# A Matemática Discreta Por trás do Bitcoin: Blockchain

**Universidade Federal de Santa Catarina**

**Disciplina: Matemática Discreta**

Artur de Faria Rodrigo

Mathias Petry Peixoto

Daniela Oliveira Ambrosio

UFSC

# O Que é Blockchain?

- Criado em 2008 por Satoshi Nakamoto
- Foi apresentado como um conceito para possibilitar a existência do Bitcoin
- É um registro digital descentralizado, imutável e transparente que armazena informações em blocos interligados em uma cadeia cronológica
- Em vez de depender de uma autoridade central, como um banco, a validação e a segurança das transações são realizadas por uma rede de participantes, tornando a tecnologia segura e confiável para diversas aplicações além das criptomoedas.

# Função Hash Dentro do Blockchain

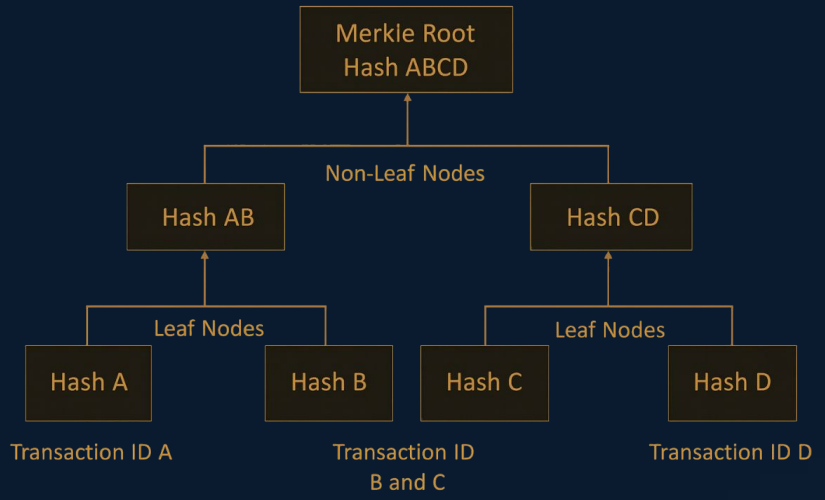
- Serve como a corrente dos blocos
- A versão usada é a SHA256
- Utiliza de dados como o Nonce, merkle root, hash do block anterior, timestamp e outros
- *Hash do bloco = SHA256(SHA256(cabeçalho do bloco)*
- Permite o blockchain ser seguro, irreversivel e imutavel.

**Imagem Ilustrativa:**

# Discreta dentro da Hash em Blockchain

## Merkle root:

- É o resumo criptográfico único de todas as transações em um bloco de blockchain




## Influência da aritmetica modular:

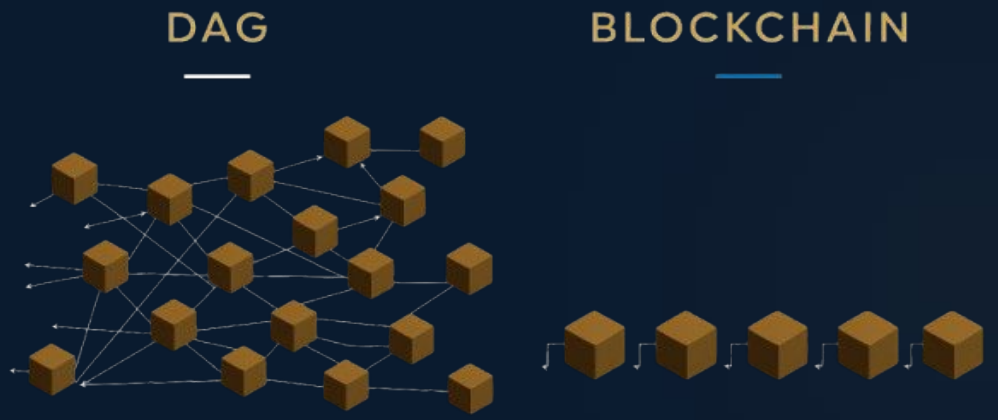
- Dentro das funções hash, à uma influência da aritmética modular, que faz com que qualquer mudança no cabeçalho produza uma hash muito diferente.

