



Hyperledger
FOUNDATION



Capítulo Brasil

Introdução ao Hyperledger Besu e Hyperledger Fabric

Marcelo Creimer

Magno Alves Cavalcante (moderador)



11 de dezembro de 2023

segunda-feira



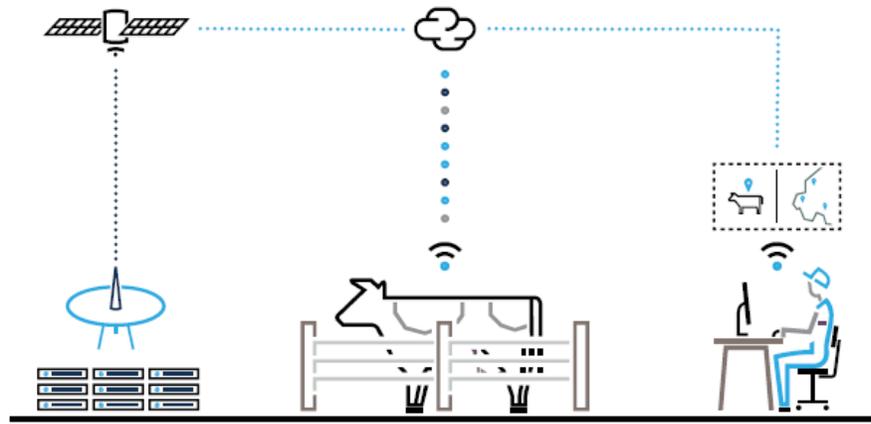
19:00

Horário de Brasília (GMT-3)

<https://wiki.hyperledger.org/x/6gDBBg>



Modelos Mentais para Redes Descentralizadas



Yesterday: Closed and centralized



Today: Open and in the cloud



Tomorrow: Open and decentralized

Características de Blockchain

Tecnologia de Registro Distribuído

Criptografia de Chave Pública

Rede Descentralizada

Registros Imutáveis

Rastreabilidade dos Registros

Integridade dos Dados

Transparência nas Transações

Auditabilidade do Sistema

Resistência a Fraudes

Automação por Contratos Inteligentes

Algoritmos de Consenso

Terceira Parte Confiável





850 projetos

17.000+ empresas contribuidoras

750.000+ contribuidores

2.000.000+ de desenvolvedores treinados

51.000.000+ de linhas de código adicionados cada semana

Projetos Linux Foundation



Listagem parcial

Membros Linux Foundation





Hyperledger

F O U N D A T I O N



Hyperledger

FOUNDATION



98K+ Members



180+ Groups



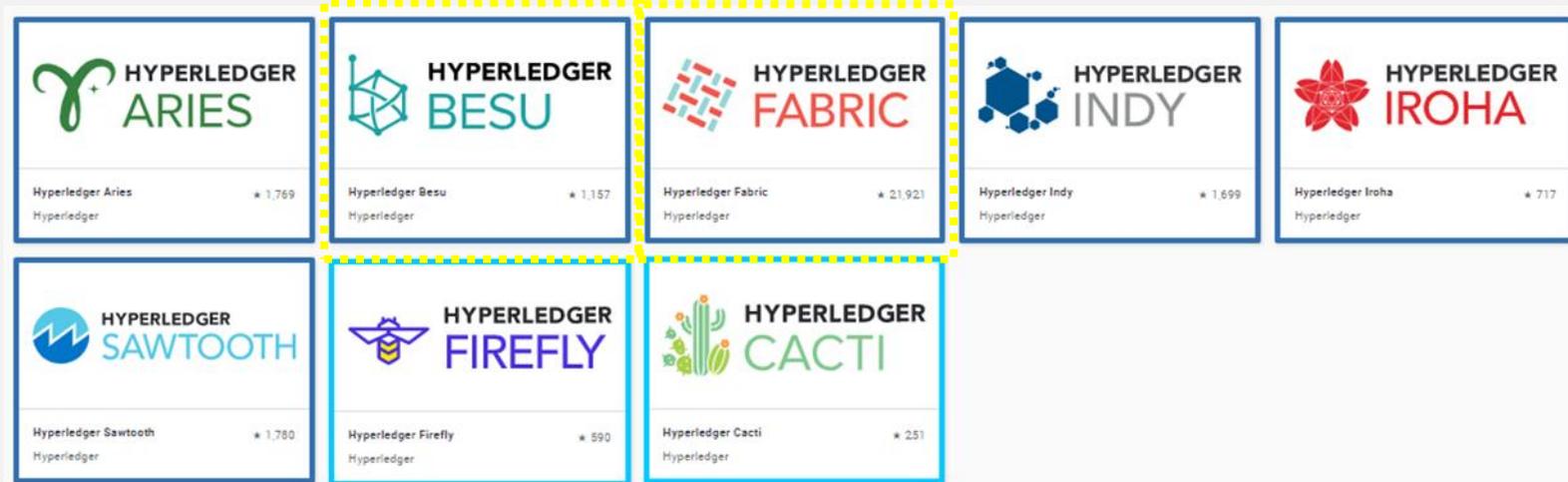
80+ Countries





Hyperledger
FOUNDATION

Projetos em produção (“Graduated”)



Projetos em desenvolvimento (“Incubating”)



Hyperledger Besu

EVM



HYPERLEDGER

BESU



HYPERLEDGER BESU

Criado como um cliente do tipo Ethereum, e desenvolvido pelo time de Protocolos da Consensus

Lançado com o nome Pantheon

Novembro / 2018

Agosto / 2019

Março / 2020

Juntou-se aos projetos Hyperledger

Primeiro projeto Hyperledger a rodar em rede pública

Hyperledger Besu passa do status de projeto incubado para ativo



- Cliente do tipo Ethereum open-source, escrito em Java e desenvolvido sob a licença Apache 2.0
- Baseado em EVM (Ethereum Virtual Machine)
 - ✓ Aceita smart contracts construídos na linguagem Solidity
- Aplicações corporativas em rede privada:
 - ✓ Segurança
 - ✓ Alto desempenho
 - ✓ Privacidade
 - ✓ Permissionamento
- Protocolos de consenso:
 - ✓ Proof of Authority (QBFT, IBFT 2.0, ou Clique)
 - ✓ Proof of Work (Ethash)
 - ✓ Proof of Stake (Ethereum)



Interface

- O Besu inclui uma interface de comando de linha e API JSON-RPC para executar, manter e monitorar nós em uma rede Ethereum.
- Desenvolvedor pode usar API via RPC sobre HTTP ou via WebSocket.
- Pub/Sub também é suportado.

Smart Contracts

- Suporta smart contract e desenvolvimento de DApps, por meio do uso de ferramentas como Truffle, Remix e Web3.JS.

