

Outubro 2025

SEMANA INTEGRADA DA COMPUTAÇÃO 2025

CRIPTOGRAFIA E BLOCKCHAIN

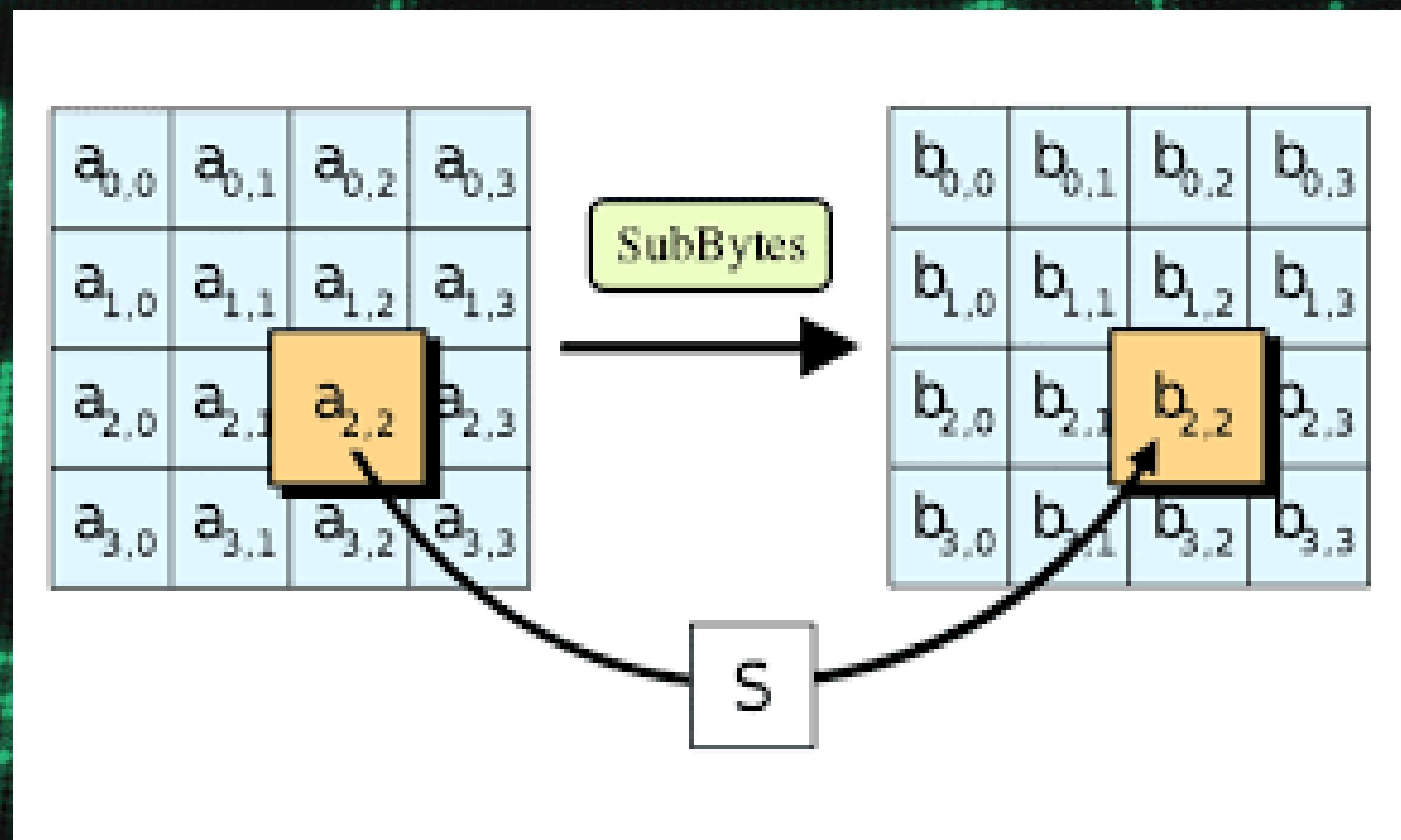
Tipos de criptografia

- SIMÉTRICA (MESMA CHAVE) → AES

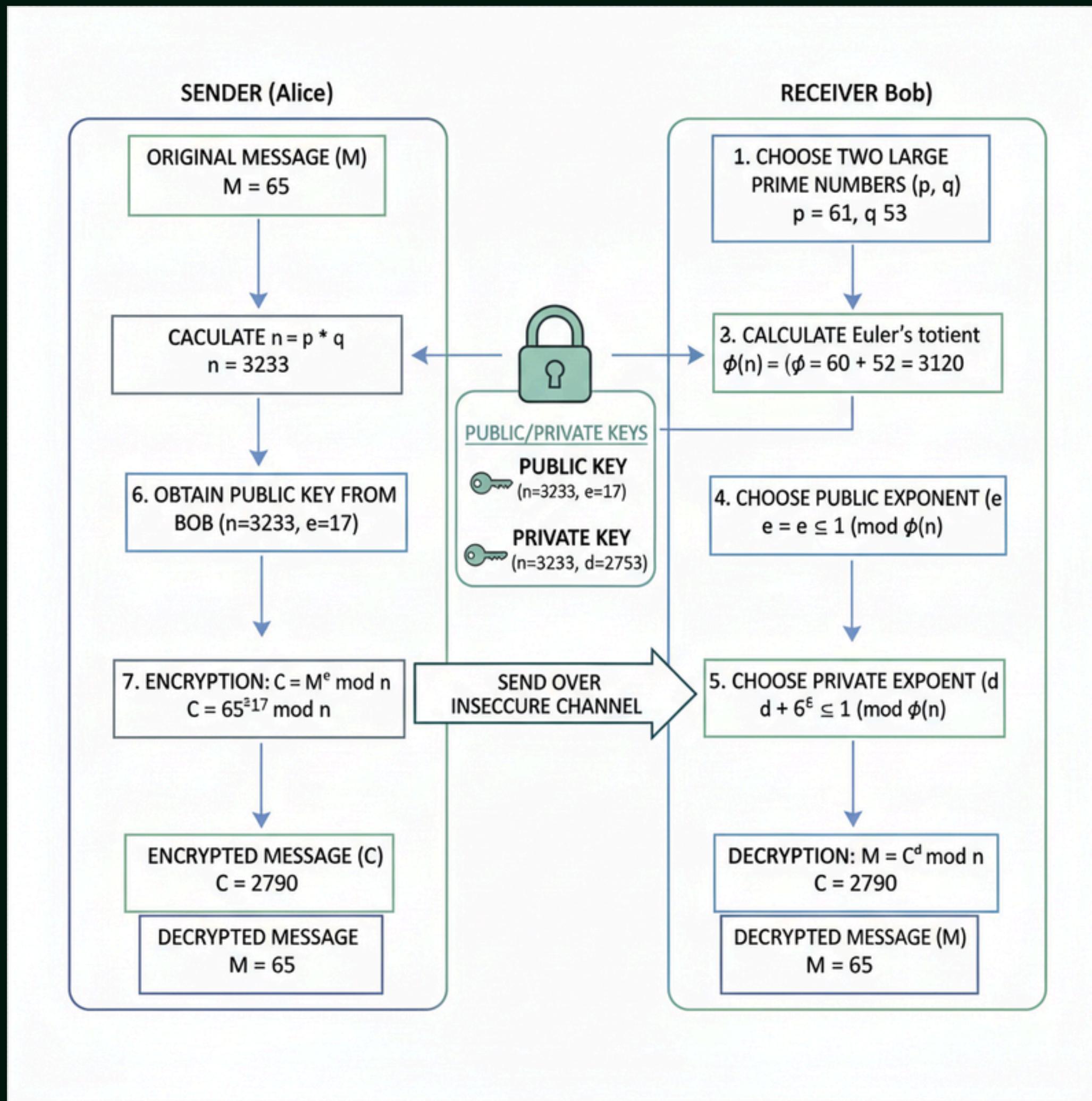
- ASSIMÉTRICA (PAR DE CHAVES) → RSA, ECC

- HASH FUNCTIONS (IMPRESSÃO DIGITAL ÚNICA) → SHA-256

ADVANCED ENCRYPTION STANDARD



RIVEST-SHAMIR-ADLEMAN



O algoritmo **RSA** é um dos primeiros e mais usados algoritmos de criptografia de chave pública.

- **p** e **q**, dois números primos aleatórios(quanto maior melhor);
- **n** será o produto de **p** e **q**. Esse valor irá fazer parte da chave privada e pública.
- **φ(n)** Esta função calcula a quantidade de inteiros positivos menores que **n** que são coprimos (não compartilham fatores além de 1) com **n**;
- **d** é um número inteiro que será a chave privada. Ele é calculado de tal forma que seja o inverso multiplicativo de **e** módulo **φ(n)**. Isso significa que quando **e * d** é dividido por **φ(n)**, o resto é 1.

POR QUE É SEGURO?