## Colisões:

- Algo inevitável matematicamente pelo princípio de Pombal, já que o domínio é infinito e o número de saídas é limitado ($2^{256}$)

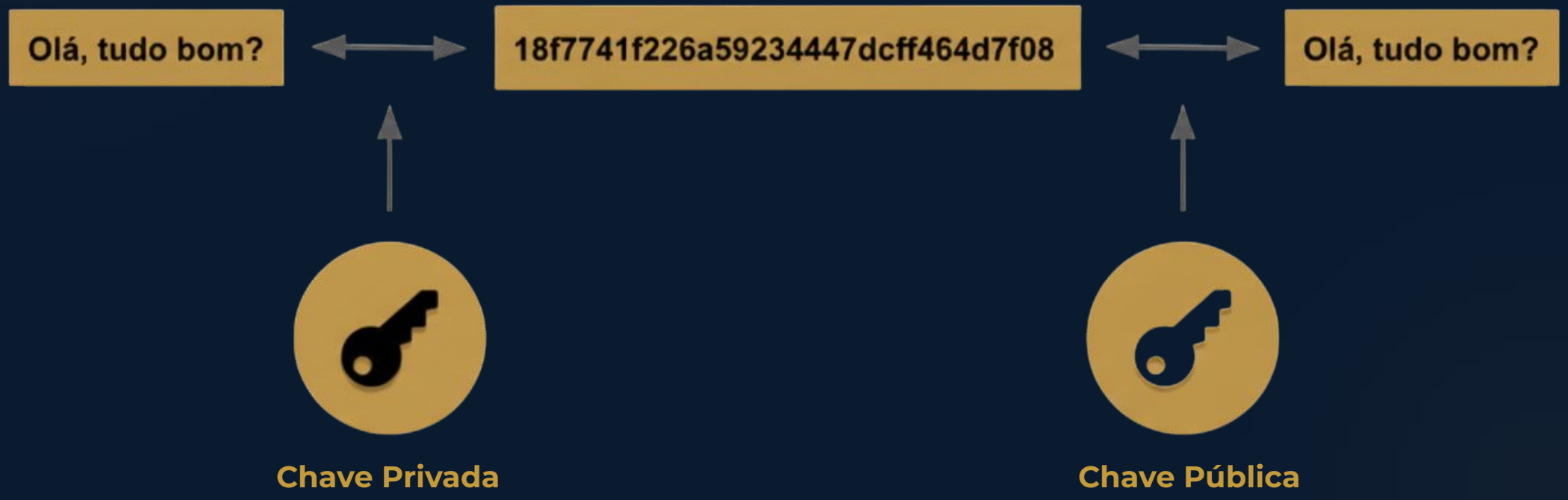
## Representação em grafos:

- O Blockchain pode ser representado como um DAG(Grafo Acíclico Dirigido).