Características

Ethereum Virtual Machine (EVM): Máquina Virtual Turing completa

Algoritmos de consenso:

- **Proof of Authority:** Usado quando os participantes se conhecerem:
 - **IBFT 2.0:** Transações e blocos são validados por contas aprovadas, conhecidas como validadores.
 - **Clique:** Mais tolerante a falhas que o IBFT 2.0, pois tolera até a queda de metade dos validadores.
- **Proof of Work (Ethash):** Era o protocolo usado para atividades de mineração na mainnet Ethereum.

Características

Armazenamento: Besu utiliza RocksDB, como banco de dados do tipo chave-valor.

Dividido em:

- **Blockchain:**
 - Cabeçalhos, que formam a cadeia (*chain*) de dados;
 - Corpo do bloco, que contém a lista de transações ordenadas de cada bloco;
 - Recibos de transação com metadados.
- **Estado global (*World state*):**
 - Cada cabeçalho de bloco referencia um estado global via um “*hash stateRoot*”;
 - O estado global é um mapeamento de endereços para contas.

Características

Monitoramento: Besu permite monitoramento de nó e desempenho de rede.

- Desempenho de nó: Usando o Prometheus ou as métricas de debug da API JSON-RPC
- Desempenho de rede: monitorado com ferramentas como o Block Explorer e o EthStat.

Privacidade: Transações privadas entre as partes envolvidas. Outras partes não podem acessar o conteúdo, a parte que enviou, ou a lista de participantes.

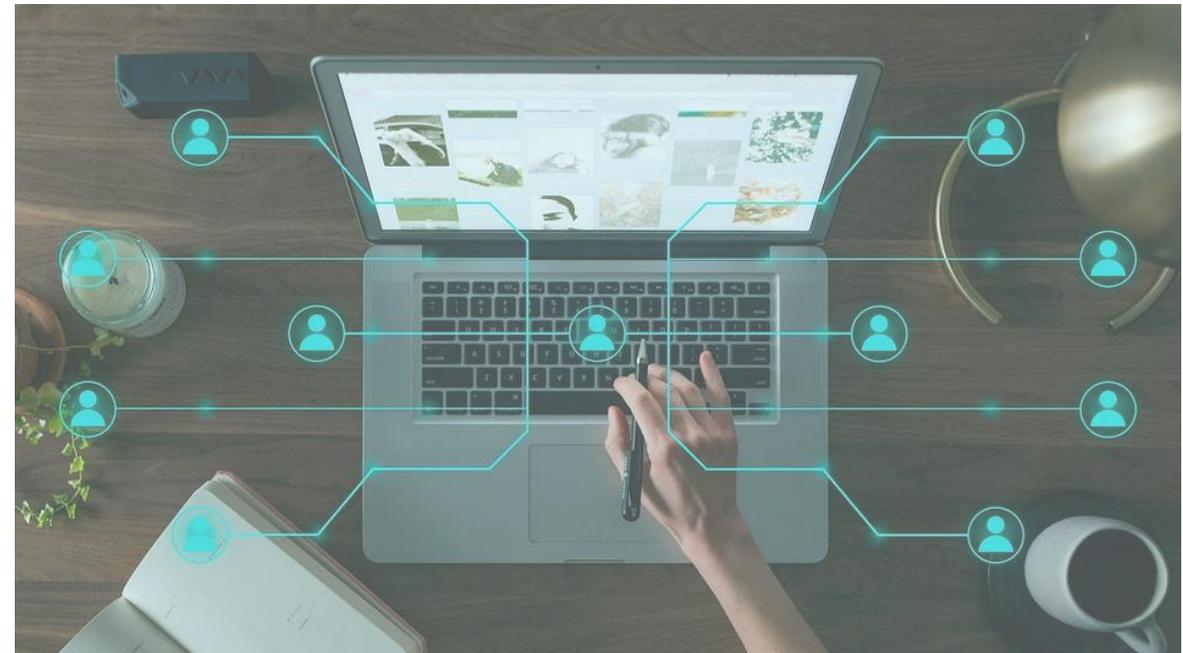
Permissionamento: Permite somente nós e contas especificados participarem, habilitando permissionamento de nó e/ou conta na rede.

Nós estáticos (Static nodes)

- Conjunto de nós confiáveis configurados
- Isentos dos limites de **maximum peer** e **remote connection**
- Besu tenta manter conexões com todos os nós estáticos desconectados
- Bootnodes e nós estáticos são métodos paralelos de se encontrar peers
 - Bootnodes → descoberta (discovery) de peers
 - Static nodes → configurar um conjunto específico de conexões

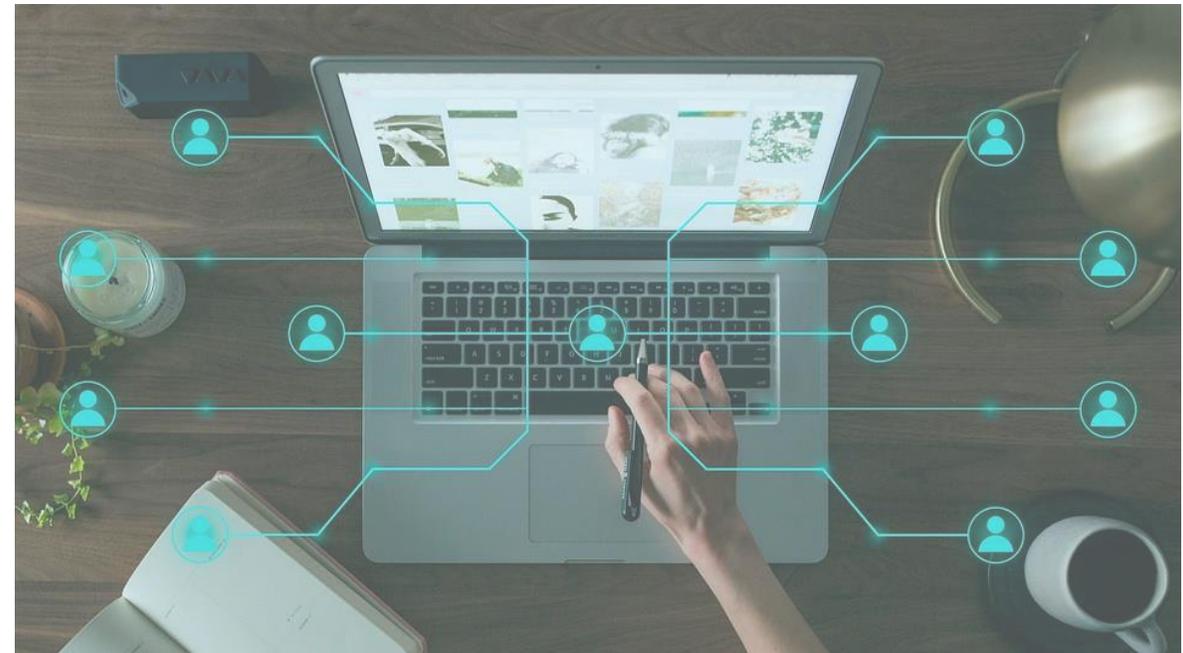
Protocolos de Consenso >> Proof of Authority (PoA)

- Algoritmo baseado em reputação
- Proposto em 2017 por Gavin Wood (co-fundador da Ethereum)
- Solução prática e eficiente principalmente para redes privadas
- Considera o valor da identidade, sendo que a reputação do nó é que está em jogo



Protocolos de Consenso >> Proof of Authority (PoA)

- Blocos e transações são verificados por participantes pré-aprovados, que agem como moderadores do sistema
- Indivíduos podem receber o direito de se tornar validador, então há um incentivo para ele manter essa posição, mantendo sua boa reputação
- Por segurança, o PoA somente aceita aprovação de blocos não consecutivos pelo mesmo validador



PoA no Besu

Besu implementa 3 protocolos de consenso: **QBFT**, **IBFT 2.0**, e **Clique**.

