PROJETO ILIADA

META 3 – REDES DE EXPERIMENTAÇÃO DE APLICAÇÕES BLOCKCHAIN, ARTEFATOS E SUA GOVERNANÇA

Relatório da Atividade:
3.1. Definição de Plataformas, infraestrutura e governança

Definição de Plataformas, infraestrutura e governança

maio 2024

Blockchain em evolução.

PROJETO ILÍADA

PROJETO ILIADA cpqd RNP MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Ciclo de Aprovação e Autoria

Autores	***Data***
Allan Edgard Silva Freitas (IFBA) Bruno Evaristo (CPQD) Billy Anderson Pinheiro (Amachains) Ismael Ávila (CPQD) Luiz Eduardo Folly de Campos (RNP) Ramon da Gama Cordeiro (CPQD)	07/MAI/2024

Revisores aprovadores	***Data***
Barbara Evellyn Santos (RNP) Eduardo Yamamoto Bandin (CPQD) Luiz Eduardo Folly de Campos (RNP) Silvia Helena Marion (CPQD)	09/MAI/2024

Aprovadores Finais	***Data***
Barbara Evellyn Santos (RNP)	13/MAI/2024

SUMÁRIO

1. Introdução

A meta 3 do projeto ILÍADA (Integrando Livros-razão/ledgers, Infraestrutura e Aplicações Descentralizadas) tem como objetivo instalar plataformas blockchain disponíveis publicamente em um conjunto de recursos computacionais administrados pela RNP, CPQD e por instituições da academia ou indústria que tenham interesse em participar da rede. As atividades de disseminação previstas ajudarão a atrair instituições interessadas em compartilhar seus recursos computacionais e a participar da governança da rede. Será necessário realizar um mapeamento mínimo das necessidades do ecossistema de aplicações blockchain para identificar as plataformas mais utilizadas da atualidade e para definir os requisitos técnicos da rede blockchain. A presente meta prevê a participação de especialistas em eventos nacionais e internacionais promovidos pelas organizações de desenvolvimento tecnológico de redes blockchain tais como a Hyperledger Foundation e Ethereum Foundation.

A atividade A.3.1 consiste em realizar as seguintes ações de planejamento: (i) levantamento de projetos de redes blockchain similares no país e no exterior para replicar as melhores práticas; (ii) definição das plataformas blockchain a serem suportadas; (iii) especificação dos recursos computacionais mínimos necessários; e (iv) definição da quantidade de nós de computação que serão alocados pela RNP, CNPq e eventuais instituições interessadas.

2. Objetivo do documento

O objetivo deste documento é apresentar plataformas blockchain que possam ser suportadas no projeto Ilíada, bem como requisitos técnicos de infraestrutura de tecnologia da informação para instanciar nós blockchain, assim como o projeto do primeiro ambiente distribuído entre RNP e CPqD com uma rede blockchain funcional. Este relatório é um dos componentes importantes para garantir a infraestrutura blockchain que suportará as pesquisas em aplicações blockchain a serem desenvolvidas por universidades, instituições de pesquisa e startups. O levantamento de redes blockchain que estão funcionando, bem como o levantamento de plataformas que podem ser suportadas no projeto e suas respectivas configurações são etapas importantes para garantir que o projeto Ilíada atende as necessidades dos interessados, com intuito de garantir que aplicações descentralizadas sejam executadas nas redes blockchain criadas ao longo da meta 3 do Ilíada.

2.1. Público-alvo

Este documento é destinado a todos os envolvidos diretamente e indiretamente na execução do projeto, a saber:

- MCTI;
- RNP;
- CPQD;
- Softex;
- Participantes da chamada da meta 4, ou seja, empresas e universidades.
- Demais instituições que venham a participar da rede distribuída.

3. Contextualização e áreas estratégicas

Nesta seção, serão apresentadas algumas das experiências anteriores relacionadas ao tema Blockchain, desenvolvidas tanto na RNP quanto no CPqD. Essas experiências poderão servir como fonte de informações e orientação para as arquiteturas adotadas no projeto Ilíada. Além disso, será realizado um levantamento inicial das demandas de pesquisa relacionadas ao tema Blockchain, destacando os artigos publicados no Brasil sobre blockchain nos últimos 5 anos. Esse levantamento também fornecerá informações cruciais para as definições e arquiteturas empregadas no projeto Ilíada, contribuindo para a contextualização do ambiente em que a rede do Ilíada está inserida.

3.1. Projetos e iniciativas RNP e CPqD

A seguir serão apresentadas duas iniciativas importantes dentro do tema blockchain, que contribuíram para a experiência da RNP e CPqD nesta área e têm grande potencial de contribuição para o projeto Ilíada.

3.1.1. Identidade Digital Descentralizada

A) Conceitos da Identidade Digital Descentralizada

As primeiras referências sobre Identidade Digital Descentralizada (IDD) datam de 2012, porém as primeiras iniciativas de desenvolvimento ocorreram a partir de 2015 [Reed 2021]. Afinal, o que é a IDD? Infelizmente não existe um consenso. Pode-se dizer que IDD é um conjunto de princípios sobre como o controle de identidade e dos dados pessoais deve funcionar nas redes digitais [Allen 2016].