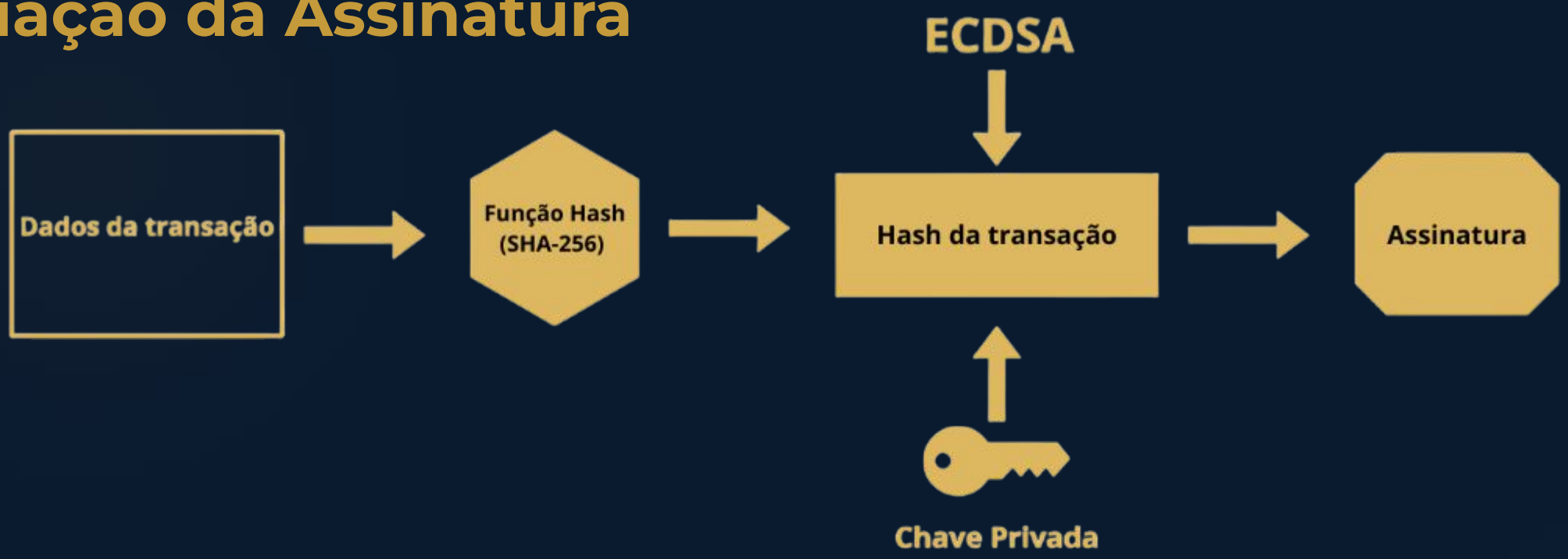


# O Que Garante a Segurança das Transações?

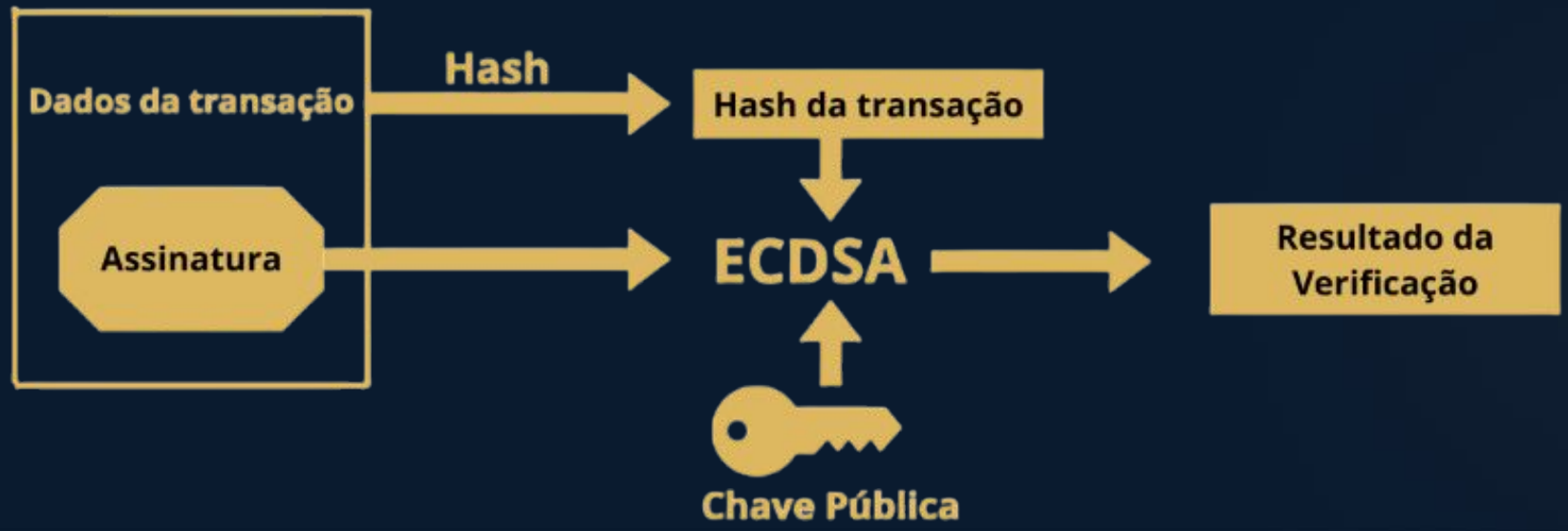
- Geração das chaves por meio do ECDSA - secp256k1