Protocolos de prova de autoridade:

- Quando os participantes se conhecem e há um nível de confiança entre eles
- Tempo de bloco rápido
- Tempo de vazão das transações muito maior que o PoW (antigo protocolo da Ethereum Mainnet)

Na QBFT e IBFT 2.0, um grupo de nodes atuam como validadores (validators)

Na Clique, um grupo de nós atua como assinantes (signers)

Os nós validadores e assinantes votam na inserção e remoção de nós

Qual protocolo escolher?

	QBFT	IBFT 2.0	Clique
Finalidade imediata	Sim. Não há forks e todos os blocos válidos são incluídos na chain principal		Não. Há ocorrência de forks e reorganizações da chain
Número mínimo de validadores	4		Pode usar apenas 1 (mas sem oferecer redundância)
Vivacidade	Necessitam pelo menos 2/3 dos validadores operando para produzir blocos (Para produção recomenda-se pelo menos 4 nós)		Mais tolerante. Tolera metade dos validadores falhar
Alcançar consenso e adição de blocos	Menos rápidas		Mais rápida
Aumento do número de validadores	Aumenta o tempo para adicionar blocos na rede		Aumenta a probabilidade de forks
Recomendada para uso corporativo	Sim	Não	Não

Privacidade

No Besu, é a garantia de que o conteúdo das transações seja visualizado apenas pelos participantes da rede

A lista de participantes da rede também não é aberta ao público.

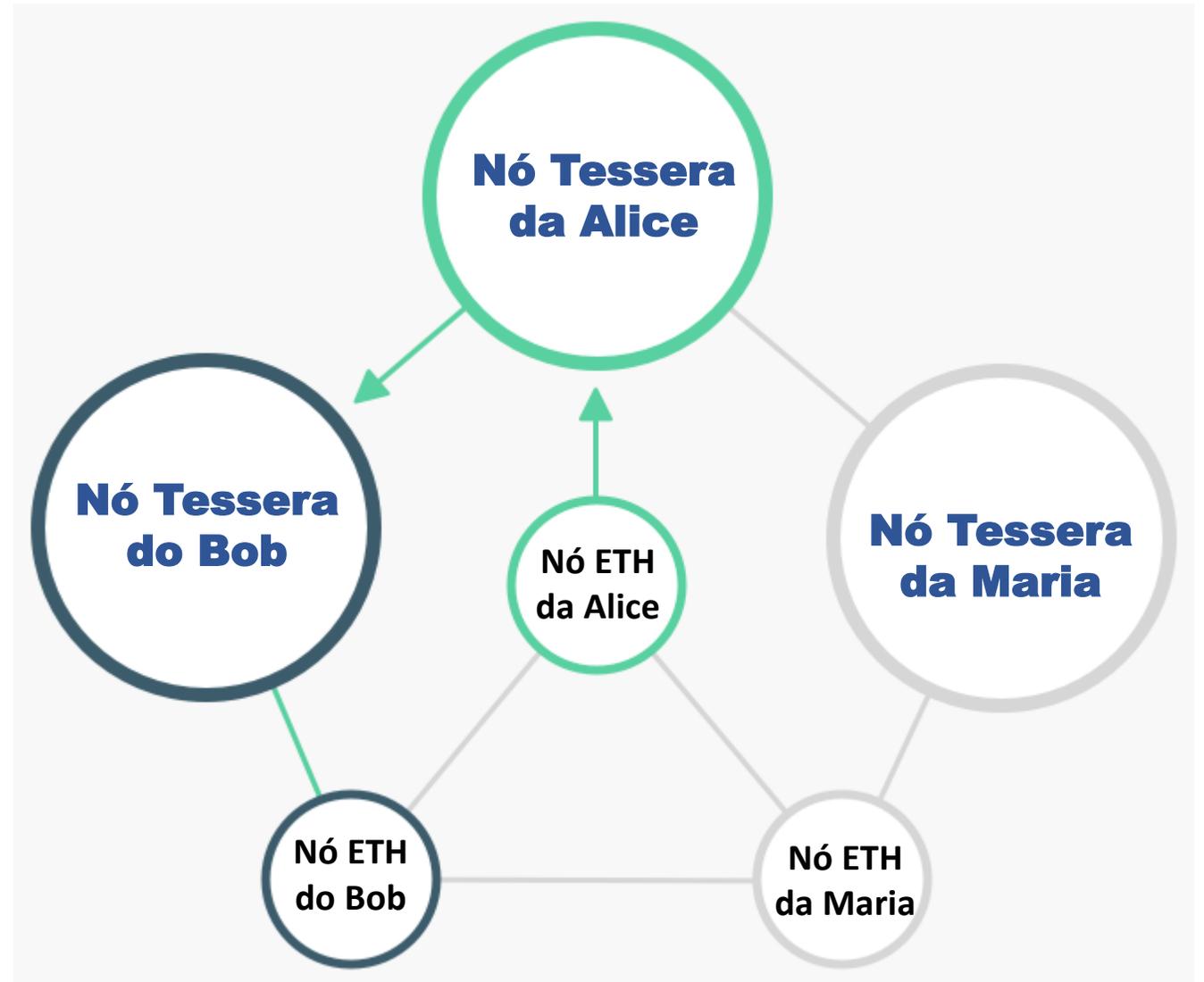
Tessera é o gerenciador de transações privadas, desenvolvido pela Consensusys

Cada nó Besu que envia ou recebe transações privadas precisa de um nó Tessera exclusivo seu

Gerenciador de transações privadas também são conhecidos pelo nome “Enclave”

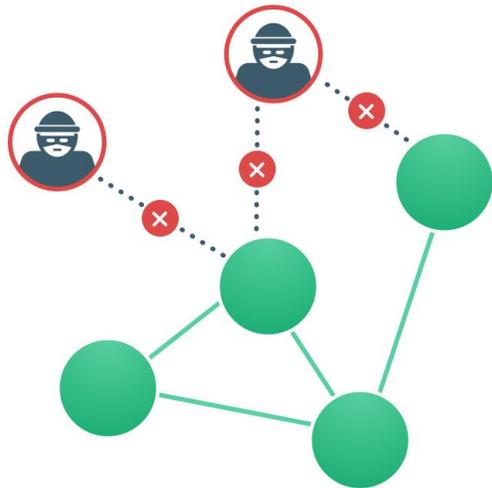
“Alice” enviando uma transação privada para “Bob”

1. Transações privadas passam do nó Besu para o nó Tessera associado.
2. O nó Tessera encripta e distribui diretamente (ponto a ponto) a transação privada para os nós Tessera participantes da transação.
3. Por default, cada participante em uma rede privada usa seu próprio nó Besu e Tessera.