A segurança do **RSA** reside no fato de que é extremamente difícil fatorar números grandes. Para um atacante que intercepta a chave pública $\{e, n\}$ e a mensagem criptografada **C**, ele precisaria descobrir **d** para descriptografar a mensagem. Para descobrir **d**, ele precisaria de **φ(n)**, e para descobrir **φ(n)**, ele precisaria saber **p** e **q**. Fatorar **n** (descobrir **p** e **q** a partir de **n**) é computacionalmente inviável quando **p** e **q** são números primos muito grandes (centenas de dígitos).

CONTRAS ?

- Lento
- Força Bruta



Uma função hash criptográfica é um algoritmo matemático que mapeia dados de tamanho arbitrário para um output de tamanho fixo, chamado hash, digest ou resumo.

1. Determinístico: Mesma entrada = mesma saída.
2. Rápido: Fácil de calcular o hash.
3. Irreversível (Uma Via): Impossível (ou computacionalmente inviável) reverter do hash para a entrada original.
4. Efeito Avalanche: Uma pequena mudança na entrada resulta em um hash drasticamente diferente.

APLICAÇÕES

- Hashes são usados para ligar blocos de transações (cada bloco contém o hash do bloco anterior), garantir a integridade das transações e no processo de "mineração" (Proof of Work).
- Verificação de Integridade de Dados.

