

Algoritmos de Consenso em Blockchain

Acquila Santos Rocha

Sistemas Distribuídos

01 de Maio de 2021

Agenda



1. Introdução

2. Consenso Distribuído

- Introdução
- Proof of Work - PoW
- Proof of Stake - PoS
- Practical Byzantine Fault Tolerance - pBFT
- Delegated Practical Byzantine Fault Tolerance - dpBFT

3. Comparativo

4. Referências



Introdução

O que é Blockchain?



Blockchain é uma tecnologia que provém uma base de registros distribuída denominada *ledger*, composta por blocos de transações.

Características gerais

1. Cada bloco possui três seções principais: dados, hash e hash do bloco anterior.
2. O primeiro bloco é chamado **Bloco Gênesis**.
3. O hash determina a identidade de cada bloco como uma impressão digital e é exclusivo para cada bloco.
4. O campo de dados é composto por um conjunto de dados.

Estrutura da Blockchain

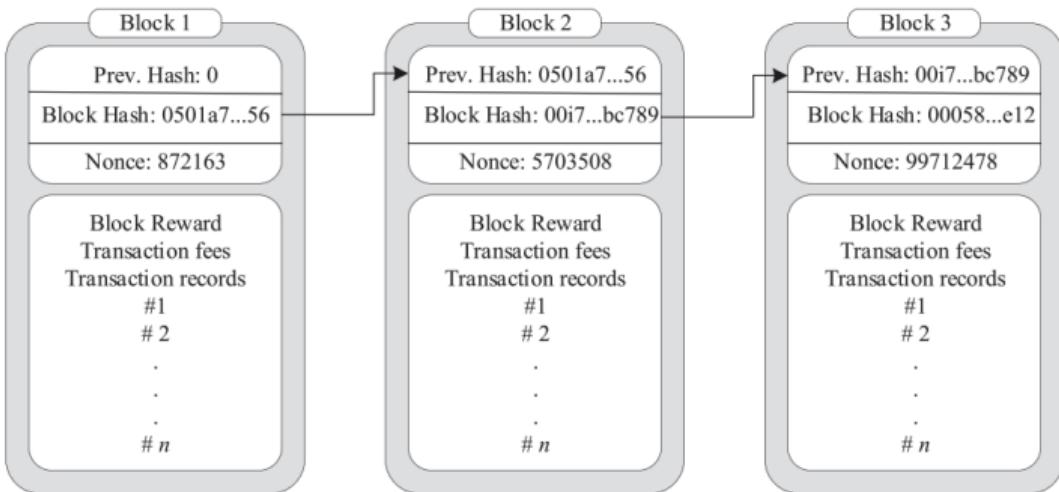


Figure 1: Estrutura da blockchain [Bamakan et al., 2020]

Categorias da Blockchain



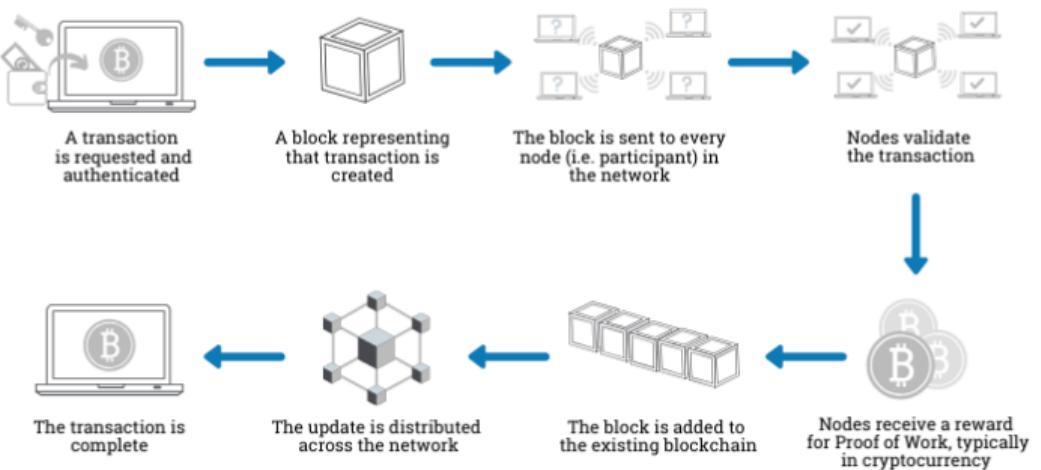
Tipos

1. **Blockchain Pública:** descentralizada e sem permissão. As informações estão disponíveis para todos os membros da rede e todos podem participar do consenso.
2. **Blockchain por Consórcio:** É apresentável para todas as pessoas, mas a manipulação do *ledger* é limitada para determinados grupos;
3. **Blockchain Privada:** As informações da blockchain são apresentadas somente a um grupo especial e sua manipulação só é permitida por um grupo autorizado de peers.

