Introdução ao Projeto Hyperledger

Hyperledger Brazil Bootcamp – junho/2019

Marcelo Creimer, Innovation Manager, eZly Tecnologia

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

THE LINUX FOUNDATION

16B US$

Custo estimado de desenvolvimento dos 100 maiores projetos

35.000

Público nos eventos anualmente, vindos de mais de 11.000 empresas de 113 países

1 Milhão

Profissionais inscritos nos treinamentos gratis open-source

10 / 10

Maiores provedores de serviços de cloud são contribuidores e membros

- Fundada no ano 2.000
- Fornece suporte financeiro, intelectual, infra-estrutura, serviços, eventos e treinamento
- Dedicada a construir ecossistemas sustentáveis em projetos open-source

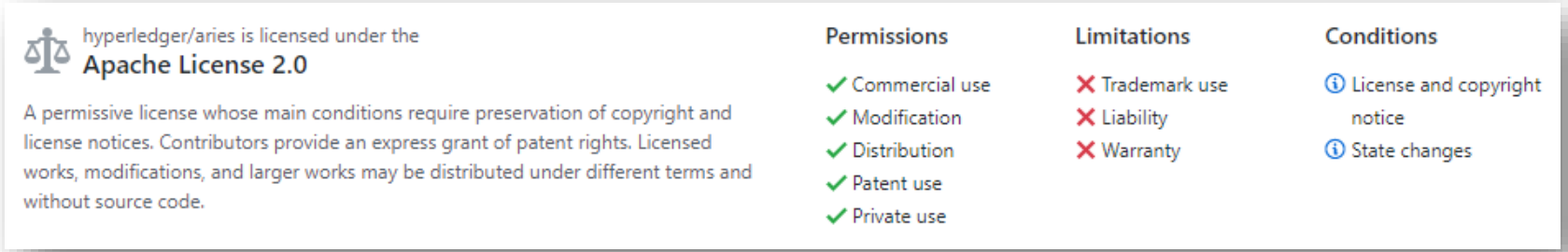
HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Projetos Linux Foundation

- Hospeda o projeto Linux, de Linus Torvalds
- Fornece ambiente para o desenvolvimento do kernel Linux
- O sucesso do Linux catalizou o crescimento da comunidade open source community

HYPERLEDGER

- O Hyperledger é um projeto “guarda-chuva” open source
- Criado e hospedado pela Linux Foundation desde 2015
- Objetiva promover e alavancar tecnologias blockchain *cross-industry* para garantir auditoria, transparencia, e confiança entre parceiros de negócios
- 270+ empresas envolvidas
- 28 empresas codificando o Fabric
- 160 engenheiros dedicados



Hyperledger em números

Membros do Hyperledger

Listagem parcial

Componentes de um Blockchain para Negócios

Ledger do tipo append-only

Smart Contracts para processar requisições de transações

Privacidade nas transações através de acesso permissionado

Algoritmo para consenso nas gravações no ledger

Guarda-chuva Hyperledger

Frameworks

Ferramentas

HYPERLEDGER FABRIC

Tipo: Framework
Status: **Ativo**

- Primeiro projeto disponibilizado para produção
- **Base de 500+ projetos**
- Permite componentes, como os serviços de consenso e membership, serem plug-and-play
- Alavanca a tecnologia de container hospedando smart contracts (“chaincode”)
- Alto grau de confiabilidade, felixibilidade, resilência e escalabilidade.
- A criação de canais (“channels”), permite um grupo de participantes ter um ledger separado de transações

HYPERLEDGER SAWTOOTH

Tipo: Framework
Status: **Ativo**

- Permite a mudança do algoritmo de consenso *on-the-fly*, simplesmente emitindo uma transação
- Proof of elapsed time (PoET) - algoritmo de consenso com a escalabilidade do PoW mas sem o alto consumo de energia
- Transaction families - permite aos desenvolvedores escreverem smart contracts na linguagem que preferirem.
- Compatibilidade com smart contracts Ethereum
- **Pode ser configurado para ser não-permissionado.**
- Paralelismo para execução de transações - scheduler divide blocos em fluxos paralelos

HYPERLEDGER IROHA

Tipo: Framework
Status: **Ativo**

- Incorpora o “Yet Another Consensus”, exclusivo algoritmo de consenso BFT
- Suporte à manipulação de contas e ativos digitais com commandos e queries rápidos
- Os peers são também nodes de validação, que distribuem transações parcialmente assinadas, como parte de transações multi-signature
- Blocos armazenados em arquivos, e o state do ledger em **banco de dados PostgreSQL**.
- Permite análises e relatórios complexos acessando o banco de dados
- Fornece um conjunto de commandos com as principais operações para o gerenciamento de ativos e identididades digitais.
- Aplicações podem ser escritas em Python, Java, JavaScript e C++, além de Android e iOS

