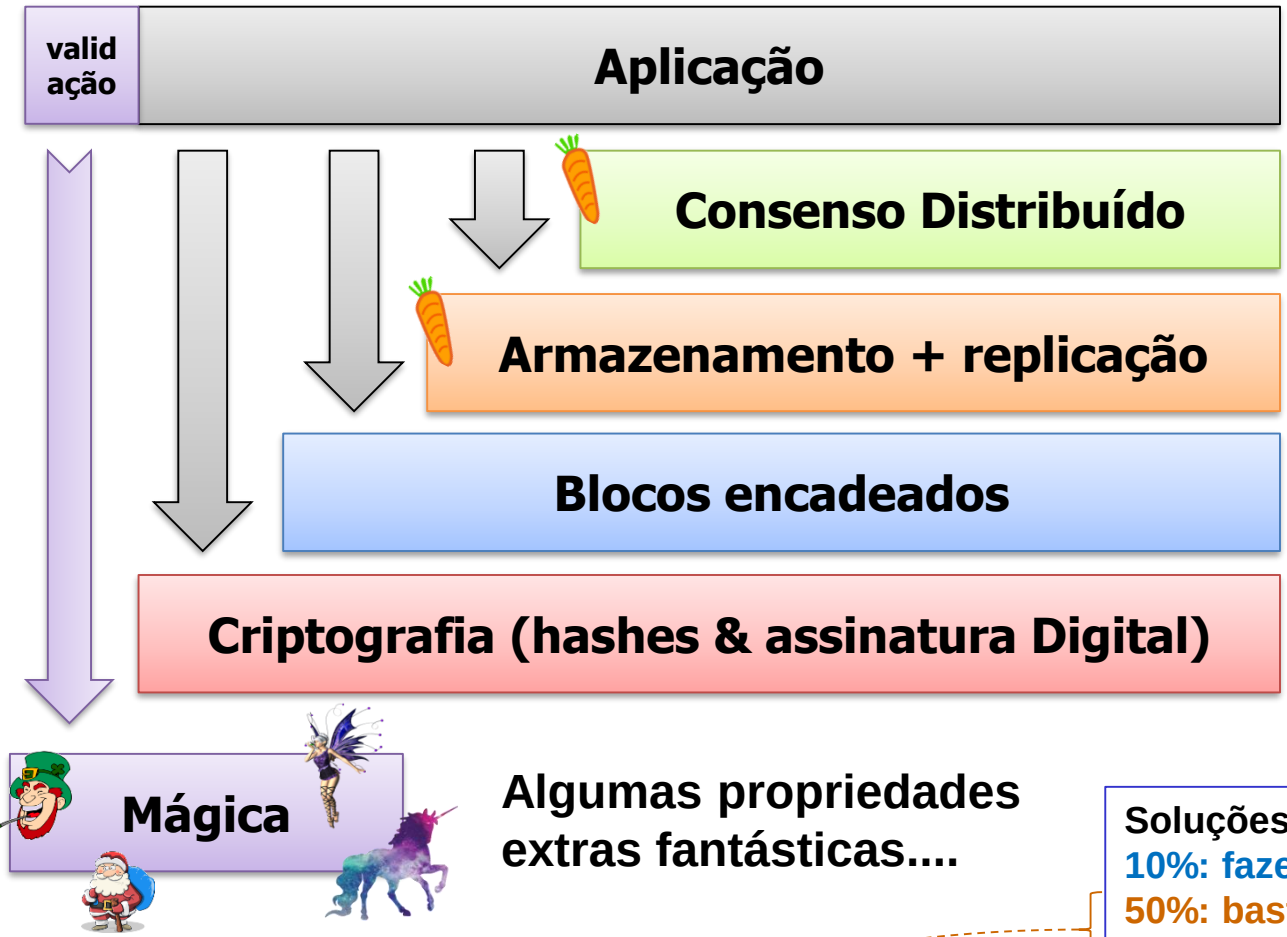
Detecção de alterações, Irretratabilidade

Blockchain: *"A structure for storing data in which groups of valid transactions, called blocks, form a chronological chain, with each block cryptographically linked to the previous one."* **MIT Technology Review**

➔ **Obs.:** Merkle Tree configurada p/ só aceitar adições de dados satisfaz essa definição…

Fonte: https://www.technologyreview.com/s/610885/a-glossary-of-blockchain-jargon/

Blockchain: só que não…



Ex.: transferência de ativos digitais

Visão uniforme por toda a rede

Disponibilidade, resistência a censura

Ordenação de dados

Detecção de alterações, Irretratabilidade

Algumas propriedades extras fantásticas....

Soluções no mercado (minha experiência):
10%: fazem bastante sentido
50%: bastam assinaturas digitais
20-30%: basta sist. arquivos distribuído
10-20%: requerem "mágica"

Log transparente pode ser útil

Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

Como funcionam blockchains

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

Apoio financeiro: d24n.org <https://d24n.org>
ripple impact | university blockchain research initiative

USP

Referências

- S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". Whitepaper, 2008. URL: https://bitcoin.org/bitcoin.pdf. Veja também (tradução paara português): https://cointimes.com.br/whitepaper-do-bitcoin-traduzido/
- A. Narayanan, J. Bonneau, E. Felten. "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction". Princeton University Press, 2016. ISBN: 0691171696. Available: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1
- L. Lantz and D. Cawrey. "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications". O'Reilly Media, 2020. ISBN: 1492054704
- I. Eyal, E. Sirer (2014). Majority is not enough: “Bitcoin mining is vulnerable”. In Int. Conf. on financial cryptography and data security (pp. 436-454). Springer, Berlin Heidelberg. URL: https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf
- Vídeos (inglês):
  - CuriousInventor. How Bitcoin Works in 5 Minutes (Technical). YouTube, Apr 14, 2014. URL: https://youtu.be/l9jOJk30eQs
  - How Bitcoin Works Under the Hood (22 min), YouTube, Jul 15, 2013. URL: https://youtu.be/Lx9zgZCMqXE