Do ponto de vista tecnológico, pode-se dizer que IDD é um conjunto de tecnologias que se baseiam em conceitos de gerenciamento de identidade, computação distribuída, Distributed Ledger Technology (DLT), e criptografia. Esses conceitos centrais foram estabelecidos ao longo de décadas. A novidade é como eles são reunidos para criar um novo modelo de gerenciamento de identidade digital.

Embora a IDD esteja muito relacionada com a identidade de pessoas, e suas necessidades individuais de segurança, privacidade e controle de dados pessoais, o modelo também se aplica às organizações e coisas. Na verdade, se aplica a qualquer entidade que precise de identidade segura na internet.

Os modelos baseados em SSI (Self-Sovereign Identity - Identidade Autossoberana) são considerados a camada de identidade da Internet, e possuem as seguintes características [Sovrin 2018]:

- Ausência de uma autoridade central;
- A maioria deles baseada em blockchain;
- Uso de tecnologias baseadas em padrões, com destaque para os esforços do W3C e DIF;
- Centralizado no usuário, pois ele define o que, como e onde seus dados serão apresentados ou utilizados;
- Altos níveis de segurança e privacidade;

- Mecanismos de governança para garantir a confiança entre os membros da rede;
- Conforme com o Regulamento Geral de Proteção de Dados (GDPR) e a lei brasileira de proteção de dados, enfatizando que os dados pessoais não são colocados na rede blockchain.

Um sistema baseado em SSI é constituído pelos seguintes componentes básicos [Reed 2021]:

- Credencial verificável (VCs): trata-se de um conceito chave de um sistema SSI e é a representação digital de credenciais físicas, tais como uma Carteira Nacional de Habilitação (CNH), Registro Geral de Identidade (RG), diploma e certificados, dentre outros exemplos. De acordo com a definição do W3C, a credencial verificável pode representar todas as mesmas informações que uma credencial física representa. A adição de tecnologias, tais como assinaturas digitais, torna as credenciais verificáveis menos vulneráveis e mais confiáveis do que suas credenciais físicas [W3C 2022]. Geralmente, a identidade digital de um usuário de um sistema SSI será composta por um conjunto de credenciais verificáveis;
- Carteira digital: uma carteira digital consiste em software que permite que o usuário gere, armazene, gerencie e proteja chaves criptográficas, credenciais verificáveis, identificadores descentralizados (DIDs) e outros dados privados confidenciais. As carteiras podem ser instaladas em diferentes dispositivos, tais como smartphones e notebooks;
- Agente digital: é um módulo de software que gerencia as interações da carteira com os demais atores do sistema, ou seja, os emissores e verificadores de credenciais. Um agente digital é para uma carteira digital o que um sistema operacional é para um computador ou smartphone;
- Identificador Descentralizado (DID): no nível mais básico, DID é simplesmente um novo tipo de identificador global, não muito diferente das URLs. DIDs são considerados como uma nova camada de identidade digital descentralizada semelhante ao que é a infraestrutura de chave pública (PKI) para a Internet. Os DIDs são a contrapartida criptográfica das credenciais verificáveis e juntos são os considerados os pilares da padronização SSI. Eles foram projetados para serem controlados por seu proprietário, sem qualquer meio centralizado, como uma certificação de autoridade [W3C 2021];
- Registro de dados verificáveis: local onde são registrados DIDs, chaves públicas e schemas de dados das credenciais verificáveis. Pode ser uma blockchain, uma DLT, como por exemplo a Hyperledger Indy [Nakamura 2019] ou outras formas de registros dos dados.
- Conforme mostrado na Figura 1, um sistema IDD pode ser representado pelo triângulo da confiança, que é composto pelos seguintes atores:
- Emissor: na sua maioria, são organizações como agências governamentais emitindo documentos oficiais (CNH, RG, etc), instituições financeiras, universidades emitindo diplomas e outros certificados, corporações emitindo credenciais de empregos, Vale destacar que um indivíduo ou até mesmo uma coisa podem ser emissores, por exemplo, um sensor devidamente equipado pode emitir uma credencial assinada digitalmente sobre a uma leitura [Reed 2021].

- Usuário: são indivíduos, pessoas ou coisas que detêm as credenciais nas suas carteiras digitais e que apresentam comprovantes oriundos de credenciais, quando solicitados pelos verificadores;
- Verificador de credenciais: são aqueles que solicitam credenciais digitais, para realizar alguma ação, por exemplo, liberar o acesso ao serviço digital após verificar a autenticidade, que pode ocorrer em uma blockchain.