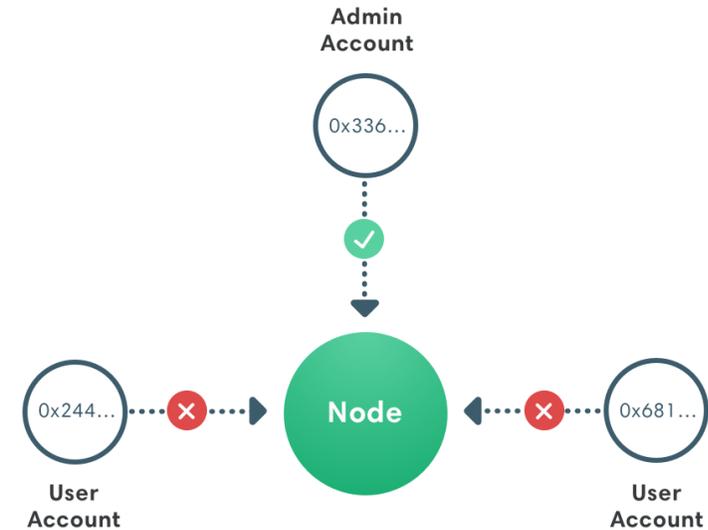
Permissionamento

Permissionamento de Nós



- Restrição de acesso somente a nós conhecidos
- Sistema de governança para controlar conexões para um nó em particular

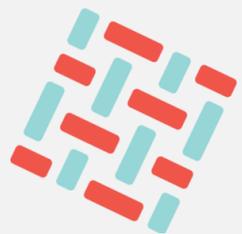
Permissionamento de Contas



- Garante o onboarding e requisitos de identificação
- Permite suspender contas
- Restringe as ações que uma conta pode realizar

Hyperledger Fabric

Ledger by Fabric



HYPERLEDGER
FABRIC

- Ativos (Assets)
- Chaincodes (Smart Contracts)
- Livro-Razão (Ledger)
- Privacidade
- Serviços de Segurança e Associação
- Consenso

Ativos (Assets)



- Os ativos podem variar do tangível (imóveis e bens de consumo) ao intangível (contratos e propriedade intelectual).
- As operações com os ativos são feitas usando contratos inteligentes.
- Representados no Fabric como uma coleção de pares de chave-valor, com as alterações de estado registradas como transações no livro-razão do Canal (Channel).
- Os ativos podem ser representados no formato binário ou JSON

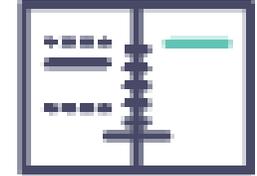
Chaincodes



Software que define ativos, e as instruções de transação para modifica-los estado

- Chaincode é um software que define ativos, e as instruções de transação para modifica-los.
- É a lógica de negócio.
- Garante a aplicação das regras para ler ou alterar os pares de chave-valor ou outras informações do banco de dados de estado.
- Suas funções são executadas no banco de dados de estado atual do livro-razão e são iniciadas por meio de uma proposta de transação.
- O resultado da execução de um chaincode é um conjunto de atualizações de chave-valor que podem ser enviadas à rede e aplicadas ao livro-razão de todos os pares.

Livro-Razão (Ledger)



Registro sequencial e resistente a violações de todas as transições de estado

- As transições de estado são resultado de invocações do chaincode, as “transações” enviadas pelas partes participantes.
- Cada par (“peer”) mantém uma cópia do livro-razão para cada canal (“channel”) do qual eles são membros.
- Permite consulta e atualização através de pesquisas baseadas em chave, intervalo e chave composta
- As transações contêm as assinaturas de todos os pares endossantes e são enviadas para o serviço de ordem
- Se torna imutável uma vez que uma transação é validada e confirmada
- O livro-razão de um canal contém um bloco de configuração que define suas políticas e listas de controle de acesso.

Privacidade



- Fabric emprega um livro-razão imutável por canal e também um “chaincode” que pode manipular modificar o estado atual dos ativos.
- O livro-razão pode ser segregado para incluir apenas um conjunto específico de participantes, isolando/segregando suas transações e o livro-razão.
- O chaincode pode ser instalado apenas nos pares que precisam acessar os estados do ativo para executar leituras e gravações
- Quando um subconjunto de organizações em um canal precisa manter seus dados de transação confidenciais, um conjunto privado de dados (coleção) é usado para segregar esses dados em um banco de dados privado
- Para ofuscar ainda mais os dados, os valores no chaincode podem ser criptografados (em parte ou no total) E podem ser descriptografados apenas pelo usuário que possui a chave correspondente que foi usada para gerar o texto criptografado.

Serviços de Segurança e Associação



- Fabric suporta uma rede transacional em que todos os participantes têm identidades conhecidas (“permissionada”).
- A infraestrutura de chave pública é usada para gerar certificados criptográficos
- O controle de acesso a dados pode ser manipulado e controlado em uma rede ampla e nos níveis de canal.
- O permissionamento, juntamente com os canais, possibilita privacidade e a confidencialidade em ambientes onde são preocupações fundamentais.

Consenso



- Compreende todo o fluxo da transação, desde a proposta e endosso, até a ordem, validação e registro.
- É o processo completo de verificar a validade e coerência de um conjunto de transações de um bloco.
- O consenso é alcançado quando a ordem e os resultados das transações de um bloco atendem às verificações explícitas dos critérios da política.
- Inclui o uso das políticas de endosso e chaincodes.
- Faz a verificação da versão atual do livro-razão, protegendo contra operações com registro duplicado e outras ameaças
- Realiza verificações de identidade ativa em todas as direções do fluxo da transação.
- Implementa listas de controle de acesso
- Os dados transferidos são repetidamente assinados, verificados e autenticados à medida que uma proposta de transação passa pelos diferentes componentes da arquitetura.

O que é uma identidade?

Certificados digitais X.509 determinam as permissões exatas dos recursos e acessos as informações que os atores têm em uma rede blockchain

Não basta ter um cartão de crédito válido – ele também deve ser aceito pela loja!

PKIs e MSPs trabalham juntos da mesma maneira – uma PKI fornece uma lista de identidades e um MSP diz quais deles são membros de uma determinada organização que participa da rede.