Caso de uso: Bitcoin [Nakamoto, 2019]



How does a transaction get into the blockchain?





Consenso Distribuído

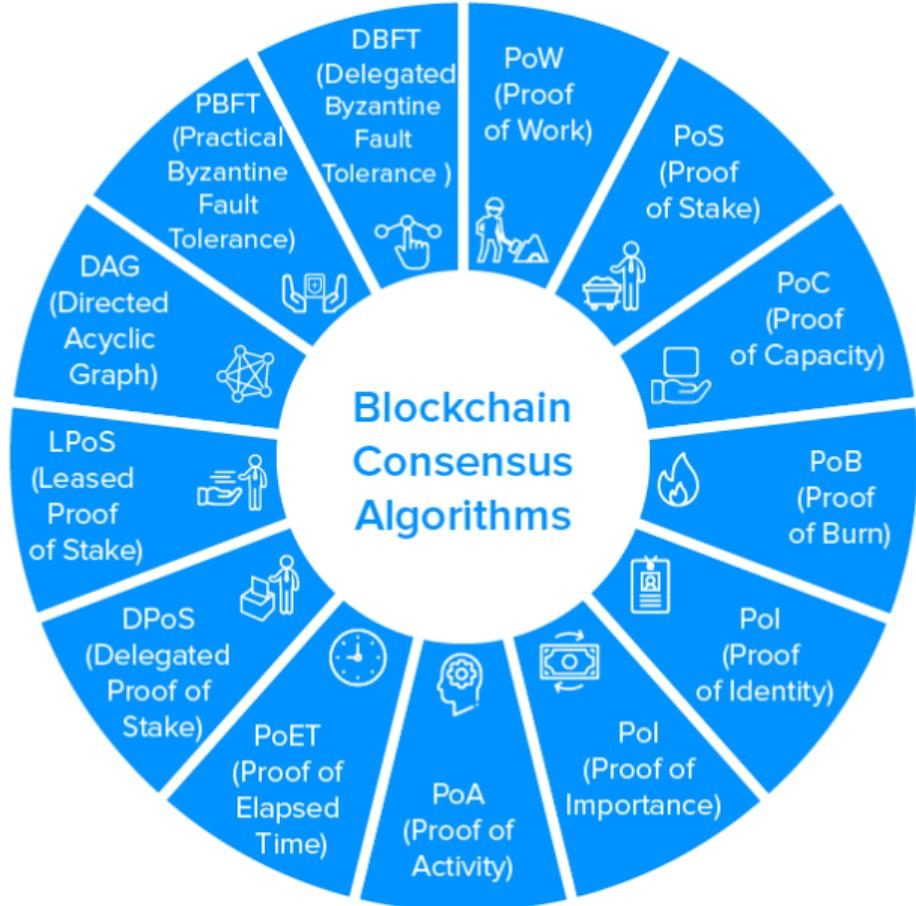
Introdução



O que é?

- É utilizado para preservar o **acordo** entre os nós da rede [Bamakan et al., 2020].
- Por ser um sistema dinâmico e autorregulado, a *blockchain* requer a incorporação de um mecanismo seguro para garantir a autenticidade das transações, fazendo com que os participantes cheguem a um **consenso** [Lashkari and Musilek, 2021].

O blockchain público requer a participação de usuários para verificação e autenticação das transações.