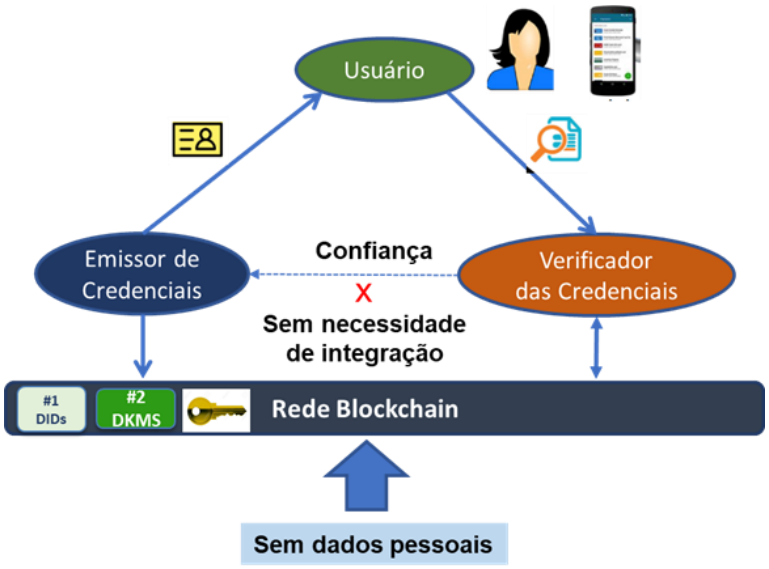


Figura 1-Triângulo da Confiança do Metassistema SSI.

A confiança trazida pelo triângulo, representado na Figura 1, é reforçada por uma estrutura de governança, também denominada de framework de governança, encarregada de especificar as políticas e procedimentos que os emissores devem seguir para emitir uma credencial. Em alguns casos a estrutura de governança específica os termos e condições com os quais os titulares devem concordar em obter credenciais — ou com os quais os verificadores devem concordar em verificar as credenciais. As estruturas de governança também podem especificar modelos de negócios para troca de credenciais, políticas de responsabilidade, seguro e outros requisitos legais e comerciais [Reed, 2021].

B) Experiência do CPQD em IDD

Desde 2016, o CPQD tem se dedicado à exploração e desenvolvimento da Identidade Digital Descentralizada, aproveitando sua expertise em tecnologias blockchain. Através de estudos aprofundados, projetos de pesquisa e desenvolvimento, e a promoção do crescimento do ecossistema de Identidade Digital Descentralizada no Brasil e internacionalmente, o CPQD consolidou sua posição no campo. Essas iniciativas foram impulsionadas por diversos fundos de incentivo à inovação e investimentos próprios do CPQD, resultando na criação de produtos e componentes tecnológicos inovadores, soluções customizadas e produtos adaptados para diferentes plataformas de

Blockchain ou DLTs (Distributed Ledger Technology), incluindo Hyperledger Fabric, Hyperledger Indy, Hyperledger Besu e Corda.

O CPQD colabora com as seguintes comunidades de desenvolvimento e padronização:

- Hyperledger Foundation: Desde outubro de 2018 é membro associado do projeto Hyperledger da Linux Foundation e participa do chapter Brasil deste projeto. Participa ativamente dos grupos de trabalho técnicos, contribuindo para a evolução dos componentes em desenvolvimento;
- Comunidade Sovrin: desde 2019 o CPQD participa da comunidade global de identidade digital descentralizada, participando no conselho da comunidade, mantendo um nó validador e colaborando com as discussões relacionadas com padronização da identidade digital descentralizada e governança de redes de identidade digital;
- DIF – Decentralize Identity Foundation: participa de vários grupos de discussão da organização;
- ABNT – Associação Brasileira de Normas Técnicas: participa do grupo de trabalho ABNT/CB-021 – Tecnologias da informação e Transformação Digital, mais especificamente o subgrupo CE-021:002.307 - Blockchain e Tecnologias Distribuídas, que tem conexão direta com o grupo de trabalho ISO/TC 307.

O CPQD participa das seguintes iniciativas de redes IDD:

- Sovrin: desde junho de 2019 é nó validador da rede global de identidade digital descentralizada denominada Sovrin, que utiliza o framework Hyperledger Indy;
- CT – Blockchain RNP – ID: participou da implantação da rede e, atualmente, participa da operação da rede de identidade digital descentralizada do comitê técnico de blockchain da Rede Nacional de Pesquisa – RNP, que utiliza o framework Hyperledger Indy.

A tabela a seguir apresenta as principais iniciativas realizadas com entidades de governo.

Nome	Descrição e framework DLT utilizado	Entidades envolvidas	Duração (Meses)
FinID – Identidade Digital Descentralizada para o setor financeiro	Desenvolvimento de uma Identidade Digital para o Setor financeiro baseada na identidade digital descentralizada para o Laboratório de Inovação Financeira e Tecnológica (LIFT) do Banco Central, na edição de 2019, usando o framework Hyperledger Indy.	Banco Central, Fenasbac e CPQD	6
RegConID – Registro de	Desenvolvimento sistema de gestão de identidade e	Banco Central,	6

