Hash Tree aplicada ao Blockchain

AAED - Alexandre Ferreira

12 de novembro de 2024

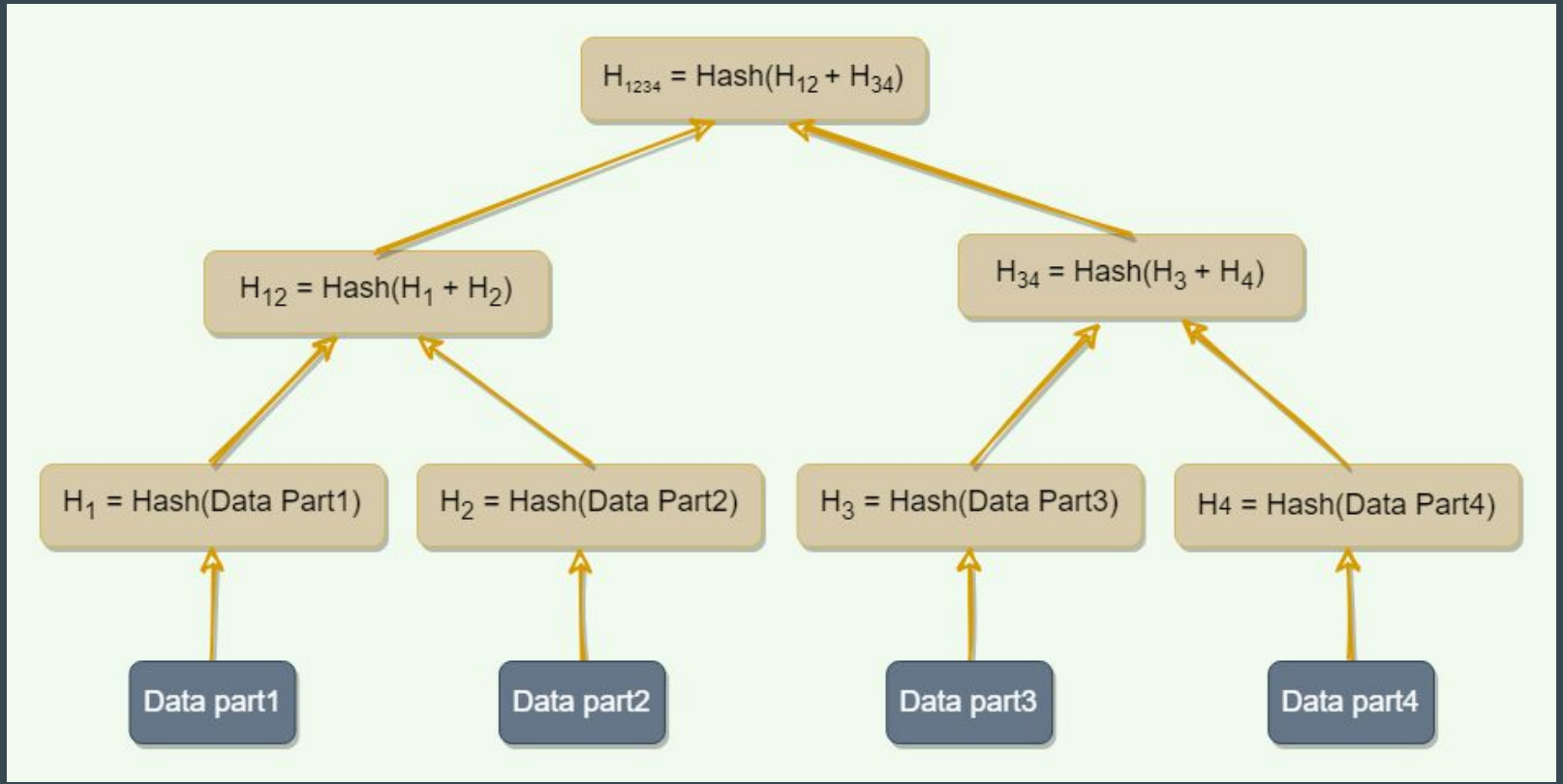
Definição

- Também conhecida como Árvore de Merkle
- Estrutura em árvore que permite verificar a integridade e a consistência de dados em grandes volumes de informação
- Amplamente utilizada em blockchain, e sistemas de arquivos distribuídos, e redes P2P

Estrutura

- Nodos Folha - Os dados são divididos em blocos e transformados hash
- Nodos Intermediários - Cada par de nodos folha é combinado e gerado um novo hash
- Cada nodo na árvore é um hash
- A raiz de Merkle é o hash que representa todo o conjunto de dados.