HYPERLEDGER BURROW

Tipo: Framework
Status: Incubado

- Contribuição original da Monax, co-patrocinada pela Intel.
- Cliente modular com um interpretador permissionado de smart contract parcialmente desenvolvido para a especificação da **EVM (Ethereum Virtual Machine)**
- Pretende ser a maneira mais rapida e fácil de rodar Smart Contracts do Ethereum em um contexto permissionado.
- Fornece flexibilidade e facilidade no Kubernetes para bootar redes complexas
- Avançada governança de transações permitindo configurações de validadores, tokens nativos, etc com a rede no ar
- Migração da rede (de POC para Piloto, Beta, Produção) sem precisar alterar configurações da rede.
- Compativel com o “Agreements Network”

HYPERLEDGER INDY

Tipo: Framework
Status: **Ativo**

- Concebido para **identidade descentralizada**, pensado em *Privacy by Design*
- Fornece ferramentas, bibliotecas, e componentes reutilizáveis para criação e uso de DIDs
- Permite interoperabilidade entre as identidades em diferentes tipos de blockchains
- Criou especificações, terminologia e padrões de desenho para identidade descentralizada
- Auto-Soberania – Armazena dieversos tipos de identifições distribuidas, que só podem ser alteradas pelo próprio dono.

HYPERLEDGER GRID

Tipo: Framework
Status: Incubado

- Objetiva acelerar o desenvolvimento de **soluções de supply-chain** para todas as indústrias
- O Grid não é um blockchain; é um framework contendo tecnologias e bibliotecas que trabalham em conjunto para permitir aos desenvolvedores escolher os components mais apropriados para o seu caso de uso.
- Pretende inicialmente fornecer implementações referência em modelos de dados e lógicas de negócio para smart contracts, sempre baseados em padrões abertos e melhores práticas da indústria

HYPERLEDGER QUILT

Tipo: Ferramenta
Status: Incubado

- Oferece interoperabilidade entre ledgers implementando o **Interledger Protocol (ILP)**
- O ILP possitibilita *atomic swaps* entre ledgers de qualquer tipo
- Cria um formato padrão para endereços e pacotes de dados para permitir conexão entre os diferentes ledgers

HYPERLEDGER CELLO

Tipo: Ferramenta
Status: Incubado

- Planeja aprimorar o modelo de deploy, reduzindo esforços na criação, gerenciamento e encerramento de blockchains.

- **Facilita o deploy em várias infra-estruturas** (baremetal, VMs, containers e clouds), contribuindo para o “Blockchain as a Service (BaaS).”

- Fornece dashboards com informações em real-time contendo:
  - O status do blockchain
  - Estatísticas como eventos, performance dos chaincodes, utilização de recursos, etc
  - Gerenciamento do blockchain, para sua criação, configuração e deleção.
  - Deploy e upload de chaincode

- Atualmente suporta o Fabric, mas planeja suportar em seguida o Sawtooth e então outros frameworks

- Arquitetura no estilo micro-service, com a maioria dos components plugáveis.

HYPERLEDGER COMPOSER

Tipo: Ferramenta
Status: Incubado

- Conjunto de ferramentas de colaboração para facilitar a criação de aplicações blockchain e smart contracts
- Construido em JavaScript, permite o uso de modernas ferramentas, como node.js, npm, CLI e editores populares
- **Abstrai o lado técnico, permitindo ao usuário se concentrar na lógica do negócio.**
- Sua abordagem se baseia em ativos, transações e suas interações.
- Suporta infra-estruturas já existentes de redes Fabric.

HYPERLEDGER EXPLORER

Tipo: Ferramenta
Status: Incubado

- **Objetiva criar um explorador genérico de blockchain para web**
- Pode ver, invocar, fazer o deploy ou consultar blocos, transações e dados associados
- Atualmente suporta o Fabric, mas está sendo trabalhado para suportar outros blockchains
- Fornece *dashboards* para visualização de informações sobre blocos, logs de nós, estatísticas, smart contracts, transações e qualquer outra informação armazenada no blockchain.
- Pode ser integrado com qualquer plataforma de autenticação/autorização

HYPERLEDGER CALIPER

Tipo: Ferramenta
Status: Incubado

- Ferramenta de benchmark
- Permite os usuários **medirem a performance** de implementações específicas de blockchain com um conjunto pré-definido de casos de uso.
- Gera relatórios contend indicadores como TPS (Transactions Per Second), latência da transação, uso de recursos, etc.
- Permite a escolha do blockchain de melhor desempenho para a aplicação do usuário
- Objetivos do projeto:
  - Permitir visualização em real-time dos principais indicadores
  - Criação de uma GUI que permita gerar a configuração dos testes de maneira mais amigável