Nome	Descrição e framework DLT utilizado	Entidades envolvidas	Duração (Meses)
Consentimento e Identidade para o Open Banking	consentimento para compartilhamento de dados para a fase 2 do open banking baseado em blockchain para o Laboratório de Inovação Financeira e Tecnológica (LIFT) do Banco Central, na edição de 2020, usando os frameworks Hyperledger Indy e R3 Corda.	Fenasbac, CIP, ABBC, R3 e CPQD	
DvP com Real Digital Tokenizado	Desenvolvimento de um sistema de KYC com credenciais verificáveis reutilizáveis emitidas pela ClearSale para transações de pagamento ante entrega de criptoativos usando real o conceito de CBDC para o Laboratório de Inovação Financeira e Tecnológica (LIFT) do Banco Central, na edição especial "Challenge Real Digital" de 2022, usando os frameworks Hyperledger Aries e Indy	Banco Central, Mercado Bitcoin, Bitrust, ClearSale e CPQD	6
Emissão de Credencial Verificável com dados da Base de Dados do TSE	Prova de conceito desenvolvida em 2019, juntamente com a Secretaria de Governo Digital (SGD) do Ministério da Economia, para emissão de uma credencial verificável do cidadão a partir dos dados do TSE com o objetivo de miticar as fraudes do Gov.Br	CPQD e SGD do ME	9
Uso de Credencial Verificável emitida a partir de adados do Gov.Br	Prova de conceito desenvolvida em 2023, juntamente com a Secretaria de Governo Digital (SGD) do Ministério da Gestão e Inovação dos Serviços Públicos, para emissão de uma credencial verificável do cidadão a partir do cadastro do Gov.Br e acesso aos serviços de governo digital.	CPQD e SGD do MGI	6

Tabela 1-Iniciativas com entidades de governo

A tabela a seguir mostra os projetos de P&D em andamento relacionados com o tema.

Nome	Descrição e framework DLT utilizado	Entidades envolvidas	Duração (meses)
TecSeg – Tecnologias de Segurança	Desenvolvimento de tecnologias de segurança, baseadas em blockchain, para IoT, redes e aplicações 5G e serviços de governo digital. Frameworks a serem utilizados: Hyperledger Fabric, Indy e Besu	Ministério das Comunicações (FUNTTEL), FINEP e CPQD	42
5G Saúde - Segurança privAcidade InclUsão qualiDade na telemEdicina no contexto da Web3.0	Desenvolvimento em tecnologias Blockchain e de Identidade Digital Descentralizada para os desafios da saúde pública no Brasil e as oportunidades advindas da pesquisa, desenvolvimento e integração de tecnologias digitais no dia-a-dia de profissionais e pacientes.	Ministério das Comunicações (FUNTTEL), FINEP e CPQD	30
Agro Trace Chain – ATC Ciclo 2	Desenvolvimento, em parceria com a empresa Safe Trace, da versão para produção do ATC - registro e rastreabilidade na cadeia da carne bovina no Brasil, considerando a identidade digital do boi e do pecuarista. Frameworks: Hyperledger Fabric e Indy	Safe Trace, EMBRAPII e CPQD	15

Tabela 2-Projetos de P&D em IDD

3.1.2. Rede Blockchain Brasil (RBB)

A Rede Blockchain Brasil (RBB) é uma rede fundada pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e o Tribunal de Contas da União (TCU), através de um acordo de cooperação assinado em 2022 pelas duas instituições. O propósito da RBB é ser uma rede público-permissionada nacional disponível para fomento da adoção de tecnologia *blockchain* no setor público Brasileiro permitindo otimização de recursos, redução de custos e superar barreiras para inovação no âmbito público. Assim, a RBB serve como uma ferramenta de fomento de aplicações de interesse público-nacional sobre a tecnologia blockchain.

A sugestão da rede surgiu em um workshop onde setores de tecnologia da informação do governo perceberam que havia diversas iniciativas de *blockchain* em diferentes instituições, entretanto as iniciativas estavam isoladas e enfrentando os mesmos desafios. Então foi proposto unir esforços para coletivamente superar os desafios em comum, integrar as iniciativas e garantir o reuso das soluções entre as organizações. A RBB utilizou como modelo redes implementadas com certo sucesso como LACCHAIN - rede do Banco Interamericano de Desenvolvimento (BID) - com foco na América Latina, ALASTRIA e EBSI (*European Blockchain Service Infrastructure).* Essas redes inspiraram o projeto da RBB para criar uma rede público-permissionada. Ambientes públicos de blockchain são interessantes para a transparência, prestação de contas e confiabilidade. Enquanto que ambientes privados são interessantes no aspecto de segurança de nós e da rede, pois os validadores são entidades previamente conhecidas e autorizadas para fazer parte da rede. Portanto, uma rede público-permissionada atende as necessidades da RBB apresentando a transparência, auditabilidade e confiança, enquanto resguarda a segurança dos nós com menor custo, menor desafio regulatório e tecnológico.

A RBB é uma rede que utiliza o *framework* Hyperledger Besu, o *framework é* compatível com *Ethereum Virtual Machine* (EVM), e permite conectar nós na rede *Ethereum mainnet* (pública), bem como criar redes ou conectar nós em uma rede permissionada. Na RBB é possível instanciar Nós *boot*, *validator*, *writer* e *observer*.

FORMAS DE PARTICIPAÇÃO

A RBB possui três tipos de participantes: partícipes patronos, partícipes aderentes associados e partícipes aderentes parceiros. Os partícipes patronos são: TCU e BNDES. Partícipes aderentes associados são: Dataprev, CPQD, RNP, Prodemge e Prodest. E por fim, partícipe do aderente parceiro PUC-Rio.