Outubro 2025

BLOCKCHAIN

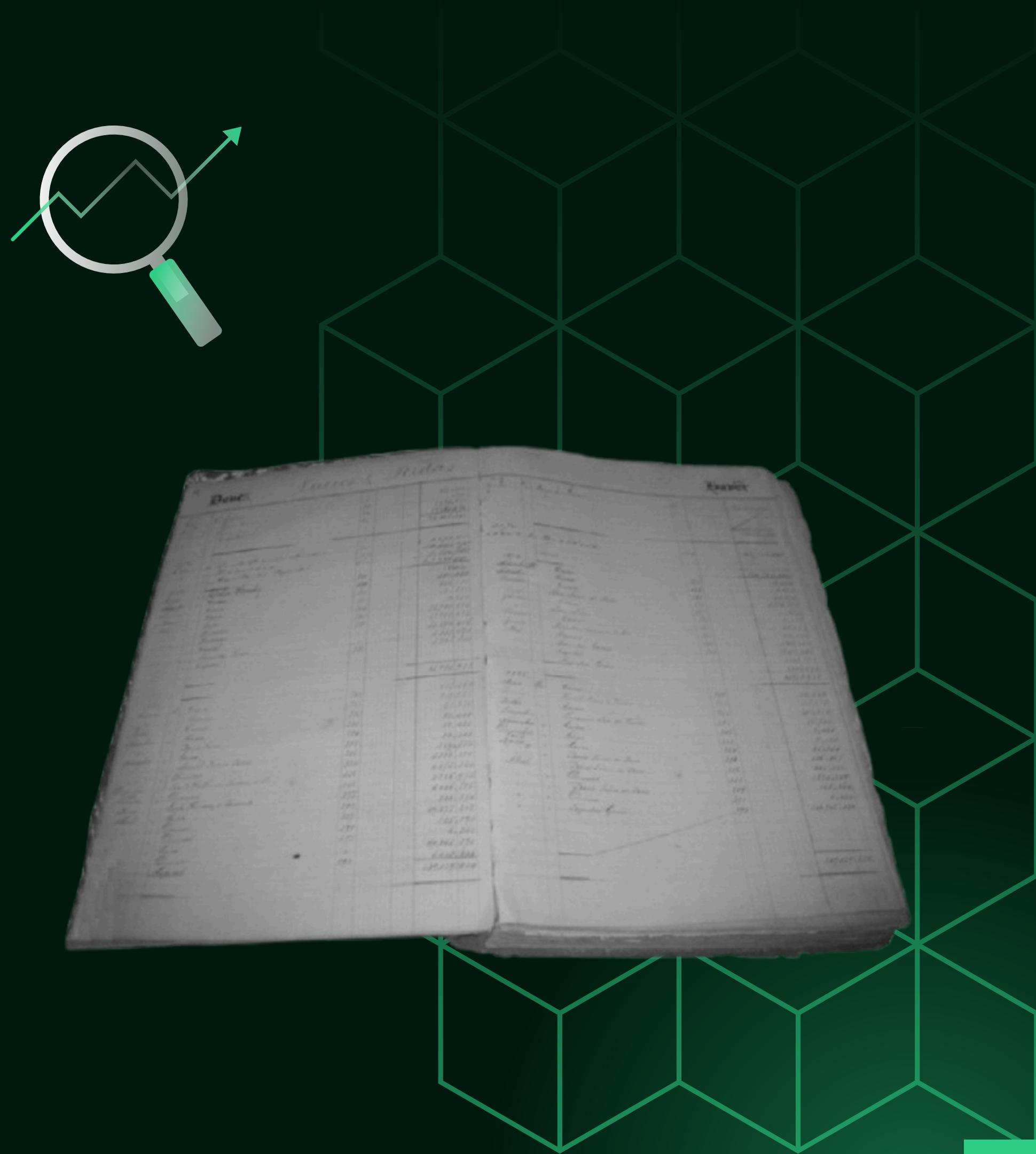
WHAT IS

LIVRO RAZÃO

O QUE É

O livro razão é um dos instrumentos usados pela contabilidade para escriturar as movimentações econômicas que acontecem no cotidiano das empresas.

- Confiabilidade ?
- Autenticidade ?
- Integridade ?
- Disponibilidade ?



BLOCKCHAIN LIVRO RAZÃO DISTRIBUIDO

Blockchain é uma implementação inovadora e segura de um livro razão, podendo ser dita como um livro razão digital distribuído.

Uma blockchain é conjunto de **blocos** lógicamente encadeados através do mecanismo de hash criptográfico

