



Resumo: Blockchain GoLedger

Módulo 3

Gabriel dos Santos Schmitz

Novembro 2024

This document provides an in-depth overview of Hyperledger Fabric, a permissioned blockchain framework tailored for enterprise applications. It explores key components such as the Orderer, responsible for transaction ordering and network consensus; the Certification Authority (CA), which manages permissions through digital certificates; and the Membership Service Provider (MSP), ensuring secure authentication. The analysis covers the functionality of Chaincodes as smart contracts for asset management and the role of Clients in facilitating external interactions with the blockchain. Emphasis is placed on privacy features like Private Data Collections, enabling selective data sharing among organizations while maintaining transparency through cryptographic validation. The document concludes by highlighting the framework's flexibility in governance and detailed permission control, making it a robust solution for complex business networks.

Gabriel dos Santos Schmitz: UTFPR. Eu agradeço colegas e orientador por comentários e discussões úteis. Este trabalho foi apoiado por Grupo PQC UTFPR

1. Conceitos de Hyperledger Fabric

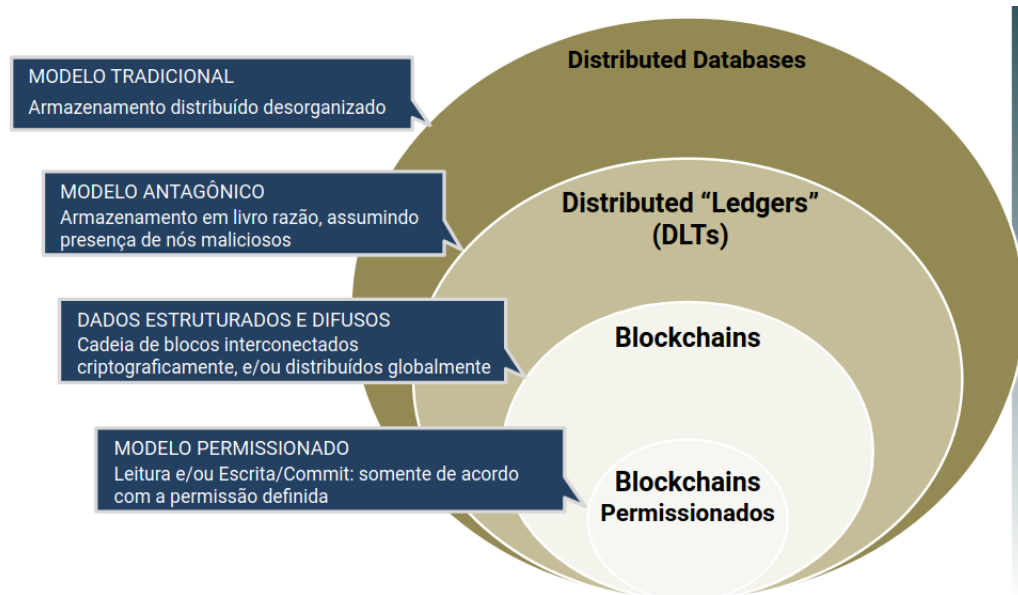


FIGURE 1. Tecnologia integrada

- . Em um blockchain não permissionado, qualquer pessoa pode criar nós na rede, identificando-se por meio de pares de chaves criptográficas geradas aleatoriamente. A rede utiliza ativos escassos, como criptomoedas, para realizar transações, possibilitando o registro de eventos entre partes desconhecidas. O uso da rede envolve custos pagos em criptomoedas, e o acesso ao ledger é feito por meio de wallets.
- . Redes de blockchain permissionado são compostas por consórcios ou reguladores, com as organizações participantes sendo identificadas criptograficamente. A entrada na rede exige autorização, exceto para os fundadores. Essas redes permitem que processos compartilhados sejam codificados em contratos inteligentes e seguidos por regras de consenso, baseadas em leis e normas. Existem diversos frameworks disponíveis para o desenvolvimento dessas redes.