Os partícipes patronos têm compromisso de executar nós que auxiliam no consenso da rede (*validator)*, e nas deliberações possuem direito a voto de desempate e veto de propostas apresentadas. Os partícipes aderentes associados possuem o compromisso de executar nós que auxiliem no consenso (*validator*), enquanto que nas deliberações possuem direito a voto. Os partícipes aderentes parceiros possuem o direito de executar nós que enviem transações (*writer)* para a rede e tem acesso a todo o *ledger*, enquanto que nas deliberações possuem direito de apresentar proposta e participar das reuniões. A Figura 1 apresenta a topologia da RBB.

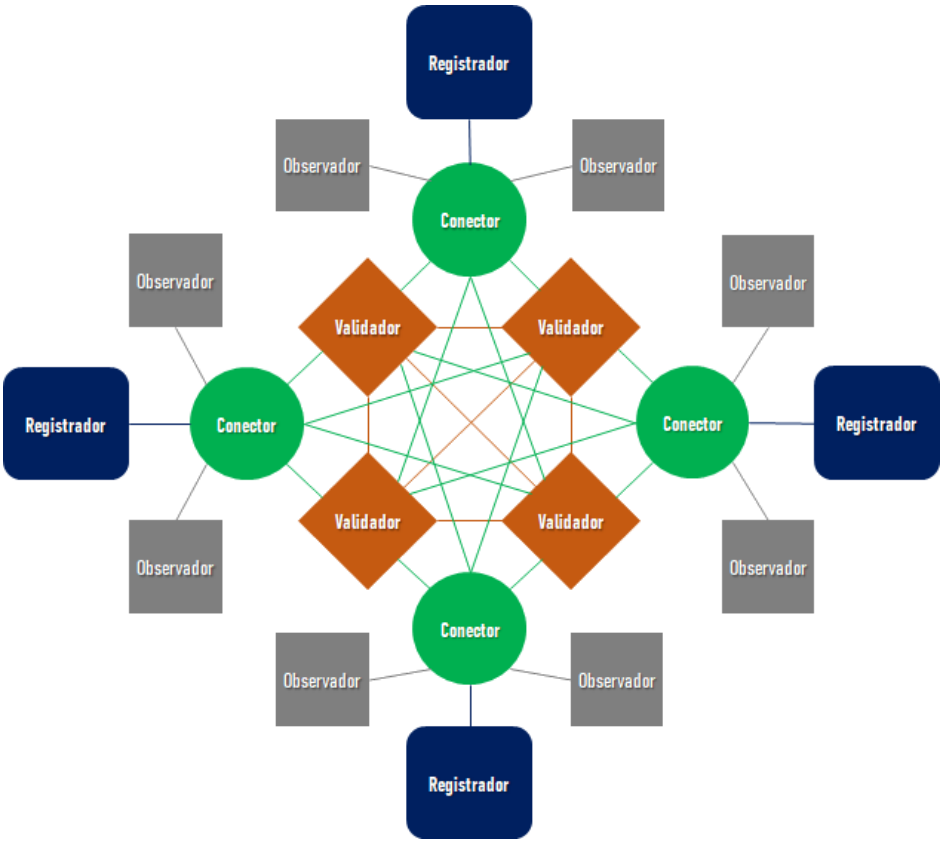


Figura 2- Topologia Rede RBB . Fonte: Rede Blockchain Brasil.-

MODELOS E DEFINIÇÕES

A RBB utilizou inicialmente os modelos de arquitetura e implantação desenvolvidos pela LACChain, de acordo com a Figura 1, configurando nós dedicados do tipo *boot* com conexão remota a outros nós *boot* das outras instituições, nós dedicados do tipo *writer* e do tipo *observer-boot* com conexão local, e nós dedicados do tipo *validator* com conexão local e remota aos outros nós *validator* das outras instituições. Os nós *boot* têm o papel de concentrar as conexões locais, os nós *writer* são usados para leitura e escrita na rede, os nós *observer-boot* são usadas para leitura da rede por outras entidades, e os nós *validator* fazem parte do consenso da rede e escrita da blockchain. Posteriormente a RBB desenvolveu seus próprios scripts de implantação visando personalizar a configuração da rede para suas próprias necessidades.

GOVERNANÇA

A RBB possui governança parcialmente centralizada, sendo as decisões tomadas através dos comitês técnico e executivo. O comitê executivo é responsável por desenvolver e atualizar o regulamento da RBB, decidir sobre aceitação de novos participantes, definir critérios para aceitação de casos de uso e definir esforços necessários para evolução da rede. Por outro lado, o comitê técnico acompanha o funcionamento da rede, propõe ao comitê executivo alterações nos componentes

técnicos da RBB, apoia o comitê executivo nas questões técnicas e evolução da rede, e fornece dados para análises e tomadas de decisões.

3.2. Demanda Acadêmica de pesquisa em Blockchain

O número de publicações acadêmicas sobre blockchain tem se intensificado no Brasil por meio dos eventos da SBC. Um estudo demonstrou um explícito amadurecimento das pesquisas nesse tema e maior disseminação dessas, considerando o aumento notável de publicações no período de 2017 a 2021 [GONÇALVES et al. 2022], indicando diversos eventos que agregam a comunidade científica especializada e os domínios de pesquisa que vem atraindo a atenção dessa comunidade: 21 eventos distintos no Brasil, alguns desses com mais de uma edição somando um total de 37 eventos, e um total de 98 artigos publicados no período de 2017 a 2021. Os artigos foram publicados na trilha principal de simpósios, em workshops, minicursos e salões de ferramentas. Neste documento, tivemos acesso aos dados primários do levantamento citado, e os atualizamos com as publicações até a presente data.