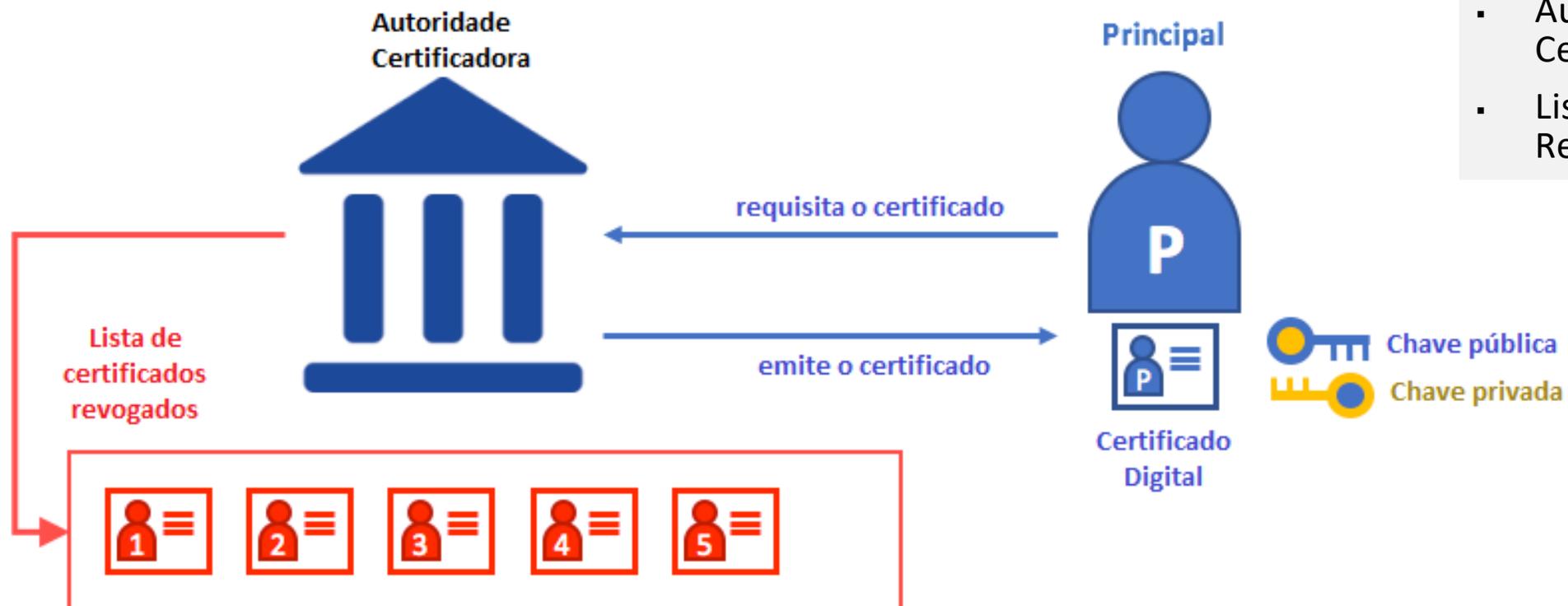
MSPs transformam
identidades verificáveis
em membros de uma
rede blockchain

O que são PKIs?

Infraestrutura de chave pública (PKI = *Public Key Infrastructure*)

Coleção de tecnologias da Internet que fornece comunicações seguras em uma rede

- Principais elementos para a PKI:
- Certificados Digitais
 - Chaves Públicas e Privadas
 - Autoridade Certificadora
 - Lista de Certificados Revogados



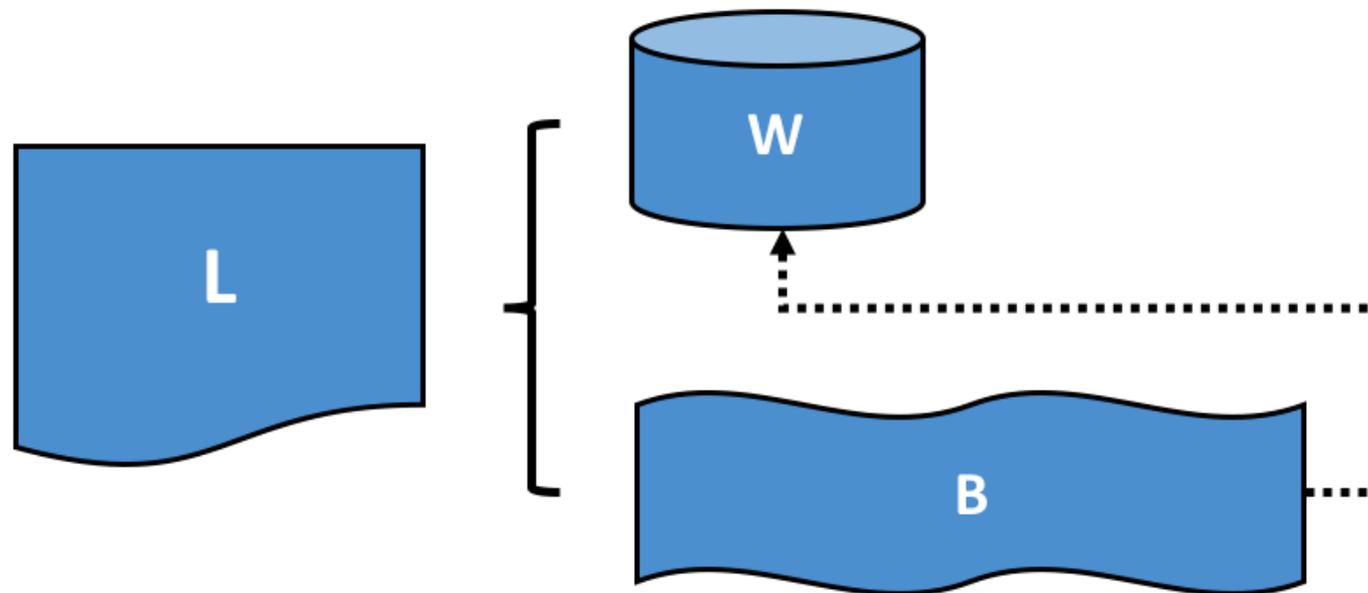
Por que preciso de um MSP?



O Livro-razão (*Ledger*)

Um Ledger **L** compreende o blockchain **B** e o estado global **W**, onde o blockchain B determina o estado global W.

Também podemos dizer que o estado global W é derivado do blockchain B.

