Enterprise Blockchain e Hyperledger Fabric
Resumo do curso

Carlos Henrique Veeck
chvmv@cin.ufpe.br

Enterprise Blockchain

- Ledger Descentralizado
    - Pode guardar qualquer tipo de dados
- Imutável
- Não Anônima
- Não Transparente para todos
- Não necessita de verificação de todos os nós para append
- Smart Contracts

Canais

- Forma de manter dados visíveis para apenas nós selecionados.
- Permite realizar transações de forma privada, sem expor para toda a rede.

Uma feature importante das enterprises blockchains é não ser anônima, como resolver:

Membership Service Provider (MSP):

- Contêm uma lista de todos os participantes envolvidos na rede blockchain.
- Provê uma identidade para esses participantes.

Fabric CA

- Autoridade certificadora que gera chaves para inicializar o MSP.

Outra feature é não ser totalmente transparente, ou seja, controlar quem acessa determinadas informações?

Access Control List (ACL):

- Controle de permissões a nível de canal e blockchain.

Também não queremos que todos os nós verifiquem as transações para evitar atrasos, como resolver esse problema:

Committing Nodes

- Nós especiais contêm todas as cópias do Ledger para verificação.
- Isso diferencia o Hyperledger do Ethereum blockchain.
- Isso deixa o sistema mais rápido e eficiente.

Endorsing Nodes

- Nós que executam os contratos inteligentes.

Ethereum Networks:

- MainNet (Live Network):
    - Proof of Work
- Ropsten (Test Network):
    - Proof of Work
    - Cross-Client
- Rinkeby (Test Network):
    - Proof of Authority
    - Geth-Client
- Kovan (Test Network):
    - Proof of Authority
    - Parity-Client

Ordering Service:

- A ordem das transações pode ser muito importante para uma blockchain.
- Ordering Node:
    - Componente que mantém a sequência de transações na Network Hyperledger.

State Database:

- É uma database que armazena um par de chave-valor do estado mais recente do ledger.

Introdução ao Hyperledger Fabric:

- Iniciado pela Linux Foundation como um projeto para criar aplicações baseadas em Blockchain.
- É um dos softwares mais populares para Enterprise Blockchain.

	Bitcoin	Ethereum	Hyperledger
Crypto Currency	Yes	Yes	No
Permissioned	No	No	Yes
Smart Contracts	No	Yes	Yes
Consensus Protocol	Pow	Pow	Many

Hyperledger Transactions:

1. Cliente inicia transação.
    a. Quando a requisição chegar, a rede verifica a identidade do cliente com o Membership Service Provider (MSP).
    b. Quando a identidade do cliente for confirmada, a rede verifica as permissões de acesso na Access Control List (ACL).
2. Cliente envia a proposta de transação em forma de broadcast para todos os Endorsing Peers.
3. Endorsing peers rodam o chain code e retornam o resultado para o cliente em forma de Signed Transaction Proposals.
4. O cliente verifica se o consenso foi atingido nessas respostas dos Endorsing Peers.
    a. Se ao menos 2/3 das respostas estiverem iguais, o consenso foi atingido e o cliente avança para próxima etapa.
5. Cliente faz broadcast da proposta para o Ordering Service
    a. Informa os ordering nodes que existe uma nova transação para ser guardada no ledger.
6. Transações são ordenadas e um bloco é criado com essas transações.
    a. O Bloco é enviado em broadcast para os peers.
7. Os Peers validam as transações do bloco e informam o cliente.
8. Caso validado, todos os peers adicionam uma cópia desse bloco no seu ledger.