Neste sentido, observamos que o biênio de 2022-2023 incrementa em 53 artigos a produção citada, com o advento inclusive de um evento próprio no Congresso da Sociedade Brasileira de Computação (CSBC), o Colóquio em Blockchain e Web Descentralizada, realizado como sessão especial em evento satélite do CSBC 2022 e como um evento próprio em sua primeira edição oficial no CSBC 2023.

Estes números indicam se manter a tendência de interesse na área, que embora tenha forte apelo nas comunidades de Redes de Computação e Sistemas Distribuídos e de Segurança (as quais detém a maioria dos artigos em eventos por estas organizados), deve-se mencionar que as publicações estão em eventos que envolvem ao menos 7 comissões especiais (CE) da Sociedade Brasileira de Computação (SBC), o que indica blockchain como um tema de interesse para diferentes áreas da computação.

Uma análise mais aprofundada dos microdados extraídos das publicações, indica, quando foi possível obter tal referência, plataformas de interesse estudadas em uma publicação. Uma mesma publicação pode fazer referência ao estudo de mais de uma plataforma, sendo computadas todas as plataformas relacionadas, ou ainda não haver referência alguma, não sendo contabilizado (quando a publicação envolver aspectos teóricos ou mesmo uma abordagem que foi simulada ou experimentada sem se relacionar a uma plataforma de blockchain de uso corrente). A tabela a seguir apresenta este levantamento para o período de 2017-2023.

Plataforma Blockchain	Número de publicações em que é referenciada
Ethereum	45
Hyperledger Fabric	30
Bitcoin	17
Hyperledger Indy	7
Hyperledger Sawtooth	3
Hyperledger Ursa	2
Cardano	2
Hyperledger Aries	2
Neo	2
Hyperledger Besu	1
Casper	1
Monero	1

Tabela 3- Referência a plataformas de blockchain em publicações em veículos e eventos da Sociedade Brasileira de Computação no período de 2017-2023.

Os dados indicam uma predominância de interesse na Ethereum, primeira plataforma a dispor de contratos inteligentes, e no Hyperledger Fabric, primeira plataforma modular para uso permissionado. A Bitcoin foi a terceira plataforma mais citada, uma análise qualitativa dos trabalhos sugere que em muitos casos é por ter sido pioneira, embora provê menos possibilidades de uso tecnológico, pela ausência de mecanismos nativos como os de contrato inteligente existentes em plataformas como Ethereum e Hyperledger Fabric.

Outro aspecto importante é no interesse por plataformas que trabalhem aspectos de identidade digital descentralizada, como o Hyperledger Indy (em alguns casos referenciado de forma combinada com Hyperledger Aries e Hyperledger Ursa).

Por fim, deve-se observar que Hyperledger Besu é uma implementação alternativa da plataforma Ethereum provida pela iniciativa Hyperledger da Linux Foundation, provendo alguma flexibilidade e recursos para desenvolvedores e entidades que queiram utilizar Ethereum em um ambiente mais controlado, e desta forma pode ser um mecanismo adequado para atender a interesses diversos da academia de experimentação com ambiente Ethereum.

Desta forma, a reflexão quanto ao cenário acadêmico nacional sugere plataformas de experimentação de uso geral como Hyperledger Fabric e Ethereum (que pode ser provido pelo Hyperledger Besu), e plataformas de propósito específico para tratar de identificação digital descentralizada, como Hyperledger Indy em combinação ou não com outras plataformas Hyperledger.

4. Plataformas de Blockchain

Uma plataforma blockchain pode ser vista como um sistema distribuído, ou seja, uma camada de software situada logicamente entre a camada de mais alto nível, composta de aplicações, e a camada subjacente composta do Sistema Operacional (SO) e da rede. Sendo assim, é necessário considerar as plataformas blockchain (Hyperledger, Ethereum, Corda, IOTA, dentre outros) [PENNEC 2020], como parte da infraestrutura que darão suporte às aplicações blockchain.

4.1. Requisitos para plataformas e componentes

Para estabelecer as plataformas blockchain, componentes e pilha de software a serem implantados nas redes distribuídas, serão considerados critérios definidos conforme os requisitos das próprias redes de blockchains distribuídas, além das necessidades ou requisitos indicados pelas aplicações e projetos de pesquisa que serão suportados pelas redes implementadas, e das características inferidas através do levantamento das demandas de pesquisa. A seguir, são apresentados os critérios gerais não-mandatórios, porém recomendados para essas indicações:

- Arquitetura OpenSource
- Desenvolvimento ativo
- Comunidade ativa e reconhecida como referência
- Suporte a redes permissionadas
- Suporte a funções de segurança
- Suporte a redes ou transações privadas
- Suporte a conteinerização

Adiante, serão detalhados alguns pontos de definição relacionados aos componentes das redes blockchain, que deverão ser considerados no momento da escolha e definição das redes serem implantadas.

