STARK INDUSTRIES

# CONSENSO

## SISTEMAS DISTRIBUÍDOS

Sérgio Caetano
Luiz Carlos

Luan César
João Victor

JUNE 2023

STARK INDUSTRIES

# Consenso em Sistemas Distribuídos

## O que é?

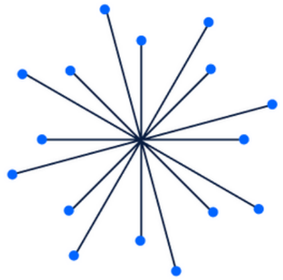
É um acordo coletivo onde os nós de um Sistema Distribuído concordam sobre o estado de um dado.

## Onde é usado?

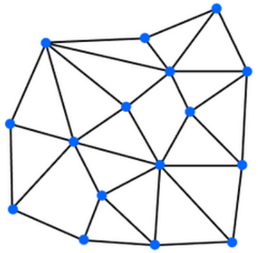
- Blockchain
- Replicação de BD
- Eleição de líder
- Exclusão Mútua
- Banco de Dados Distribuído
- Transações de BD

...

# Mecanismos de Consenso



**Leader-Based**



**BFT-Based**

**01** **Acordo**

Os nós honestos decidem pelo mesmo valor

**02** **Terminação**

Todos os nós honestos terminam a execução e chegam a um consenso

**03** **Validade**

O valor acordado ao final do consenso deve ser igual ao valor proposto inicialmente por pelo menos um nó

**04** **Tolerância a Falhas**

O algoritmo de consenso deve funcionar mesmo na presença de nós maliciosos

**05** **Integridade**

Deve ser realizado apenas um ciclo, ou seja nenhum nó deve tomar a decisão duas vezes

STARK INDUSTRIES

# Problema dos Generais Bizantinos

01 Todos devem atacar para vencer

02 O General inicia enviando a ordem de ataque ou de fuga

03 Possibilidade de falhas arbitrárias

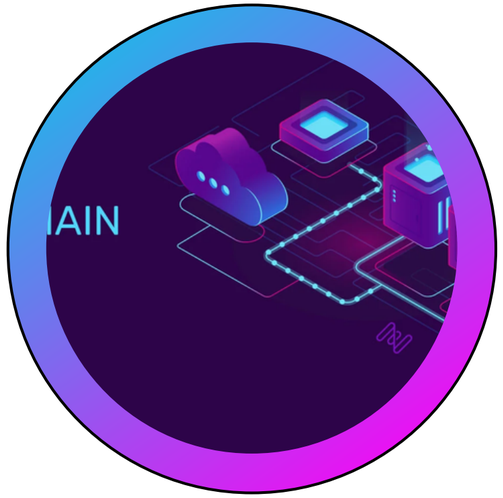
04 Canal de comunicação é seguro

STARK INDUSTRIES

# Tolerância a falhas bizantinas (BFT)

É um sistema que consegue chegar ao consenso mesmo com a presença de nós maliciosos (nós bizantinos)

Problema resolvido por Barbara Liskov e Miguel Castro. Criação do algoritmo Practical Byzantine fault tolerance.