HYPERLEDGER URSA

Tipo: Ferramenta
Status: Incubado

Biblioteca criptográfica compartilhada para evitar duplicidades e aumentar a segurança nos demais projetos

Consiste basicamente de 2 sub-projetos:

- "Base Crypto" Library
  - Biblioteca modular e compartilhada de assinaturas.
  - Possui a implementação de diversos esquemas de assinaturas com uma API comum
  - Permite alteração de esquemas de assinatura quase *on-the-fly* (ou usar e suportar diversos esquemas facilmente)

- Z-Mix
  - Oferece uma maneira genérica de criar ZKPs para diversos *building blocks* criptográficos, incluindo assinaturas, *commitments*, e encriptação verificável.
  - Sua ideia central é fornecer uma simples, flexível e segura implementação para construção de ZKPs
  - Consiste em códigos em C, mas também há diversos *wrappers* para outras linguagens de programação

HYPERLEDGER ARIES

Tipo: Ferramenta
Status: Incubado

- Obejtiva principalmente mudar a camada cliente do Indy para ser interoperável com outros **projetos de identidade**
- Sua interface irá suportar o Hyperledger Indy, mas permite a construção de outro DID (incluindo Ethereum)
- Terá um Decentralized Key Management Solution (DKMS), permitndo recovery da sua chave e backup/restore da wallet
- Coompreendido por:
  - Uma camada de interface (*resolver*) para criação e assinatura de transações;
  - Um mecanismo de carteira criptográfica para aramazenamento seguro de segredos
  - Um sistema de mensageria encriptado para interações off-ledger entre clients usando diferentes protocolos
  - Uma implementação ZKP baseada no Ursa.
  - Uma implementação do Decentralized Key Management System (DKMS) do Indy.
  - Um mecanismo para construir protocolos de alto nível tipo API baseado na mensageria
- A Sovrin Foundation é um dos principais contribuidores

Onde encontrar

E ainda:
- ✓ Container
- ✓ On-premisse
- ✓ Cloud privada

Interoperabilidade

Entre os projetos Hyperledger:

Está sendo trabalhada uma arquitetura comum a todos projetos:

- Camada DLT
- Camada Smart contract
- Camada Identidade
- Etc

Criação de building blocks

Definição de APIs padrão

Entre os projetos Hyperledger e outros blockchain:

Indy → Identidade no Corda

Fabric e Burrow → EVM Ethereum

Sawtooth → compatibilidade com contratos Ethereum

Consórcio Hyperledger
→ membro da Ethereum Foundation e vice-versa
→ membro da Ethereum Entreprise Alliance
→ R3 é membro

A Filosofia Hyperledger

Como contribuir com o Projeto

ACCOUNT
Crie sua conta na Linux Foundation

CHAT
Entre no chat de discussão

MAILING LISTS
Assine as mailing lists do Hyperledger

GITHUB
Acesso o código nos repositórios

WIKI
Fique por dentro das últimas novidades

BUG REPORTING
Procure por bugs existentes ou reporte um encontrado

Grupos de Interesse Especial (SIGs)

- Architecture Working Group
- Identity Working Group
- Performance and Scale Working Group
- Learning Materials Development Working Group
- Smart Contracts Working Group

Hyperledger Brazil Chapter

Nossos objetivos são:

- Ajudar a promover a adoção de projetos com Hyperledger
- Desenvolver a comunidade de desenvolvedores e usuários do Hyperledger;
- Promover contribuições para os projetos Hyperledger;
- Desenvolver a comunidade brasileira através de encontros, meetups, e outras atividades;
- Apoiar na geração de conteúdo em português, envolvendo documentação, material de treinamento, dentre outros;
- Aproximar e evoluir a integração com outros países de língua portuguesa.

Comunidades

Local	Membros	Eventos realizados
São Paulo	776	8
Rio de Janeiro	281	2
Brasília	192	2
Fortaleza	192	1
Porto Alegre	195	2
Florianópolis	49	-

O futuro, segundo a Hyperledger

- Cada vez mais as pessoas vão querer compartilhar dados em blockchain
- Não irá existir um único blockchain que se adeque da melhor maneira a todos os casos de uso
- A arquitetura deve ser modular e interoperável
- Idealmente, os módulos de diferentes blockchains devem ser intercambiáveis, e até uma pessoa que não seja expert poderá configurar facilmente um blockchain que atenda da melhor maneira as suas necessidades

Perguntas?

Marcelo Creimer
eZly Tecnologia – Innovation Manager
www.ezly.com.br
marcelo.creimer@ezly.com.br