Proof of Work - PoW

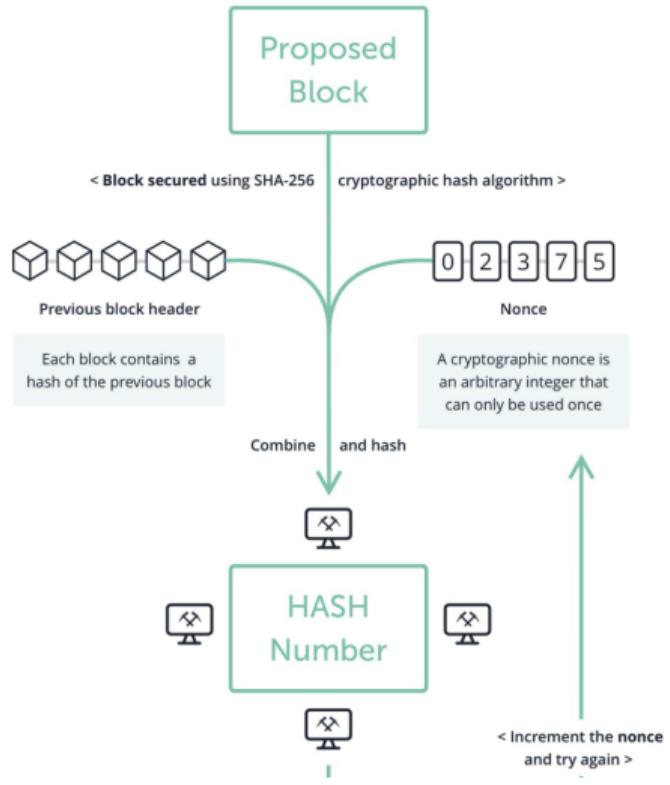


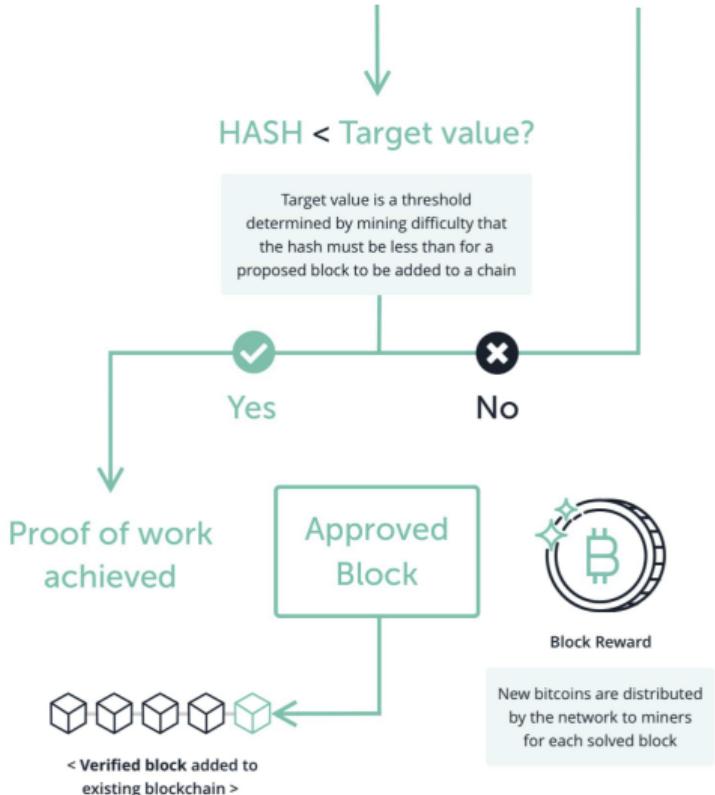
Características

Cada nó da rede calcula um valor de *hash* (nonce) do cabeçalho do bloco. Os mineradores tentam encontrar um valor de *hash* igual ou menor ao nonce.

Desvantagem

Apesar de fornecer alta segurança e descentralização, a mineração e validação dos blocos gasta muita energia [Bamakan et al., 2020].