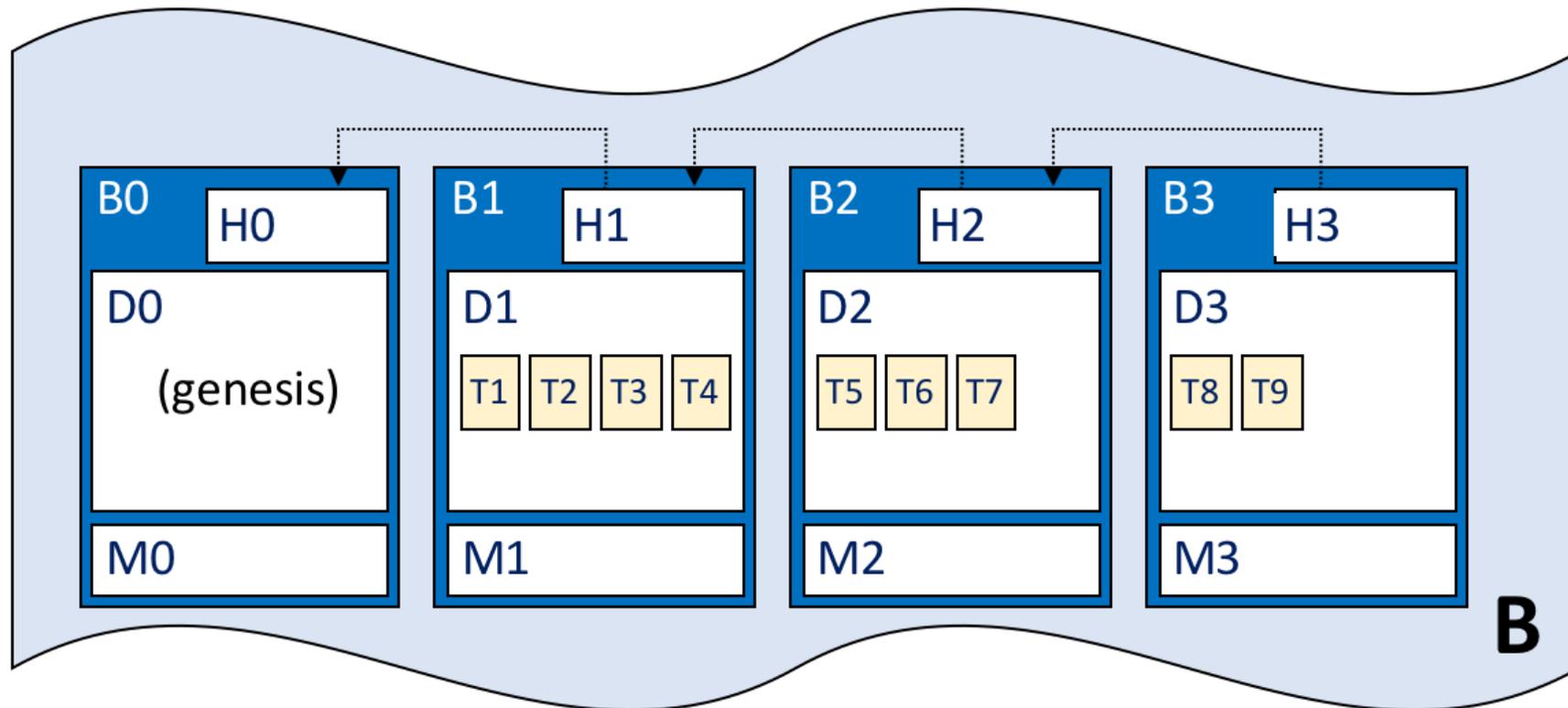


A Cadeia de Blocos da Blockchain

Um blockchain B contendo os blocos B0, B1, B2, B3.

B0 é o primeiro bloco da blockchain, o bloco genesis.

O bloco B2 tem um bloco de dados D2 que contém as transações: T5, T6, T7.

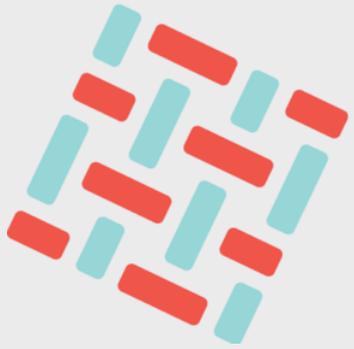


Serviço de Ordenação

- ❑ Fabric apresenta um nó chamado ordenador (também conhecido como “**nó de ordenação**”) que faz essa ordenação de transação; junto com outros nós ordenadores formam um **serviço de ordenação**
- ❑ Garante a finalidade
- ❑ Separa o endosso da ordem da execução do chaincode
- ❑ Vantagens: desempenho e escalabilidade
- ❑ Ordenantes também mantêm a lista de organizações que têm permissão para criar canais. Essa lista de organizações é conhecida como “**consórcio**”
- ❑ Se o serviço de ordens mantiver várias dessas listas, o consórcio é considerado **multi-tenancy**

Fabric ou Besu ?

Qual Hyperledger framework é melhor aplicável na sua arquitetura?



HYPERLEDGER
FABRIC

OU



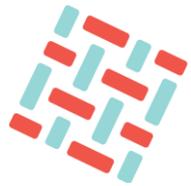
HYPERLEDGER
BESU

Rede:



HYPERLEDGER
BESU

Pública e Privada



HYPERLEDGER
FABRIC

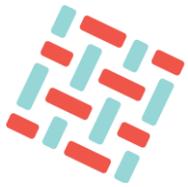
Privada

Linguagens:



HYPERLEDGER
BESU

Solidity



HYPERLEDGER
FABRIC

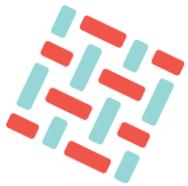
Go, Java, Node.JS

Consenso:



HYPERLEDGER
BESU

PoW, PoA, IBFT, etc



HYPERLEDGER
FABRIC

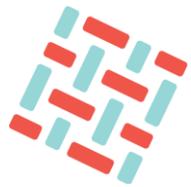
**Crash Fault-Tolerant (CFT),
Kafka ou Raft**

Participação no mercado:



HYPERLEDGER
BESU

Menos Difundido



HYPERLEDGER
FABRIC

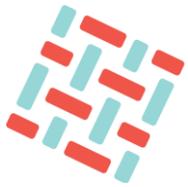
Mais Difundido

Ethereum:



HYPERLEDGER
BESU

Compatível



HYPERLEDGER
FABRIC

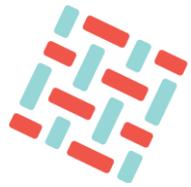
Incompatível

Privacidade:



HYPERLEDGER
BESU

Plugável (Tessera)



HYPERLEDGER
FABRIC

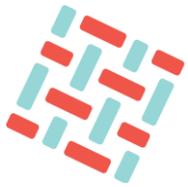
Nativa (Channels e Private Data)

Tokens:



HYPERLEDGER
BESU

ERC-20, ERC-721, ERC-1155, etc



HYPERLEDGER
FABRIC

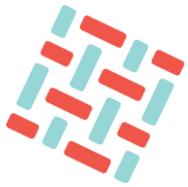
Sem Token Nativo
(mas pode ser criado)

DREX:



