

# Hyperleadger Fabric

GABRIEL DOS SANTOS SCHMITZ

UTFPR

CRISTO REI STREET,19

CEP 85902-490 TOLEDO-PR, BRAZIL

11 02 2025



**1** Seção 1 — Blockchain

**2** Seção 2 — Fabric

# Seção 1 — Blockchain

# INTRODUÇÃO AO BLOCKCHAIN

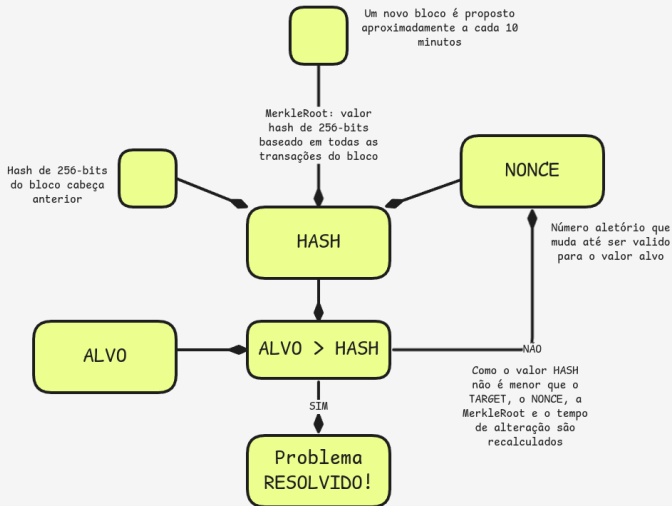
- Blockchain é uma tecnologia descentralizada para autenticar e gerenciar ativos digitais, indo além do setor financeiro.
- Evolução da atribuição de valor: do escambo a moedas universais (gado, sal, pedras Rai), inspirando NFTs e criptomoedas [1].
- A autenticidade e unicidade dos ativos são garantidas por hashes criptográficos, assegurando confiança e rastreabilidade.
- O blockchain funciona como um ledger público: uma lista imutável e transparente de transações registradas cronologicamente.
- A segurança das transações é garantida por criptografia de chaves pública e privada, prevenindo fraudes e garantindo identidade.

# O PROBLEMA DO GASTO DUPLO

- Em sistemas digitais, um mesmo ativo pode ser copiado e reutilizado, permitindo o chamado 'gasto duplo'. [3]
- Sistemas centralizados resolvem esse problema com uma autoridade confiável que valida transações.
- O Bitcoin elimina a necessidade de uma autoridade central ao usar um mecanismo descentralizado de consenso.
- As transações são registradas em blocos encadeados e protegidas por hashes criptográficos.
- O consenso é alcançado por meio da Prova de Trabalho (PoW), onde mineradores competem para resolver um problema computacional. Mais na Figura 1.
- O PoW no Bitcoin exige encontrar um número  $x$  tal que o hash de  $x$  concatenado com os dados do bloco resulte em um número menor que um determinado limite  $B$ :

Dado  $A$ , encontrar  $x$  tal que  $H(A||x) < B$

# PROOF OF WORK (PoW)



**Figure:** Mineração no Bitcoin. *Autoria própria.*

# DESAFIOS DO PROOF OF WORK (PoW)

- **Risco de 51%:** Se uma entidade controlar 51% ou mais da rede, poderá manipular a blockchain, aprovando transações fraudulentas e revertendo transações legítimas.
- **Processo demorado:** Mineradores testam muitos valores de *nonce* até encontrar a solução do problema criptográfico, tornando o processo lento.
- **Alto consumo de recursos:** A mineração de Bitcoin exige grande poder computacional, consumindo 55,27 TWh em 2019 (0,24% do total mundial), um aumento expressivo em relação a 2017 (5,027 TWh, 0,02%). Esse crescimento reflete a intensidade energética da mineração, que utiliza hardware especializado e opera continuamente, gerando preocupações ambientais e econômicas. [2]
- **Transações não instantâneas:** O tempo de confirmação varia de 10 a 60 minutos, pois as transações precisam ser mineradas e adicionadas à blockchain antes de serem finalizadas.