# Algoritmos de Consenso

01 Proof of Work

02 Proof of Stake

STARK INDUSTRIES

# Proof-of-Work

01 Novas transações são transmitidas para todos os nós. (Broadcast).

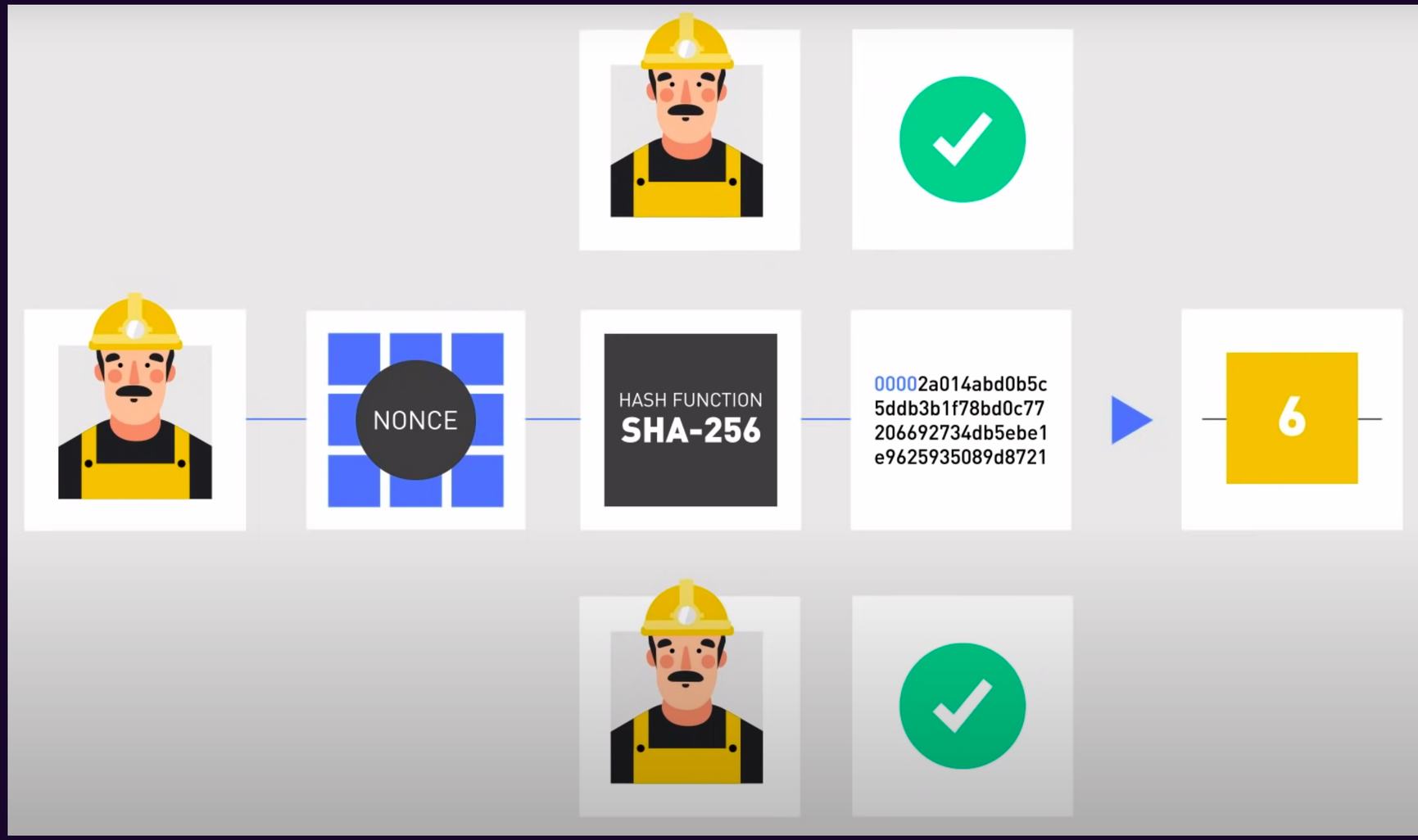
02 Cada nó coleta novas transações em um bloco.

03 Cada nó trabalha para encontrar uma prova de trabalho difícil para o seu bloco.

04 Quando um nó encontra uma prova de trabalho, ele transmite o bloco para todos os nós.

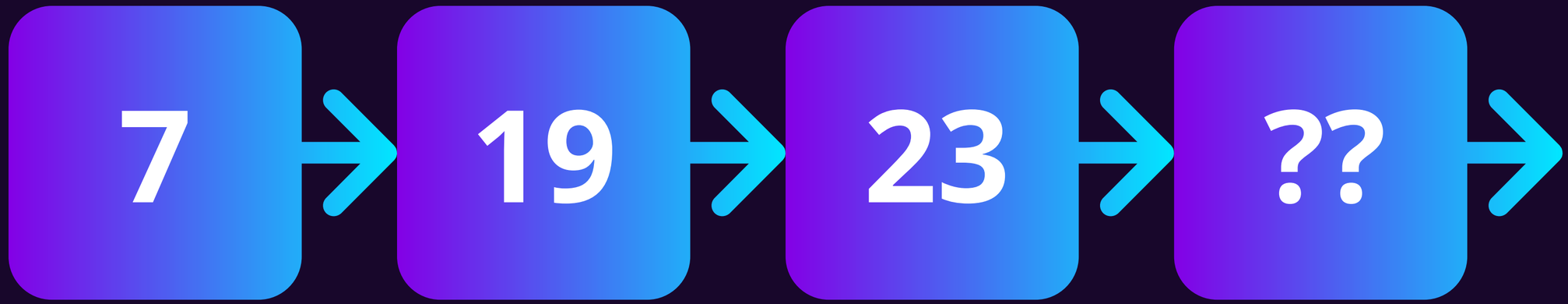
05 Os nós aceitam o bloco apenas se todas as transações nele forem válidas e ainda não tiverem sido gastas.

06 Os nós expressam sua aceitação do bloco trabalhando na criação do próximo bloco na cadeia, usando o hash do bloco aceito como hash anterior.