HYPERLEDGER
BESU

Compatível



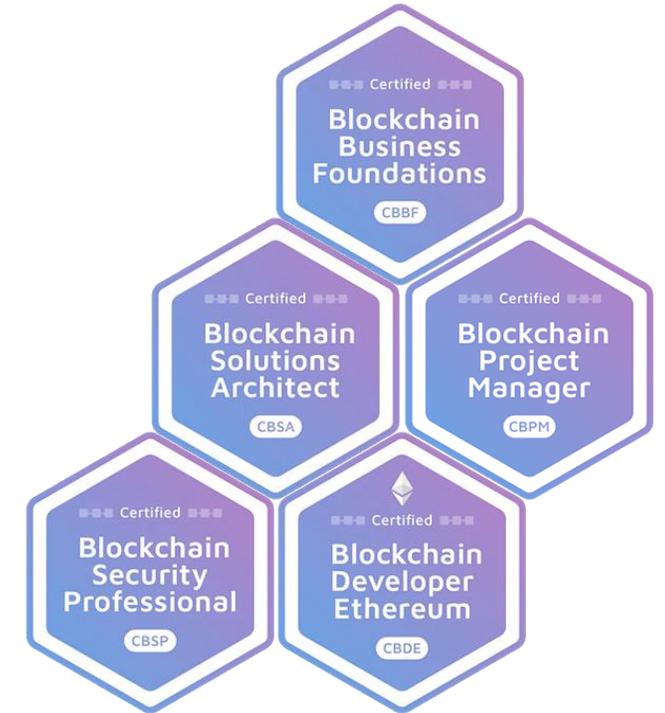
HYPERLEDGER
FABRIC

Incompatível

Certificações Profissionais

O melhor do profissional para serviço ao mercado

Certificações Profissionais







HFCP

Hyperledger Fabric Certified Practitioner

Exame totalmente reformulado,
lançado em 09/2023

Certificação Oficial



Hyperledger
FOUNDATION

O Exame

Destinada a profissionais de TI, principalmente engenheiros e desenvolvedores de software

Local	Online
Duração máxima do exame	1 hora e meia
Certificação válida por	3 anos
Tempo para marcação do exame	12 meses
Novas tentativas	1
Certificado	PDF e badge digital
Versão do Fabric 	2.5
Tipo do exame	Múltipla escolha
Idiomas disponíveis	Inglês, japonês e chinês
Nível de experiência	Iniciante
Pré-requisitos	Não há

Conteúdo Programático do Exame

Fundamentos - 16%

- Livro-razão distribuído
- Contratos inteligentes
- Consenso
- Modelo do Fabric
- Benefícios de negócios

Redes Fabric - 36 %

- Estrutura da rede
- Fluxo das transações
- Serviço de ordenação
- Pares e armazenamento do estado global
- Criação de rede
- Fornecedores de serviço de associação (MSPs)
- Manutenção e operação
- Operações relacionadas a canais
- Desenho e implantação de redes de produção

Contratos inteligentes - 24%

- Desenho e implementação
- Ciclo de vida do chaincode
- Lendo e modificando o estado do livro-razão
- Executando consultas (queries) no livro-razão
- Dados privados e suas coleções
- Políticas de endosso baseadas em estado

Aplicações cliente - 24%

- Modelo de gateway
- Serviço de par de gateway
- Chamada de contrato inteligente
- Eventos
- Conexão (Signing) Offline



Testing
Excellence



Ambiente do exame de certificação é de responsabilidade de uma empresa terceira, a Psi.

Monitoração por câmera, microfone e compartilhamento do seu desktop durante todo o exame

Diversas medidas de preparação do ambiente antes e durante o exame

Exame realizado em um browser específico que deve ser instalado na hora do exame

Cheque a sua configuração: <https://syscheck.bridge.psiexams.com/>

Registro para o Exame

- Registrar-se para o exame, te torna elegível a agendar o exame
- Registrar (“Register”) não é o mesmo que agendar (“scheduling”).
- Após o registro, você tem 12 meses para agendar e fazer o exame
- É preciso ter uma conta na Linux Foundation.
- O preço do exame é 250 dólares (sujeito à reajustes), a ser pago com cartão de crédito internacional

Menu

EXAM
Exam

Exam Preparation Checklist

Exam Code: **HFCP-BETA** Expiration Date: **August 16, 2024**

- Agree to Global Candidate Agreement** [Read Now](#) ?
- Verify Name** Status: Done [Verify Again](#) ?
- Select Platform** Platform: No Platform Required ?
- Schedule an Exam** Exam Date: September 04, 2023 - 03:30PM
America/Sao_Paulo [Cancel or Reschedule](#) ?
- Check System Requirements** Status: System Requirements Checked [Check Again](#) ?
- Get Candidate Handbook** [Read Now](#) ?
- Read the Important Instructions** [Read the Important Instructions](#) ?
- Take Exam** [Take Exam](#) true This button will become active in 7 days, 16 hours, 22 minutes ?
Exam Date: September 04, 2023 - 03:30PM
[Cancel or Reschedule](#)

If you have any issues while taking an exam, please be sure to open a support ticket with [The Linux Foundation Training & Certification Support Team](#)

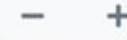
Certifique-se de obter todos os checks verdes, exceto o Take Exam, que so é habilitado 30 minutos antes do exame



REQUEST BREAK

END PROCTORING SESSION

LIVE CHAT



144%



PSI



00:18:10

English

Exam Timer

Question: 2 of 10

What is the highest mountain in the world?