<https://andersbrownworth.com/blockchain/blockchain>



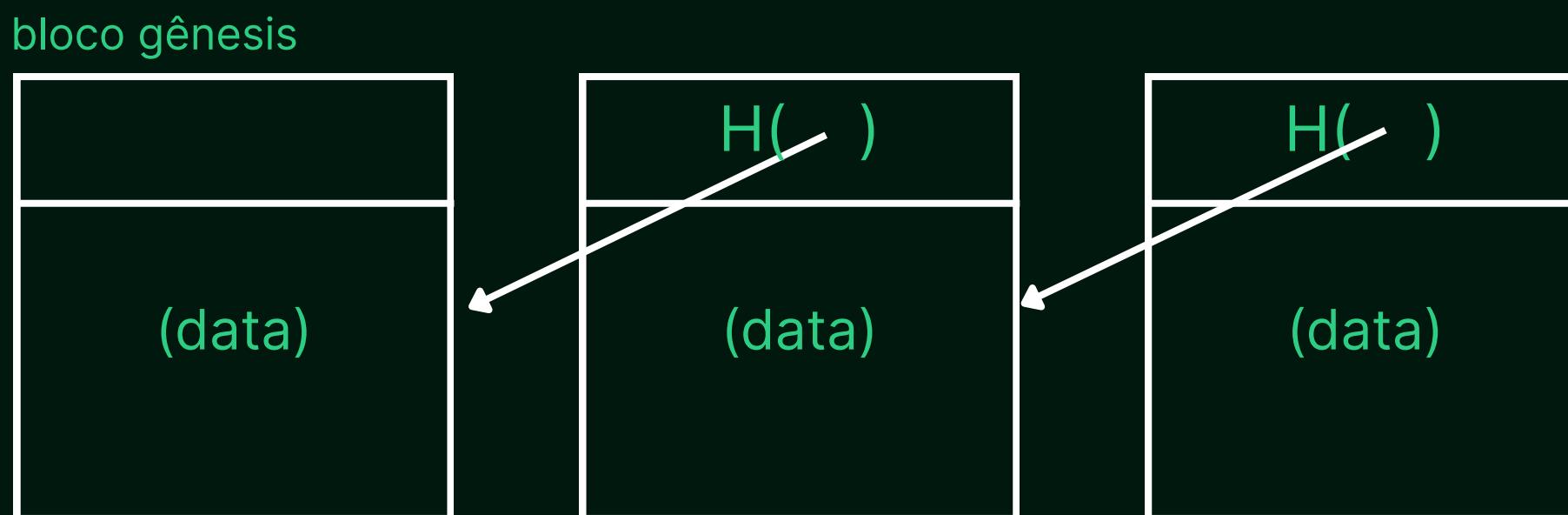


ESTRUTURA DE DADOS DE MODO SIMPLIFICADO



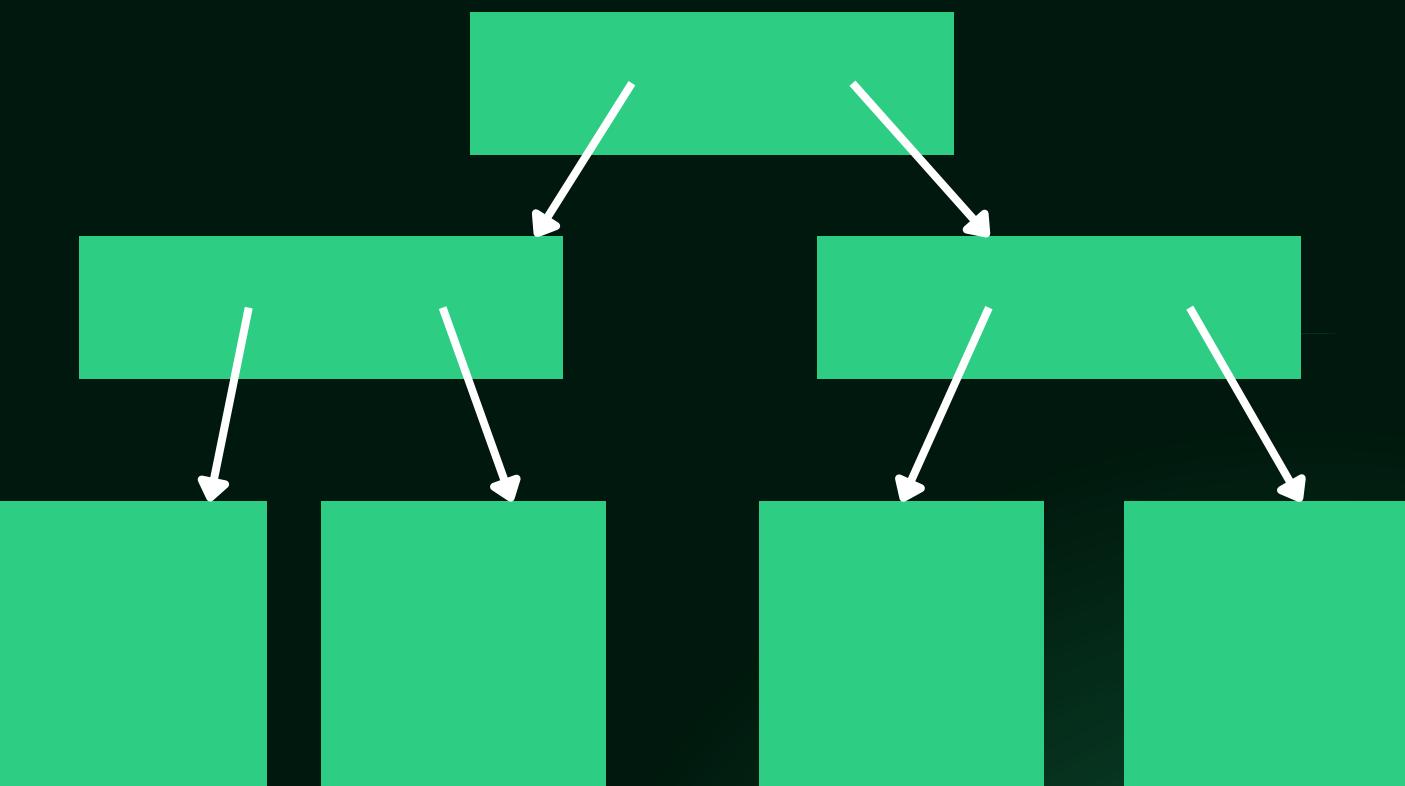
BLOCOS??