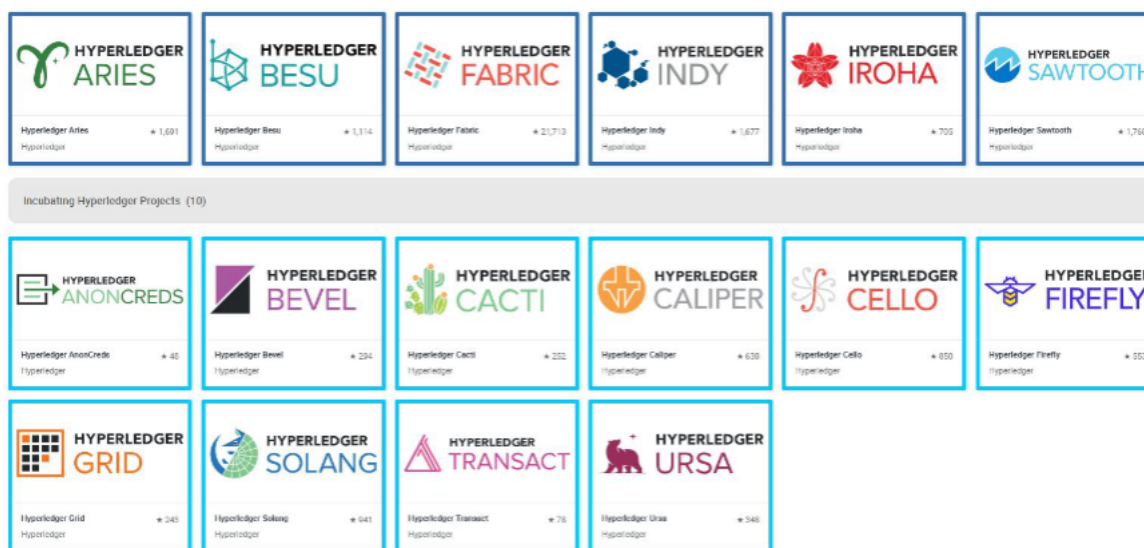


FIGURE 2. Hyperledger Foundation

- . A Hyperledger Foundation é um projeto de código aberto administrado pela Linux Foundation, focado em aprimorar tecnologias blockchain para diferentes setores empresariais. É o projeto de crescimento mais rápido na história da fundação, contando com a colaboração de empresas financeiras, bancos, IoT, logística, e indústrias tecnológicas.
- . O Hyperledger Project foi criado em 2015 com o objetivo de fomentar o uso de blockchain em ambientes empresariais e industriais. O primeiro projeto foi o Hyperledger Fabric, originalmente conhecido como OpenLedger e doado pela IBM. Os projetos da Hyperledger são categorizados em Graduados, Incubados, e Laboratório, podendo incluir frameworks, bibliotecas, ferramentas, ou clientes de acesso.

- **R1..R4:** Organizações 1 a 4 **CA1..C4:** CAs das Orgs
- **C1, C2:** Channels 1, 2 **L1, L2:** Ledgers 1, 2
- **P1..P3:** Peers das Orgs 1..3 **O4:** Ordering Service
- **S5, S6:** Chaincodes
- **A1..A3:** Clientes

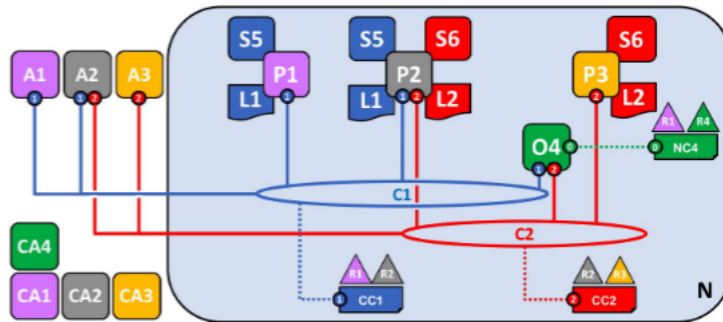


FIGURE 3. Exemplo de Rede Hyperledger Fabric

. A rede Fabric é ideal para situações que envolvem processos com múltiplas entidades ou organizações conhecidas e confiáveis, onde o registro de informações segue um sistema de credenciais hierárquicas. A governança da rede pode ser flexível, variando entre modelos democráticos e regulados, conforme a necessidade das instituições envolvidas.

2. Confiabilidade Hyperledger Fabric

. O Hyperledger Fabric utiliza o algoritmo Raft para alcançar consenso, que envolve o compartilhamento de estado entre nós com tolerância a falhas. Este modelo é semelhante ao consenso Proof of Authority, mas não é Bizantino (BFT). Os nós de ordenação são responsáveis por manter o consenso, que pode ser definido através de um chaincode ou canal. A infraestrutura também utiliza o etcd, um armazenamento chave-valor distribuído.

. No Hyperledger Fabric, a rede é permissionada, composta por consórcios ou redes de negócios, onde cada organização é representada por uma Autoridade Certificadora (CA). A confiabilidade é garantida pela comparação de informações assinadas por diferentes organizações, utilizando contratos inteligentes (chaincodes), que não são armazenados no ledger. Esse modelo se assemelha a sistemas contratuais do mundo físico, como cartórios.

. O Ethereum pode ser utilizado tanto em redes permissionadas quanto não permissionadas. Smart contracts são armazenados no ledger como bytecode, e o consenso é alcançado via PoW, PoS ou PoA, com a EVM validando o hash do bytecode antes da execução. Transações envolvem uma contagem de gas, e a reputação dos nós é utilizada nos modelos PoS e PoA, garantindo confiabilidade. Apenas o modelo PoA Clique não é BFT.

3. Componentes Hyperledger Fabric

. No Hyperledger Fabric, um Asset é um elemento compartilhado na rede, podendo ser tangível ou intangível. A rede é composta por Nodes, que são os dispositivos participantes, e utiliza um Ledger, o livro-razão das transações. A identificação dos membros é gerida pelo Membership Service Provider (MSP), enquanto a CA (Autoridade Certificadora) garante a autenticidade das identidades. A comunicação entre partes da rede ocorre através de Channels, que possuem um ledger dedicado, e os Chaincodes atuam como contratos inteligentes. A rede pode ser acessada por clientes externos, conhecidos como Clients, formando uma Business Network.