4.1.1. Tipo de Rede

Nesta seção, serão descritos alguns tipos gerais de redes blockchain, cada uma com suas características de tipos de acesso aos nós e dados da rede. Os tipos de acesso e permissões impactam em aspectos como o algoritmo de consenso e também o "trilema blockchain", no qual deve ser definido um equilíbrio entre 3 características gerais que se influenciam mutuamente, que são: a Escalabilidade, a Descentralização e a Segurança.

Quanto à finalidade, existem as blockchains genéricas, desenvolvidas para suportar uma ampla variedade de casos de uso e aplicativos, e as blockchains de aplicação específica, projetadas para atender a um propósito específico ou aplicação, como registros de saúde, cadeia de suprimentos, votação eletrônica, dentre outros. Para o projeto Ilíada, inicialmente serão configuradas redes blockchain de propósito genérico, sendo posteriormente personalizadas de acordo com as demandas dos grupos de pesquisa interessados, ou seguindo as indicações de levantamentos junto à academia, governo ou indústria.

Quanto aos níveis de permissionamento, as redes blockchain podem ser divididas em Públicas, Privadas ou Permissionadas. Esses 3 tipos serão descritos abaixo:

As blockchains públicas, ou não-permissionadas, são caracterizadas pela maior abertura do acesso aos nós e aos dados da rede. Qualquer entidade pode participar como um nó na rede, acessar o histórico completo de transações e contribuir para a validação de novos blocos. Esse modelo tende a apresentar um maior nível de descentralização, no entanto pode incorrer em menores níveis de segurança e desempenho[1]. Blockchains não-permissionadas são sistemas descentralizados planejados para executar e armazenar transações em ambiente aberto, desconfiança mútua e sem atuação de uma autoridade central. Neste tipo de blockchain o acesso e armazenamento do *ledger* é público, e qualquer interessado pode tornar-se um nó na rede, bastando cumprir os requisitos de hardware e aceitar o mecanismo de consenso para ingressar um nó próprio na rede e ter uma cópia do *ledger*. Blockchains não-permissionadas tendem a possuir maior quantidade de nós em relação às permissionadas, e por este motivo tendem a apresentar maior escalabilidade e descentralização, porém dessa forma aumentando os riscos quanto à segurança e privacidade de dados. No aspecto de privacidade, as redes não-permissionadas em geral são pseudo-anônimas, a identificação dos participantes ocorre através chave pública sem a necessidade de identidades do mundo real. As blockchains não-permissionadas são mais suscetíveis a *forks* da cadeia, por causa da natureza dos algoritmos de consenso implementados como o PoW (*Proof of Work*) que implementam segurança probabilística dos blocos de forma que a medida que novos blocos são inseridos após um determinado bloco, menor é a probabilidade deste bloco ser removido ou sofrer alteração, pois que a medida que novos blocos são adicionados torna-se matematicamente inviável a alteração do bloco em questão. Esta forma de realização adição e segurança, bem como outros aspectos do mecanismo de consenso permitem que o último bloco adicionado seja rejeitado por parte dos validadores e aceito por outros permitindo *fork*.

Já as blockchains privadas são restritas a um conjunto selecionado de participantes, geralmente controlados por uma única organização ou por um consórcio de organizações. O acesso à rede e aos dados é limitado e controlado pelas entidades autorizadas, tornando a rede mais centralizada, porém proporcionando um ambiente mais seguro e controlado. Embora possam sacrificar um pouco a descentralização em favor da segurança, esse tipo de rede costuma oferecer maior eficiência e desempenho devido ao controle mais centralizado dos recursos de infraestrutura. Adicionalmente, questões como privacidade podem ser atendidas de forma sofisticada, não só pela privacidade da rede privada como um todo, mas também através de canais privados dentro da rede blockchain, onde há interação apenas entre um subconjunto dos participantes da rede.

Finalmente, blockchains permissionadas representam um meio-termo entre as blockchains públicas e privadas. Nesse modelo, o acesso à rede e aos dados é controlado por um conjunto específico de participantes autorizados, mas esses

[1] Neste contexto, desempenho refere-se à quantidade de transações por minuto suportadas na rede.

participantes não precisam necessariamente confiar uns nos outros. Permitem a participação limitada e controlada de usuários, no qual há confiança parcial entre os membros, normalmente um consórcio responsável pela rede, e disponibiliza um alto grau personalização no permissionamento de escrita e leitura da rede. Em redes permissionadas os dados são privados ou possuem acesso controlado (redes público-permissionadas). Blockchains permissionadas podem possuir maior taxa de transferência de transações (*throughput*), garantem maior segurança e privacidade dos dados, porém são menos escaláveis e apresentam maior centralização que *blockchains* não-permissionadas. Por conta da natureza das *blockchains* permissionadas normalmente há menor quantidade de nós participantes na rede. No aspecto de privacidade, em redes permissionadas os participantes não possuem anonimato, tendo em vista que para participar da rede são necessários acordos, contratos e identificação dos participantes. Porém o acesso de leitura da rede pode ser aberto a entidades anônimas ou a público, de acordo com a natureza da aplicação. Dessa forma esse tipo de rede consegue oferecer um equilíbrio entre a descentralização e a segurança, permitindo que diferentes organizações colaborem em um ambiente confiável e controlado. Blockchains permissionadas podem utilizar algoritmos de consenso aderentes ao princípio de finalidade determinística, como a classe de algoritmos tolerantes a falhas bizantinas, isto é, uma vez que um bloco é adicionado na cadeia, mesmo que seja o último, não poderá ser mais removido, diferente das redes não-permissionadas que a segurança do bloco é probabilística. A finalidade determinística é um princípio importante para blockchains permissionadas, pois garante segurança aos dados adicionados na cadeia, permitindo que empresas e consórcios utilizem a tecnologia blockchain com maior confiança na tecnologia.