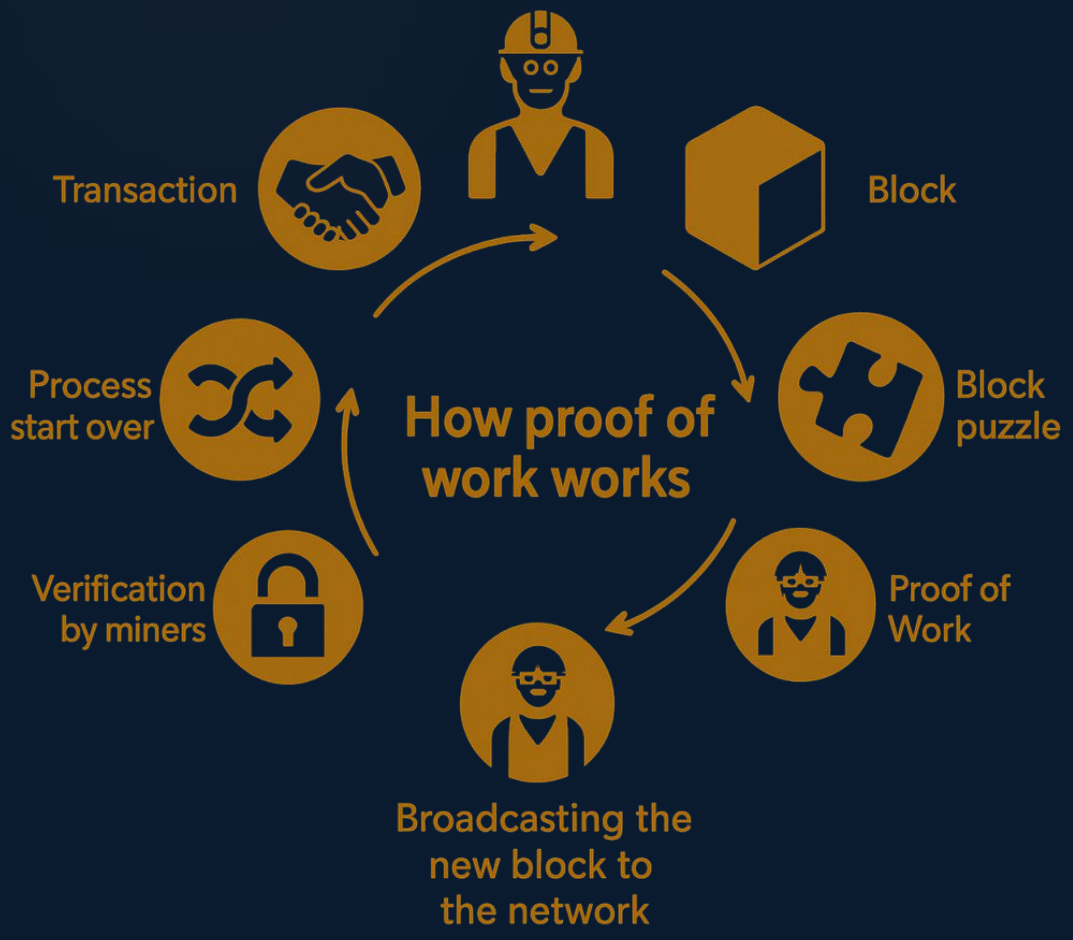
# Criação da Assinatura




# Verificação



# Prova de Trabalho (Proof of Work)




- Mecanismo de consenso utilizado na blockchain do Bitcoin
- Consome muitos recursos energéticos
- Contribui para um sistema descentralizado