Estrutura Encadeada

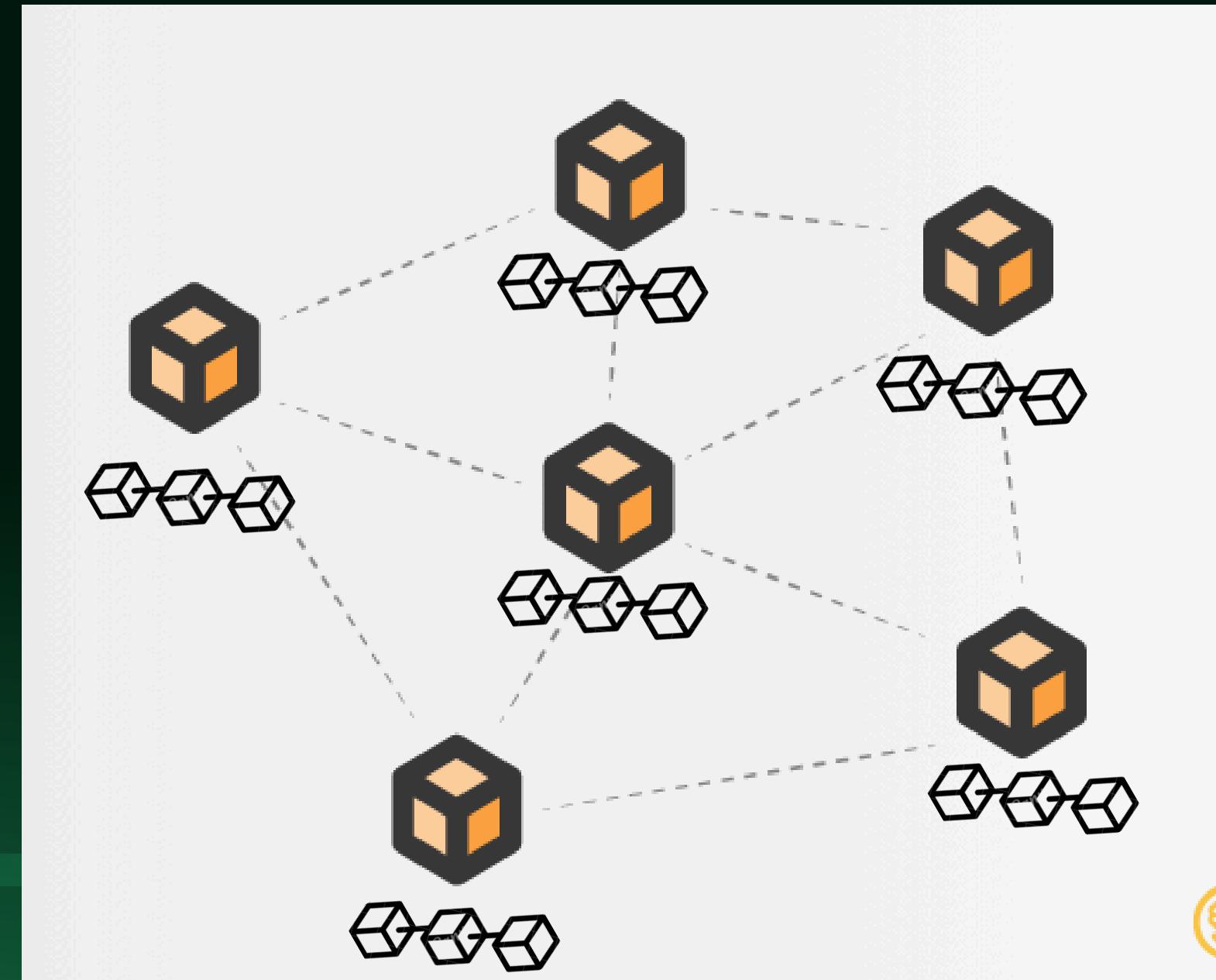


A estrutura de dados é consistida por um Header e uma lista de transações
(nesse caso apelidada por data)