Proof of Stake - PoS

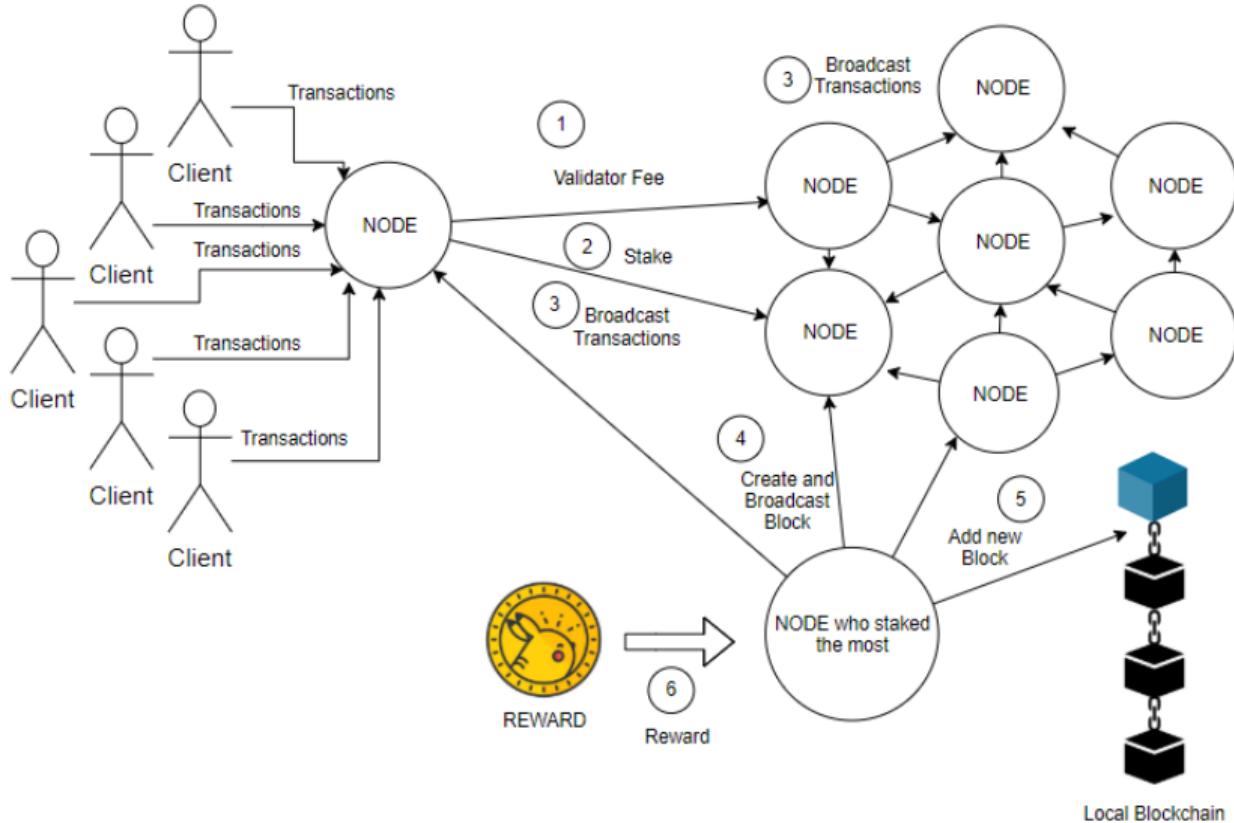


Características

O nó selecionado para minerar o próximo bloco, é escolhido por meio de um processo no qual a seleção depende dos ativos armazenados na carteira (ou pool de ações) dos nós.

Desvantagem

Embora este método não apresente alto consumo de energia, ele depende fortemente dos nós com mais "interesse" e a blockchain acaba se tornando centralizada [Bamakan et al., 2020].