# Qual a Probabilidade de Resolver o Desafio Matemático?

- A dificuldade probabilística de encontrar o nonce é o que garante o consenso da rede.
- Um bloco novo deve ser minerado a cada 10 minutos
- O Nonce é limitado a 32 bits (+4BI de possibilidades)

**Supondo que nosso desafio exigisse um hash pequeno, contendo 30 zeros a esquerda:**

Ledger

Alice pays Bob 20 LD

Alice pays You 30 LD

Charlie pays You 100 LD

1073765433

"Proof of work"

SHA256

PROBABILIDADE: $\frac{1}{2^{30}} \approx \frac{1}{1{,}000{,}000{,}000}$

30 zeros

000000000000000000000000000001
001100010110111011001000011101
100000000100011001011011010000
101111111001110001100101011100
110110111011100101011011000010
000111100010000010001001000010
111001110001101000011001001010
100001011000100110100001000000

Input

```
versao=0x20000000 |
hash_anterior=00000000000000000a1b2c3d4e5f67890abcdeffedcba0987654321ffeeddcc |
merkle_root=3f9ac1d47b82e0f6a99dc4aa77bb22c1998a0f0de34b5678c1d2e3f4a5b6c7d8 |
timestamp=2025-11-22T20:30:00Z | alvo(bits)=1d00ffff | nonce=

tx1: txid=3f9ac1d4...b6c7d8 | Alice → Bob: 0.15000000 BTC (taxa: 0.00010000 BTC)
tx2: txid=ab12ef34...90d1e2 | Carla → Diego: 0.82000000 BTC (taxa: 0.00020000 BTC)
tx3: txid=55aa9911...cc33dd | Bruno → ExchangeX: 0.05000000 BTC (taxa: 0.00005000 BTC)
tx4: txid=0f1e2d3c...4b5a69 | MinerPool123 → João: 0.30000000 BTC (taxa: 0.00015000
BTC)
tx5: txid=deadbeef...c0ffee | Maria → LojaOnline: 0.01000000 BTC (taxa: 0.00001000
BTC)
```

Output

```
51c72aeabc20fad5e00d36bbd1a3e5650c5c7e4ffc5e5ef78bfe536aed140b52
```

# Referências Bibliográficas:


MASSACHUSETTS INSTITUTE OF TECHNOLOGY. 15.S12 Blockchain and Money — Fall 2018. Disponível em: http://www.youtube.com/playlist?list=PLUl4u3cNGP63UUkfL0onkxF6MYgVa04Fn. Acesso em: 7 nov. 2025.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. [S.l.: s.n.], 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 7 nov. 2025.

RIBEIRO, L. Introdução à Blockchain e Contratos Inteligentes: apostila para iniciantes. Relatório Técnico – INE/UFSC, Florianópolis, 2021. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/221495/RT-INE2021-1.pdf. Acesso em: 7 nov. 2025.

SORIA, J. Optimal mining in proof-of-work blockchain protocols. Future Generation Computer Systems, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S1544612322007863. Acesso em: 12 nov. 2025.
SONG, J. Programming Bitcoin. [S.l.: s.n.], [20--]. Disponível em: https://cdn.bookey.app/files/pdf/book/en/programming-bitcoin.pdf. Acesso em: 7 nov. 2025.

VILA REAL, Sérgio. Funções hash na blockchain [vídeo]. Disponível em: https://www.youtube.com/watch?v=H5__Qgtlg6k. Acesso em: 7 nov. 2025.