Árvore de Merkle

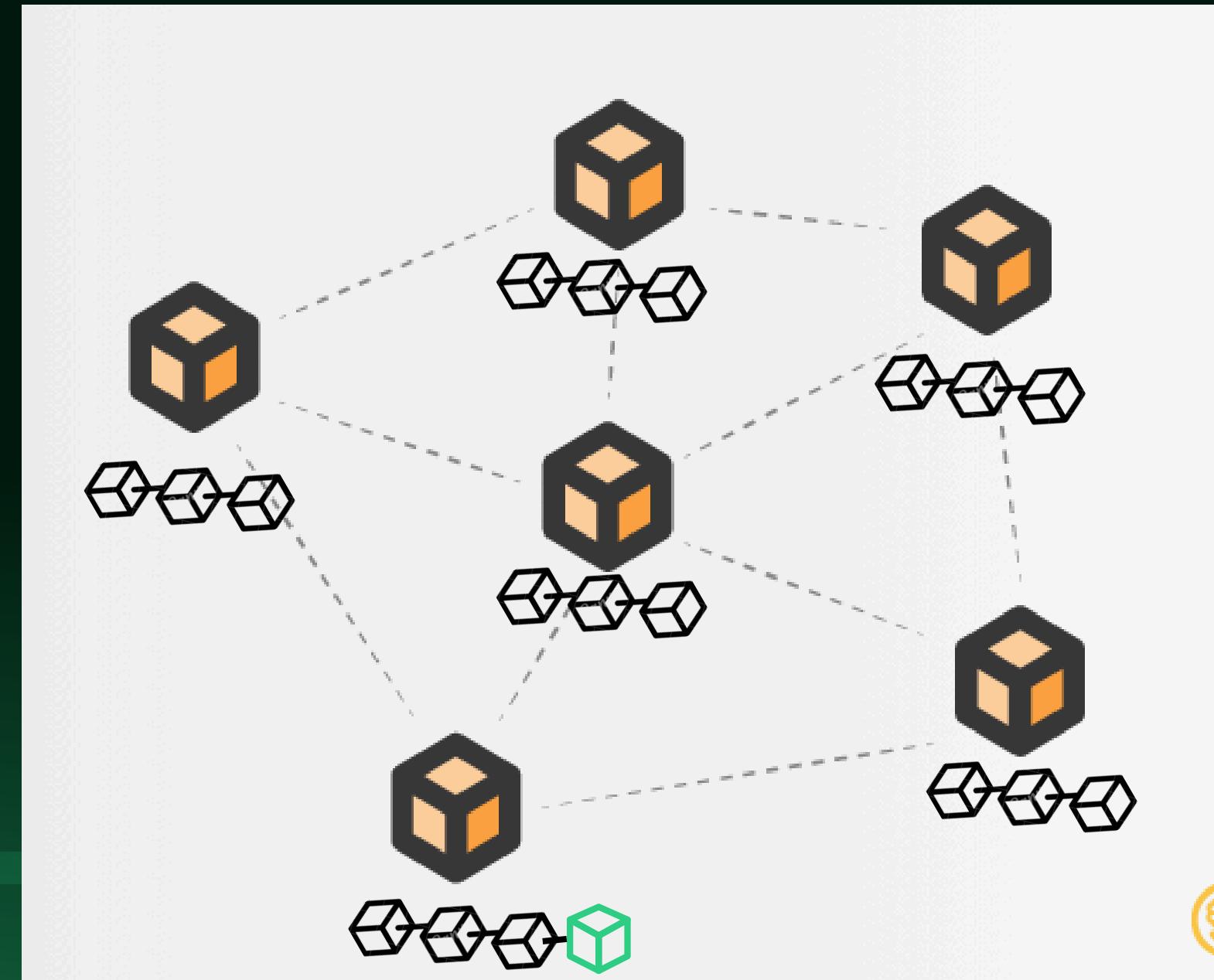


A REDE DESCENTRALIZADA



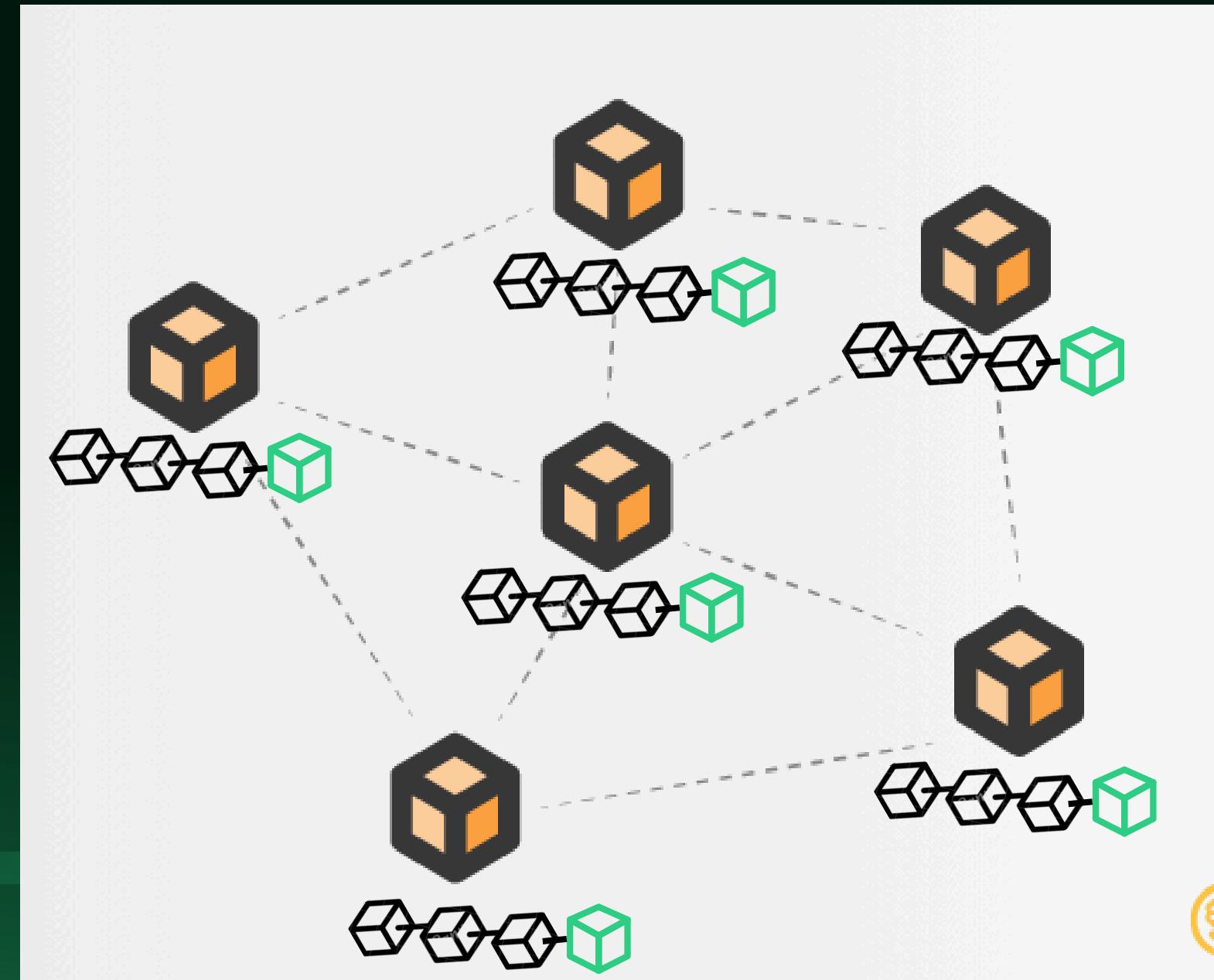
- Cópia da estrutura de dados para todos os nós
- Redes Públicas x Privadas
 - Públicas: qualquer um pode fazer parte da rede
 - Privadas: restrições para usuários participantes

A REDE DESCENTRALIZADA



- Cópia da estrutura de dados para todos os nós
- Redes Públicas x Privadas
 - Públicas: qualquer um pode fazer parte da rede
 - Privadas: restrições para usuários participantes
- Nós sincronizados e atualizados
 - Como realizar uma atualização na rede ?

A REDE DESCENTRALIZADA



- Cópia da estrutura de dados para todos os nós
- Redes Públicas x Privadas
 - Públicas: qualquer um pode fazer parte da rede
 - Privadas: restrições para usuários participantes
- Nós sincronizados e atualizados
 - Como realizar uma atualização na rede ?
 - Algoritmos de consenso (PoW, PoS etc)
 - Comunicação P2P
- Permissionadas x Não-Permissionadas
 - Permissionadas: necessitam de permissão para participar do algoritmo de consenso
 - Não permissionadas: qualquer um pode participar do algoritmo de consenso



POW - PROVA DE TRABALHO

Proof of Work consiste na solução de um puzzle criptográfico em um determinado tempo. A pessoa que terminar primeiro recebe a recompensa em criptomoedas através das **taxis de transação** e **coinbase transaction**.

Puzzle criptográfico: consiste em achar um valor do nonce de tal maneira em que o hash do bloco seja menor que um determinado valor (Threshold). Onde pode ser modificado em uma quantidade definida de blocos.