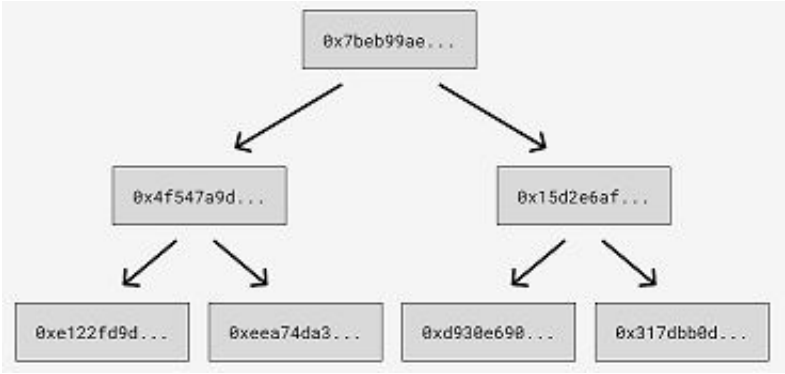
Estrutura



fonte: www.designgurus.io

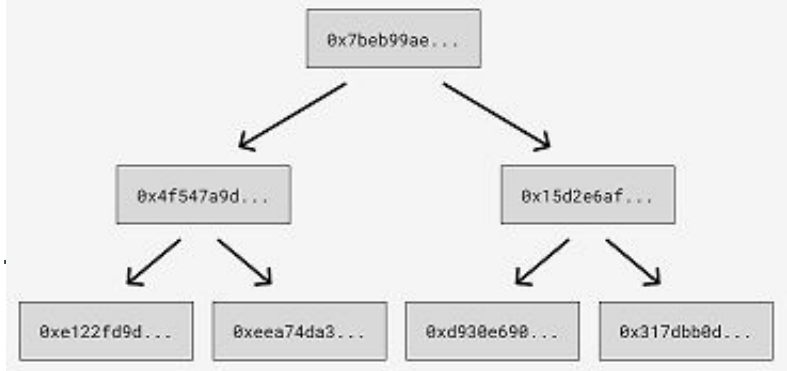
Funcionamento

- Um grande arquivo é construído a partir de vários blocos
- A integridade de um bloco poderá ser verificada a partir do caminho hash até a raíz.



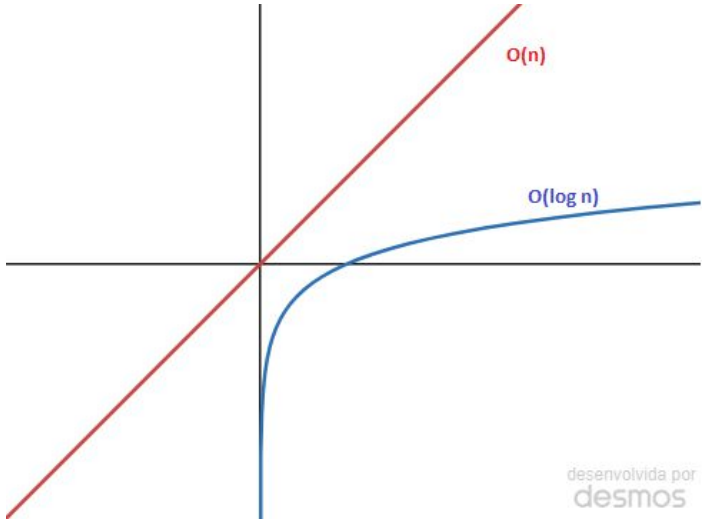
Vantagens

- Eficiência: Verifica-se a integridade de um bloco sem precisar verificar o conjunto inteiro de dados.
- Escalabilidade: Muito útil em sistemas distribuídos, onde diferentes partes da árvore podem ser armazenadas em locais diferentes.
- Segurança: Alterações em qualquer bloco da árvore mudarão o hash correspondente, sendo detectadas pela comparação com a raiz.

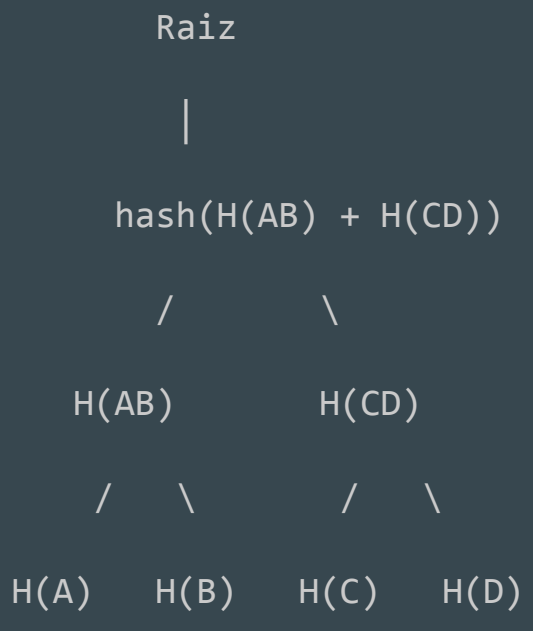


Complexidade

- Para Construção → O(n). Pois n folhas precisam ser processadas e o hash é aplicado a cada uma.
- Verificar Bloco → O(log n). Por causa da altura da árvore que é O(log n). Precisa-se calcular o hash em cada nível até a raiz.