- Mount Everest
- Alaska Range
- Smoky Mountains
- Adirondack Mountains

Flag for review

Click to Flag this item for review

Navigate between items by clicking Previous or Next

← Previous

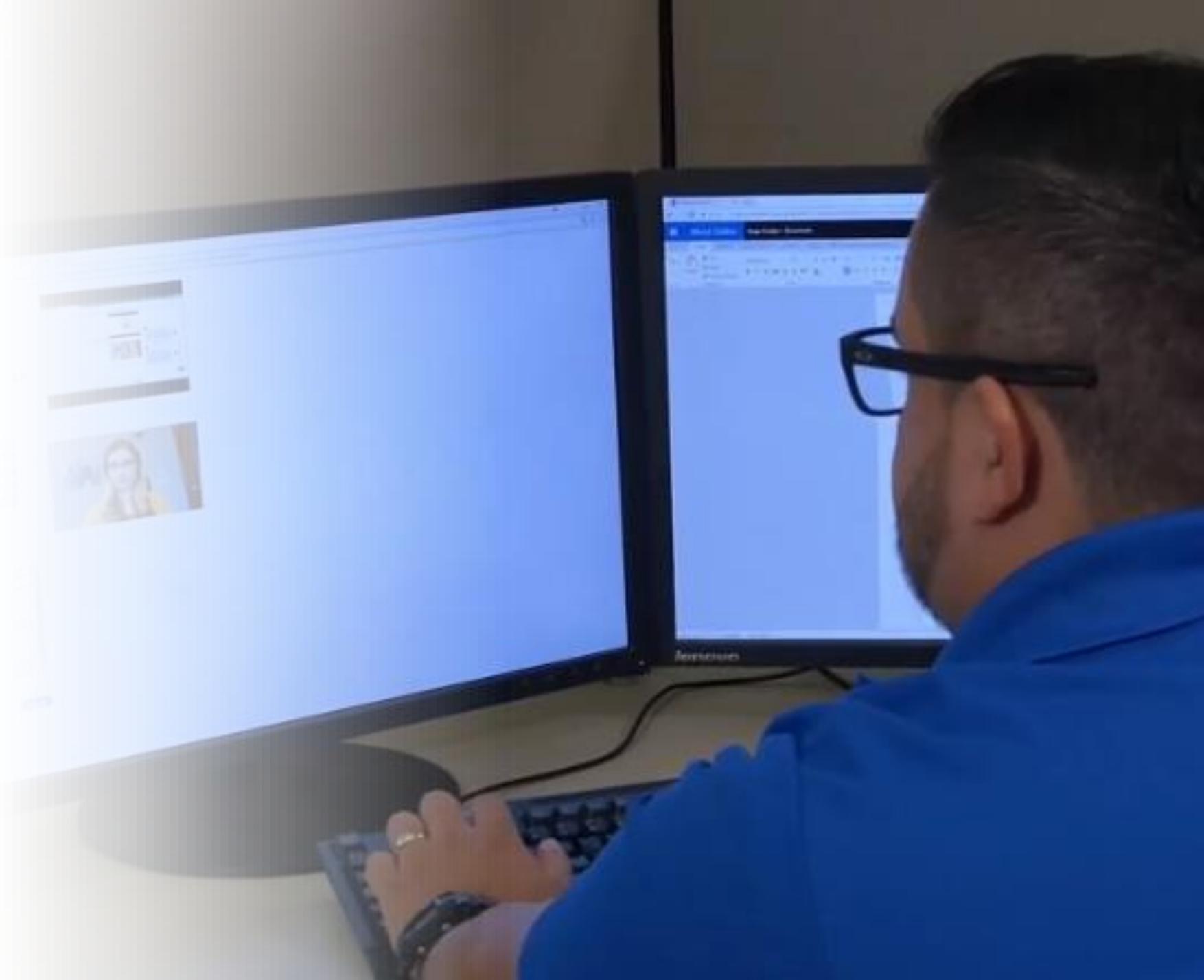
Next →

Review Items

Item 1 <input type="checkbox"/> Review ✔ Completed	Item 2 <input type="checkbox"/> Review ✔ Completed	Item 3 <input type="checkbox"/> Review ✔ Completed	Item 4 <input type="checkbox"/> Review ✔ Completed	Item 5 <input type="checkbox"/> Review ✔ Completed	Item 6 <input type="checkbox"/> Review ✔ Completed
Item 7 <input checked="" type="checkbox"/> Review ✔ Completed	Item 8 <input type="checkbox"/> Review ✔ Completed	Item 9 <input type="checkbox"/> Review ✔ Completed	Item 10 <input type="checkbox"/> Review ✔ Completed	Item 11 <input checked="" type="checkbox"/> Review ✔ Completed	Item 12 <input type="checkbox"/> Review ✔ Completed
Item 13 <input type="checkbox"/> Review ✔ Completed	Item 14 <input type="checkbox"/> Review ✔ Completed	Item 15 <input checked="" type="checkbox"/> Review ✔ Completed	Item 16 <input checked="" type="checkbox"/> Review ✔ Completed	Item 17 <input type="checkbox"/> Review ✔ Completed	Item 18 <input type="checkbox"/> Review ✔ Completed
Item 19 <input type="checkbox"/> Review ✔ Completed	Item 20 <input type="checkbox"/> Review ✔ Completed	Item 21 <input type="checkbox"/> Review ✔ Completed	Item 22 <input type="checkbox"/> Review ✔ Completed	Item 23 <input type="checkbox"/> Review ✔ Completed	Item 24 <input type="checkbox"/> Review ✔ Completed
Item 25 <input checked="" type="checkbox"/> Review ✔ Completed	Item 26 <input type="checkbox"/> Review ✔ Completed	Item 27 <input type="checkbox"/> Review ✔ Completed	Item 28 <input type="checkbox"/> Review ✔ Completed	Item 29 <input type="checkbox"/> Review ✔ Completed	Item 30 <input type="checkbox"/> Review ✔ Completed

Um profissional da PSI irá acompanhar todo o seu exame

- Observando a sua tela;
- Observando você e seu ambiente pela sua camera;
- Ouvindo o que seu microfone capta de sons;
- Estando disponível para conversa (voz ou chat) em caso de dúvidas ou de problemas técnicos, desde que não tenha relação com o conteúdo do seu exame.





Treinamentos e Capacitação



Treinamento Besu / DREX



Hyperledger Besu, o blockchain por trás do Real Digital

Aprenda sobre a tecnologia blockchain **Hyperledger** Besu, que está sendo usada pelo Banco Central para o DREX

Marcelo Creimer

4,5 ★★★★★ (32)

4 horas no total · 50 aulas · Intermediário

Mais vendidos



udemy.com/course/hyperledger-besu-blockchain-real-digital/

Cupom de desconto: **BLACK2023**

Treinamento Certificação Fabric



Preparatório Certificação Hyperledger Fabric (HFCP) 2023

Estude o conteúdo do exame de certificação do blockchain **Hyperledger** Fabric, com dicas e simulado.

Marcelo Creimer

5,0 ★★★★★ (4)

7 horas no total · 54 aulas · Intermediário

Novo e em alta



udemy.com/course/preparatorio-certificacao-hyperledger-fabric/

Cupom de desconto: **BLACK2023**

Como fazer parte do Hyperledger Brasil Chapter?



Canais de comunicação e conteúdo do Capítulo Brasil da Hyperledger Foundation:

 **Site da Hyperledger Foundation:** <https://pt-br.hyperledger.org/>

 **Wiki:** <https://wiki.hyperledger.org/display/CP/Hyperledger+Brazil+Chapter>

 **Vídeos no Youtube:** <http://tiny.cc/8xyavz>

(https://www.youtube.com/playlist?list=PL0MZ85B_96CHEj90NHTX9E7VpOVXC7Gwf)

 **Discord do Capítulo Brasil:** <http://tiny.cc/exyavz>

(<https://discord.com/channels/905194001349627914/943207619508723723>)

 **LinkedIn:** <https://www.linkedin.com/company/hyperledgerbrasil/>

 **Mailing-list:** <https://lists.hyperledger.org/g/community-brazil-chapter>



Hyperledger
FOUNDATION



Capítulo Brasil

Introdução ao Hyperledger Besu e Hyperledger Fabric

Marcelo Creimer

Magno Alves Cavalcante (moderador)



11 de dezembro de 2023

segunda-feira



19:00

Horário de Brasília (GMT-3)

<https://wiki.hyperledger.org/x/6gDBBg>