Taxas de transação: cada transação solicitada por um participante (carteira) fica em aguardo em uma **mempool**, onde é selecionada para um bloco a depender dos mineradores onde analisam sua “gorjeta” deixado para eles.

Coinbase transaction: no protocolo do bitcoin atulmente a pessoa que minerar o bloco ganha ,além das taxas, 3.125 BTC (quarto halving) que são **mintados** pela coinbase, e esse valor é diminuído pela metade a cada 210000 blocos minerados.



Bitcoin (mainnet): Rede Pública
e não permissionada



O QUE É ~~BITCOIN~~ CRIPTOMOEDAS

BTC é a **criptomoeda** nativa da rede principal (mainnet) Bitcoin. Todas as transações e emissões ficam registradas de forma permanente na blockchain, o livro-razão distribuído da rede.

Confiança: “A teoria sugere que os indivíduos enviam sinais sobre suas qualidades ao se envolverem em comportamentos que são difíceis e custosos de fingir, tornando o sinal mais confiável.”



POS - PROVA DE POSSE

A segunda criptomoeda mais famosa utiliza um algoritmo de consenso diferente: PoS

PoS → “Quanto mais criptomoedas você tiver maiores as chances de você fazer parte do comitê de validação”

PoW (Proof of Work)

- Mineradores resolvem problemas matemáticos
- Alto consumo de energia
- Segurança pela dificuldade do ataque

PoS (Proof of Stake)

- Comitê de validação selecionado pela rede
- Validadores apostam tokens como garantia
- Mais eficiente energeticamente

Confiança: “Participantes do consenso colocam algo de valor, que potencialmente pode ser destruído, caso hajam da maneira desonesta.”