## Seção 2 — Fabric



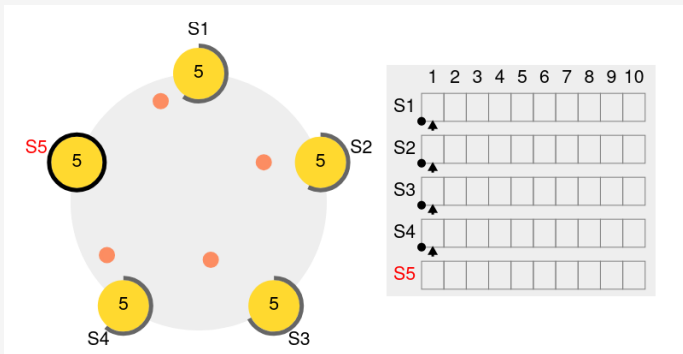
# CARACTERÍSTICAS DO HYPERLEDGER FABRIC

- **Permissão de Acesso:** Rede blockchain permissionada, onde os participantes precisam de identidade verificada.
- **Modularidade:** Suporte a diferentes mecanismos de consenso, gerenciamento de identidade e banco de dados de estado.
- **Arquitetura Flexível:** Separação entre nós de execução (*peers*) e de ordenação (*orderers*).
- **Chaincodes:** Contratos inteligentes executados fora do nó de consenso, melhorando a escalabilidade.
- **Alta Escalabilidade:** Suporte a múltiplas organizações, canais e modelos de governança distribuída.
- **Desempenho e Eficiência:** Modelo sem mineração, resultando em menor latência e maior eficiência.

# ALGORITMO DE CONSENSO RAFT

- Raft é um algoritmo de consenso projetado para gerenciar um log replicado de forma confiável [5].
- O algoritmo opera elegendo um líder, que coordena a replicação de logs entre os servidores [4].
- O líder recebe entradas de log dos clientes, propaga para os seguidores e garante que os registros sejam aplicados com segurança.
- Caso o líder falhe ou se desconecte, um novo líder é escolhido através de um processo de eleição.
- Raft divide o problema de consenso em três partes:
  - ▶ **Eleição de líder:** Escolha de um novo líder quando necessário [4].
  - ▶ **Replicação de log:** Garantia de consistência entre os servidores.
  - ▶ **Segurança:** Prevenção de registros inconsistentes ou inválidos.

# VISUALIZAÇÃO RAFT



**Figure:** Visualização de consenso Raft. *Fonte:* [6].

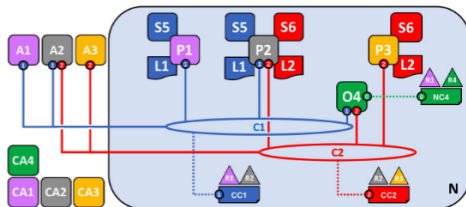
- **Certificate Authorities (CAs):** Emitem e gerenciam identidades na rede via certificados X.509.
- **Ledgers:** Livro-razão composto pelo *Blockchain* (histórico de transações) e *State Database* (estado atual).
- **Channels:** Criam redes privadas para transações isoladas e seguras.
- **Ordering Services:** Ordenam e distribuem transações em blocos, garantindo consistência.

# ELEMENTOS DE UMA REDE FABRIC







- **Peers:** Nós que armazenam o ledger e executam *chaincodes*.  
Tipos:
  - ▶ **Endorsing Peers:** Validam e simulam transações.
  - ▶ **Committing Peers:** Aplicam blocos ao ledger.
  - ▶ **Anchor Peers:** Facilitam comunicação entre organizações.
- **Organizations:** Empresas/instituições com seus próprios *peers* e regras.
- **Chaincodes:** Contratos inteligentes que processam transações e alteram o ledger.
- **Clients:** Aplicações que enviam transações, coletam aprovações e as submetem à rede.

# REDE FABRIC

- R1..R4: Organizações 1 a 4      CA1..C4: CAs das Orgs
- C1, C2: Channels 1, 2      L1, L2: Ledgers 1, 2
- P1..P3: Peers das Orgs 1..3      O4: Ordering Service
- S5, S6: Chaincodes
- A1..A3: Clientes



**Figure:** Exemplo de rede Fabric. *Fonte: Escola Superior de Redes.*

-  SEYED MOJTABA HOSSEINI BAMAKAN, NASIM NEZHADSISTANI,  
OMID BODAGHI, AND QIANG QU.  
**Patents and intellectual property assets as non-fungible tokens;  
key technologies and challenges.**  
*Scientific Reports*, 12(1):2178, feb 2022.
-  SINAN KÜFEOĞLU AND MAHMUT ÖZKURAN.  
**Energy consumption of bitcoin mining.**  
2019.
-  SATOSHI NAKAMOTO.  
**Bitcoin: A peer-to-peer electronic cash system.**  
oct 2008.
-  DIEGO ONGARO AND JOHN OUSTERHOUT.  
**In search of an understandable consensus algorithm (extended  
version).**  
2014.
-  DIEGO ONGARO AND JOHN OUSTERHOUT.  
**Raft consensus algorithm, 2014.**
-  **Diego Ongaro and John Uckele.**

**Raftscope: Super hacky visualization of raft.**