Practical Byzantine Fault Tolerance - pBFT



Características

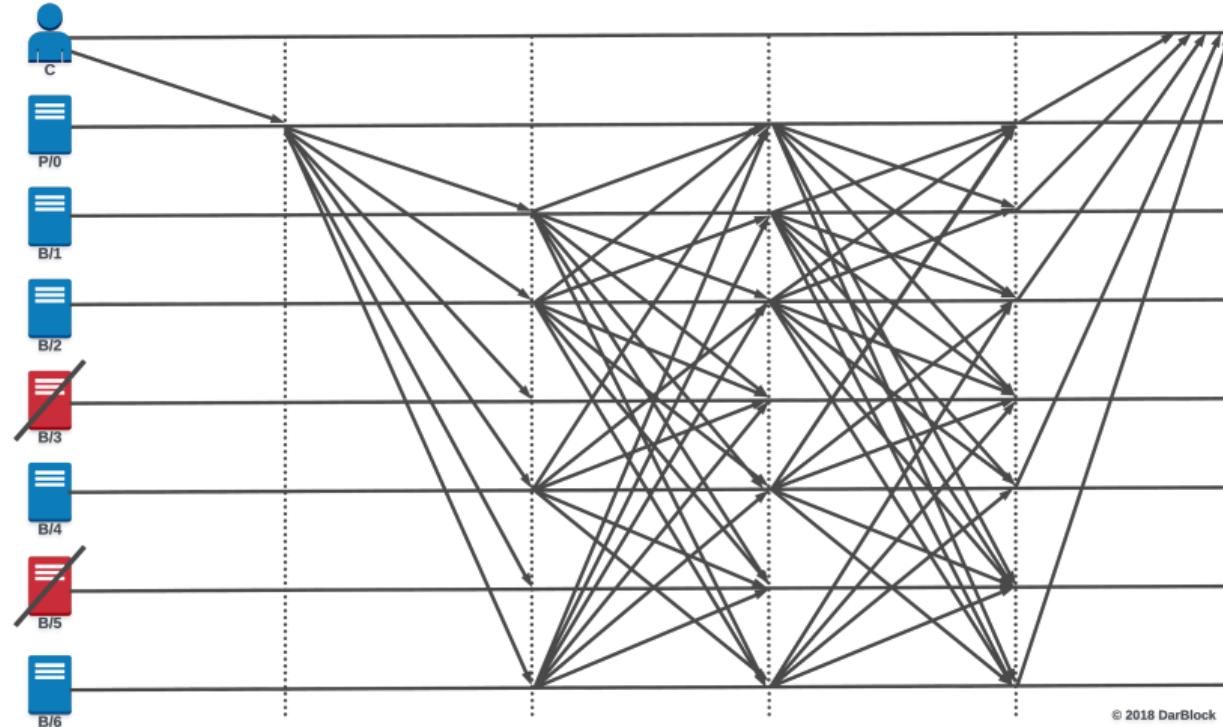
Este método de consenso é usado para resolver o problema geral bizantino. Ataques maliciosos e erros de software podem ser resultado de um comportamento arbitrário (Bizantino) de nós com defeito. Neste método, todos os nós devem participar de um processo de votação para adicionar o próximo bloco, e o consenso é alcançado quando mais de dois terços dos nós têm uma opinião favorável à criação bloco.

Desvantagem

O principal problema deste método é a possibilidade de atraso, visto que todos os nós devem votar.

pBFT Message Count

	request	pre-prepare	prepare	commit	reply
min	1	3f	$3f(3f-f)$	$(3f-f+1)(3f+1)$	$3f-1$
max	1	3f	$(3f)^2$	$3f(3f+1)$	$3f+1$



Delegated Practical Byzantine Fault Tolerance - dpBFT



Características

Este método segue as regras do PBFT, mas não requer a participação de todos os nós no processo de votação para inclusão de um novo bloco. Vários nós são selecionados como representantes de outros nós e, com base em uma série de regras, seguem um processo de consenso como o método PBFT.

Desvantagem

É menos provável que sofra atrasos do que o PBFT, mas limitar o número de eleitores pode ameaçar a descentralização da rede.



Comparativo

Tabela comparativa



	PoW	PoS	PBFT
(i) Categoria	Pública	Ambos	Privado
(ii) TPS	Baixo	Alto	Alto
(iii) Escalabilidade	Alta	Alta	Baixa
(iv) Custo	↑	↓	↓
(v) Cryptocurrencies	Bitcoin Ethereum Litecoin	Blackcoin Nxt	Ripple Stellar

Table 1: Tabela de comparações entre os diferentes mecanismos de consenso.
Adaptado [Lashkari and Musilek, 2021]

Referências I

-  **Bamakan, S. M. H., Motavali, A., and Babaei Bondari, A. (2020).**
A survey of blockchain consensus algorithms performance evaluation criteria.
Expert Systems with Applications, 154:113385.
-  **Lashkari, B. and Musilek, P. (2021).**
A comprehensive review of blockchain consensus mechanisms.
IEEE Access, 9:43620–43652.
-  **Nakamoto, S. (2019).**
Bitcoin: A peer-to-peer electronic cash system.
Technical report, Manubot.

Obrigado

Dúvidas?

acquila.santos@gmail.com



INSTITUTO DE
INFORMÁTICA
UFG