Ethereum (mainnet): Rede Pública e não permissionada (32 ETH mínimos)

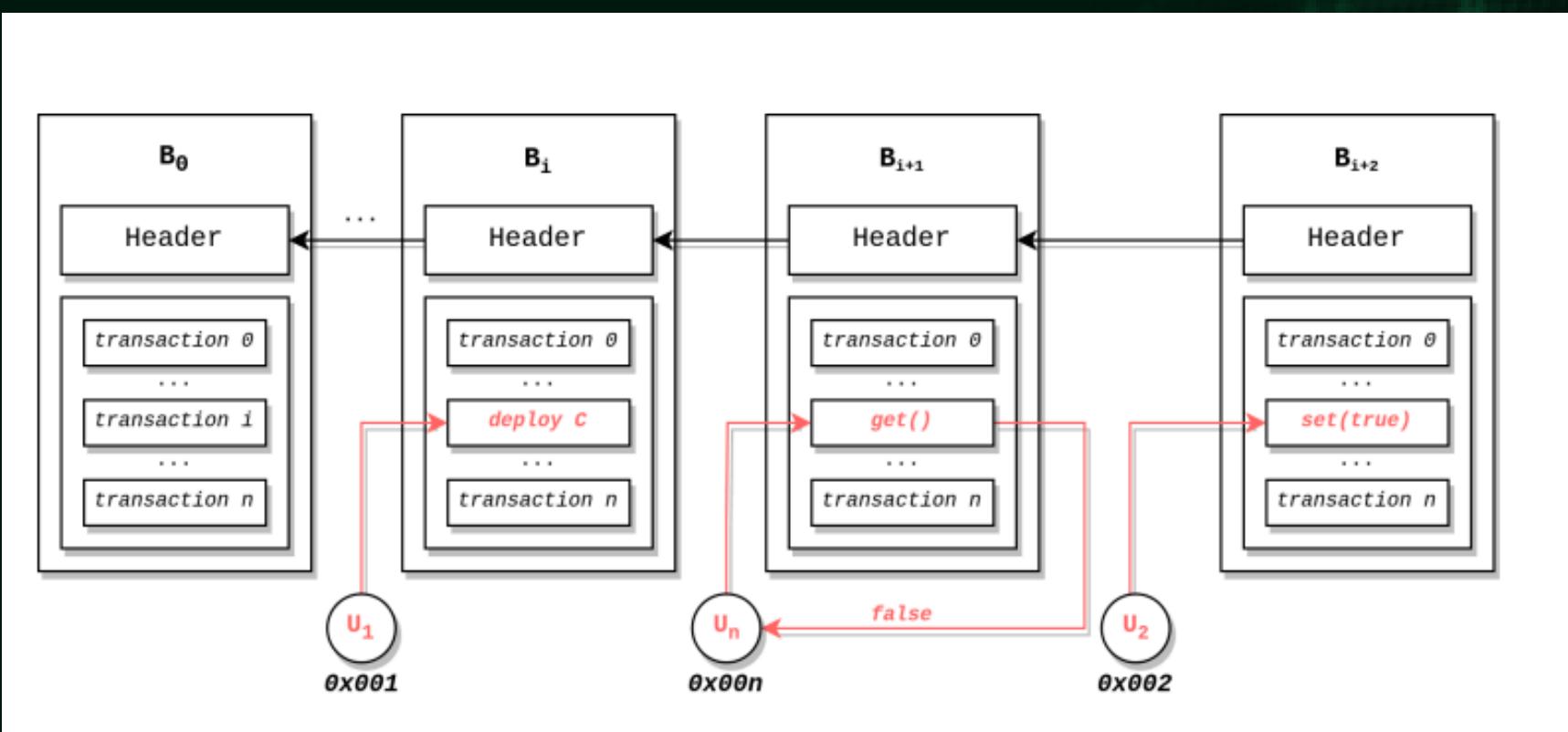


CONTRATOS INTELIGENTES

Algumas blockchains mais modernas como Ethereum possuem suporte a **Smart Contracts**.

Simplificadamente contratos inteligentes são códigos que rodam e ficam armazenados dentro da blockchain. No caso do Ethereum esses códigos são escritos em **Solidity**.

Esses códigos são executados através das EVMs (Ethereum Virtual Machines), que são um conjunto de computadores participantes da rede que rodam o código em conjunto



<https://repositorio.ufsc.br/bitstream/handle/123456789/263443/PGCC1284-T.pdf?sequence=-1&isAllowed=y>

BORA INTERAIR COM UM CONTRATO



Crie uma conta e adicione a extensão no navegador em:
<https://metamask.io/>

Minere uns Ethereum Sepolia em:
<https://sepolia-faucet.pk910.de/>



Abra Remix IDE EM:
<https://remix.ethereum.org/>

- Conecte sua metamask
- Copie o arquivo abi
- Coloque o endereço do contrato
- Interaja com o contrato



Copie o endereço do contrato e arquivo .abi em:
<https://github.com/viniciusSt1/SIC-CRIPTOGRAFIA-BLOCKCHAIN>



VALEU