Exemplo SHA-256




```
bloco A -> f3497207237fe7561d45dedcf193a63d3bfb813cae792a3b6ce2e538bb1ed874
bloco B -> 2b7ee8d2f83aac2ed9ef9a15bf2494aed9be3977611e004bd08fdc799806da58
bloco C -> 9b41c89ad146b8a13f94b3f28c0d90d051d5ab5950c147cae83e8c8246ef1083
bloco D -> 3f25c9464a5ecafe0e94188a26150b2271bcd631dc5fec4ad3d81caedb614886

f3497207237fe7561d45dedcf193a63d3bfb813cae792a3b6ce2e538bb1ed8742b7ee8d2f83a
ac2ed9ef9a15bf2494aed9be3977611e004bd08fdc799806da58 ->
dc4db1ca3e3f92c764bd349976cf6d7effa8dc4f5bee636e7987d5624f6bb242

9b41c89ad146b8a13f94b3f28c0d90d051d5ab5950c147cae83e8c8246ef10833f25c9464a5e
cafe0e94188a26150b2271bcd631dc5fec4ad3d81caedb614886 ->
fde7e1f0c6ad35cc01dd3a2a053d791b25a4e0ecd3538e62ea553c79c2c710d0

dc4db1ca3e3f92c764bd349976cf6d7effa8dc4f5bee636e7987d5624f6bb242fde7e1f0c6ad
35cc01dd3a2a053d791b25a4e0ecd3538e62ea553c79c2c710d0 ->
eb97179383cc5e0de523ea0cad1159437bac5fb204b25c760f771ab4e656b24a

RAIZ eb97179383cc5e0de523ea0cad1159437bac5fb204b25c760f771ab4e656b24a
```

Aplicação Real

- O Hyperledger Fabric é uma excelente escolha para desenvolvedores interessados em construir redes blockchain robustas e customizáveis para aplicações empresariais.
- Código no GitHub
- Mantido pela Linux Foudation
- É amplamente utilizado em áreas como cadeia de suprimentos, finanças, seguros e saúde para fornecer rastreabilidade, transparência e auditoria dos processos.

Aplicação Real

HYPERLEDGER FABRIC

Hyperledger Fabric Docs

Search docs

HYPERLEDGER FABRIC

Introduction

What's new in Hyperledger Fabric v2.x

Release notes

Key Concepts

Introduction

What is a Blockchain?

Why is a Blockchain useful?

What is Hyperledger Fabric?

Hyperledger Fabric Model

How Fabric networks are structured

Identity

Membership Service Provider (MSP)

Policies

Peers

Ledger

The Ordering Service

Smart Contracts and Chaincode

Fabric chaincode lifecycle

Private data

Channel capabilities

Security Model

Use Cases

Getting Started - Install

Getting Started - Run Fabric

Tutorials

Key Concepts / Introduction

View page source

Introduction

Hyperledger Fabric is a platform for distributed ledger solutions underpinned by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility, and scalability. It is designed to support pluggable implementations of different components and accommodate the complexity and intricacies that exist across the economic ecosystem.

We recommend first-time users begin by going through the rest of the introduction below in order to gain familiarity with how blockchains work and with the specific features and components of Hyperledger Fabric.

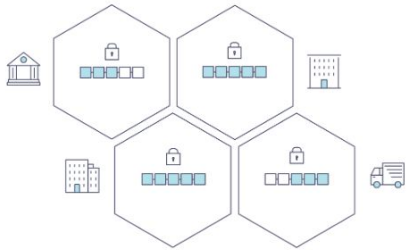
Once comfortable — or if you're already familiar with blockchain and Hyperledger Fabric — go to Getting Started - Install and from there explore the demos, technical specifications, APIs, etc.

What is a Blockchain?

A Distributed Ledger

At the heart of a blockchain network is a distributed ledger that records all the transactions that take place on the network.

A blockchain ledger is often described as **decentralized** because it is replicated across many network participants, each of whom **collaborate** in its maintenance. We'll see that decentralization and collaboration are powerful attributes that mirror the way businesses exchange goods and services in the real world.



Referências

- https://github.com/hyperledger/fabric
- https://hyperledger-fabric.readthedocs.io/en/release-2.5/blockchain.html
- ChatGPT

Muito Obrigado

Alexandre Ferreira

Engenheiro de Software,
Engenheiro Mecânico.
Projetista de robôs e aluno
especial da Unifesp