. O ledger no Hyperledger Fabric é imutável e privado, armazenando transações de configuração e de aplicação de forma cronológica. As transações podem criar, atualizar ou deletar assets, e são mantidas nos nós (peers e orderers). Um Channel é um meio de comunicação entre membros específicos da rede, definido por um conjunto de organizações, peers, um ledger, chaincodes, e nós de ordenação que asseguram as regras do canal.

. O controle de acesso é gerido através de uma Access Control List (ACL), permitindo o gerenciamento detalhado de leitura, escrita, e administração dos recursos da rede. As permissões são atribuídas por meio de Policies, como "MyPolicy", que pode permitir acesso com base nas assinaturas das organizações. As políticas podem ser aplicadas a channels, organizações, e aplicações, utilizando ferramentas como configtxgen e arquivos de configuração configtx.yaml.

. Os assets na rede podem representar elementos tangíveis ou intangíveis, armazenados em formatos binários ou JSON. Eles funcionam como entradas em uma tabela de banco de dados, com estados mantidos na rede e modificados dentro de channels. Cada asset é indexado por uma chave primária ou composta, facilitando operações de criação, modificação, e consulta no ledger.

```

1 // Description of a book
2 var Book = assets.AssetType{
3     Tag: "book",
4     Label: "Book",
5     Description: "Book",
6     Props: []assets.AssetProp{
7         {
8             IsKey: true, // Primary Key
9             Tag: "title",
10            Label: "Book_Title",
11            DataType: "string",
12            Writers: []string{'org2MSP'}, // This means only org2 can
13                                           // create the asset (others can edit)
14        },
15        {
16            Tag: "currentTenant",
17            Label: "Current_Tenant",
18            DataType: "->person", /// Reference to another asset
19        },
20        {
21            Tag: "genres",
22            Label: "Genres",
23            DataType: "[]string", // String list
24        },
25        {
26            Tag: "published",
27            Label: "Publishment_Date",
28            DataType: "datetime", // Date property
29        },
30    },
31 }

```

Listing 1. Asset Example

. Nodes são dispositivos que armazenam ledgers e contratos inteligentes na rede Hyperledger Fabric. Existem dois tipos principais de nodes: Peers, que pertencem a uma organização e mantêm cópias do ledger, e Ordering Nodes, que recebem transações, realizam o consenso, e ordenam a gravação de novos blocos. A comunicação entre nodes é realizada via protocolo GRPC com segurança TLS, e o protocolo de gossip permite comunicação Peer-to-Peer.

. Os Peers têm várias funções, como armazenar cópias do channel (ledger) e executar contratos inteligentes (chaincodes). Cada peer é identificado por um certificado digital e representa uma organização específica. Existem tipos especiais de peers, como o Anchor Peer, que comunica com outras organizações e nodes de ordenação para manter o channel sincronizado, e o Endorsement Peer, que armazena o chaincode e processa propostas de transação enviadas pelos clientes da rede. Para otimizar espaço, os peers podem utilizar snapshots do ledger.






Peer		State: CouchDb ou LevelDb
MSPs		
Ledger		
Chaincodes(endorsing)	 	

FIGURE 4. Anatomia do Peer

. O Orderer é um componente crítico no Hyperledger Fabric, responsável por garantir o consenso e o permissionamento da Business Network. Ele armazena channels, identifica permissões e valida características dos chaincodes, incluindo políticas de endosso. O Orderer recebe pacotes de transações assinadas, valida-os, organiza as transações, gera novos blocos, e os envia para os Anchor Peers, mantendo a ordem e consistência da rede.

. A Certification Authority (CA) gerencia o permissionamento da rede, representando organizações específicas por meio de uma infraestrutura PKI que utiliza certificados digitais x.509. Estes certificados são usados pelo Membership Service Provider (MSP), que abstrai o permissionamento e organiza os elementos da rede como peers, orderers, e usuários, assegurando a integridade da rede.

. Os Chaincodes são programas que realizam propostas de alterações nos assets, mas não atualizam diretamente o ledger. Cada chaincode possui uma política de endosso que define quais assinaturas são necessárias para validar uma transação. A Endorsing Policy é uma regra lógica que pode exigir assinaturas de múltiplas organizações e é aplicada para garantir a conformidade das transações.

. O Client é a interface que conecta o ambiente digital externo ao blockchain, comunicando-se com peers e orderers. Ele cria propostas de transação, recebe respostas de execução dos chaincodes e utiliza certificados digitais para autenticação. Para facilitar a comunicação, os clients utilizam um Connection Profile, um documento que descreve a configuração da rede.

. O conceito de Private Data Collection permite que certas informações dentro de um channel sejam acessíveis apenas a organizações específicas, mantendo dados sensíveis fora do ledger principal em um banco de dados transiente, como CouchDB. Os participantes de uma Business Network podem interagir utilizando os diversos componentes do Hyperledger Fabric, como channels, CAs, orderers, e clients, garantindo segurança e flexibilidade nas transações empresariais.