STARK INDUSTRIES

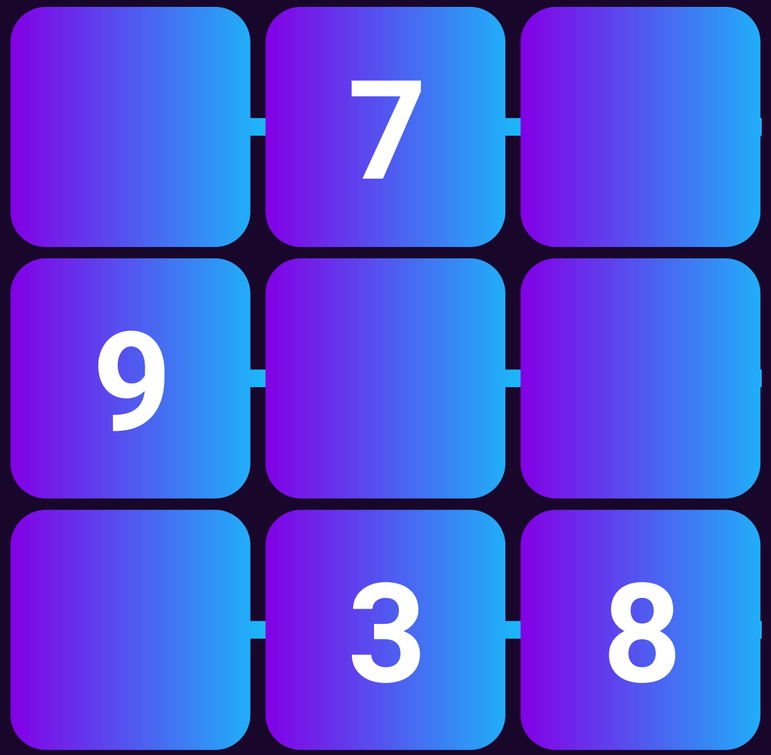
# Proof-of-Work




**Escolha um número primo maior que 23.**

STARK INDUSTRIES

# Proof-of-Work: Soma 15



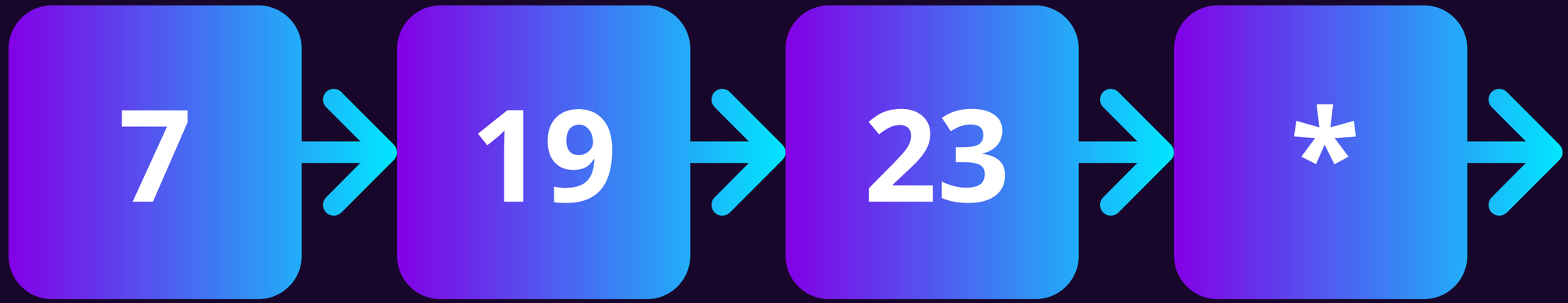

1 2 4 5 6

STARK INDUSTRIES

# Solução

STARK INDUSTRIES

# Proof-of-Work




**Insere o número primo escolhido, junto com o resultado do desafio**

01 Se a solução estiver incorreta, os outros nós rejeitam o bloco.

02 Se o valor não for primo, os nós rejeitam o bloco.

STARK INDUSTRIES

# Proof-of-Stake

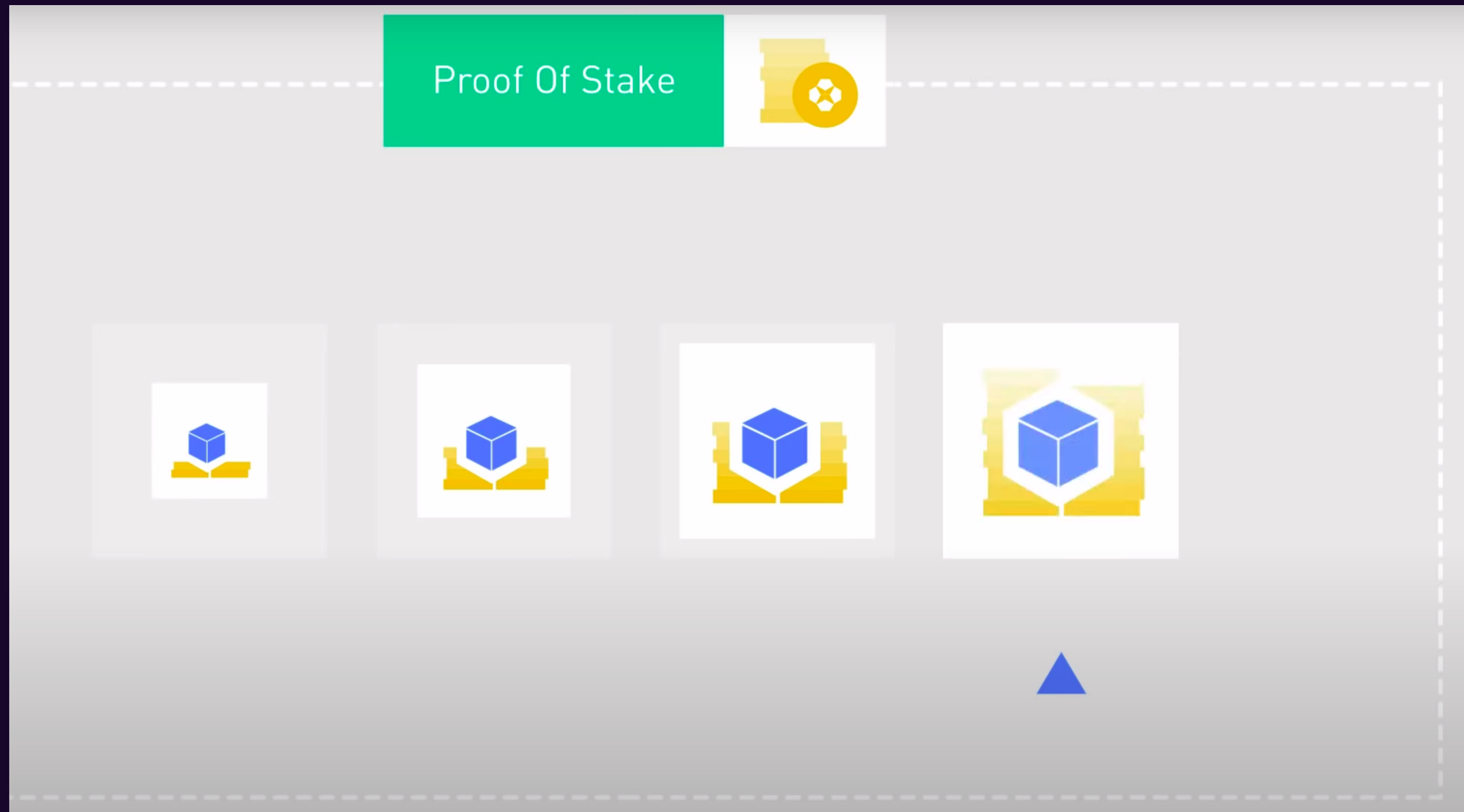
01 Direito de validar blocos e adicionar transações à blockchain com base na participação de moedas que um indivíduo possui.

02 Probabilidade de selecionar o nó baseado na quantidade de moedas separadas para staking.

03 Existem variantes que implementam randomização e Coin Age para não beneficiar apenas os nós mais ricos

04 Mais energeticamente eficiente que o Proof-of-work

05 O nó pode perder parte de suas moedas se tentar validar um bloco com transações falsas, além de perder o direito de validar transações.



# Referências

[1] Xiao, Yang, et al. "A survey of distributed consensus protocols for blockchain networks." IEEE Communications Surveys & Tutorials 22.2 (2020): 1432-1465.

[2] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008): 21260.

[3] Mingxiao, Du, et al. "A review on consensus algorithm of blockchain." 2017 IEEE international conference on systems, man, and cybernetics (SMC). IEEE, 2017.

[4] Bashir, Imran. Mastering blockchain. Packt Publishing Ltd, 2017.

[5] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine generals problem." Concurrency: the works of leslie lamport. 2019. 203-226.

[6] Castro, Miguel, and Barbara Liskov. "Practical byzantine fault tolerance." OsDI. Vol. 99. No. 1999. 1999.