O princípio de finalidade em blockchain refere-se ao momento em que se torna impossível remover um bloco anexado na cadeia. Em termos gerais existem as finalidades determinísticas e probabilísticas. A finalidade determinística garante que um bloco é finalizado no momento que é adicionado na cadeia, isto é, não existe a possibilidade de remoção do bloco após a inserção, a desvantagem desta abordagem é o custo adicional de sincronização para garantir finalidade imediata. Em contrapartida, a finalidade probabilística não apresenta garantia imediata, mas crescentes que o bloco não será removido à medida que são adicionados blocos posteriores, de maneira que torna-se mais difícil removê-lo quanto maior for a cadeia depois deste, pois torna-se computacionalmente inviável realizar a alteração ou remoção do bloco em questão. Embora a finalidade probabilística apresente como desvantagem da maior possibilidade de remoção maior em blocos que a finalidade determinística, esta abordagem favorece a disponibilidade dos dados de maneira mais rápida que a finalidade determinística, pois não necessita de sincronização adicional.

4.1.2. Governança

A governança de uma rede blockchain é definida a partir de diversas perspectivas e camadas. Algumas decisões devem ser tomadas tendo em vista o que se define como a camada de confiança humana da solução, o que envolve aspectos do ecossistema de atores envolvidos na solução e dos possíveis papeis que esses podem assumir. Isso inclui a definição de direitos e responsabilidades, por exemplo. Por outro lado, em um nível mais fundamental está a camada de confiança técnica da solução, cuja governança

envolve questões relacionadas à blockchain e seus nós, à gestão de chaves, a protocolos e outros aspectos do nível técnico. Cabe ressaltar que decisões relacionadas à privacidade de dados têm implicações tanto na camada de confiança humana quanto na técnica.

No que trata da estruturação da governança, é recomendável que essa se dê em torno de dois comitês principais: o executivo ou diretivo, responsável por questão da relação entre os atores no ecossistema, e o técnico, que cuida de temas afeitos à infraestrutura sobre a qual se apoia a solução. Opcionalmente, e caso a natureza da aplicação exija, pode-se estabelecer também um comitê de dados, responsável por supervisionar o correto uso dos dados pessoais mantidos pela solução, assegurando sua privacidade.

Entre os temas a cargo do comitê diretivo incluem-se o planejamento estratégico, as ações para adesão de participantes com vistas ao crescimento da rede, e os diversos aspectos legais aos quais a solução está sujeita. Por sua vez, a governança técnica é responsável por deliberar sobre questões como permissionamento de nós, SLA (*Service Level Agreement*), gestão de incidentes, observância de normas e padrões, entre outros assuntos. Por fim, a governança de dados deve ser responsável por incidentes relacionados a vazamento de dados, política de gestão de informações na blockchain e privacidade de dados.

A participação nos comitês pode estar condicionada a aspectos tais como nível de envolvimento de cada ente na iniciativa, os papéis que cada um assume no ecossistema, ou na condição de mantenedor de nó da rede. E, no contexto de uma blockchain permissionada, a quantidade mínima e ideal de nós deve ser levada em conta nas ações de ampliação da iniciativa.

4.2. Frameworks Blockchain

Existem no contexto de blockchain muitos frameworks e redes disponíveis para realizar pesquisa e desenvolvimento, cada uma das opções com propósitos e especificidades técnicas distintas que permitem uma gama de possibilidades de ambientes *testbed*, desta forma é importante antes de realizar a escolha de frameworks, plataformas e redes blockchain, definir o contexto e o propósito do ambiente de experimentação.

No contexto do projeto Ilíada as redes blockchain implementadas devem permitir o acesso público aos dados do *ledger*, porém a participação no consenso deve conter restrições para garantir maior segurança da rede e privacidade de informações sensíveis. Desta forma, redes blockchain permissionadas ou público-permissionadas são mais adequadas para os *testbeds* Ilíada.

A Hyperledger *Foundation*[2] Possui diversos frameworks robustos e amplamente utilizados tanto na academia quanto na indústria com muitos testes, relatórios e artigos

[2] Hyperledger *Foundation* é uma organização subsidiária da Linux *Foundation* com ênfase em fomentar a utilização de *blockchains* de código aberto através dos *frameworks* disponibilizados pela instituição - além de promover eventos, cursos e certificações.

publicados. Seus frameworks são *open source* e recebem apoio de instituições como IBM. Atualmente a Hyperledger possui alguns projetos disponibilizados para utilização em produção: Indy, Fabric, Besu, Iroha, Cacti, Anoncreds, Solang, Caliper, Firefly, Cello, Aries, Bevel e Web3J. Ainda existem outros 50 projetos em fases de experimentação.

4.2.1. Hyperledger Fabric

Hyperleger fabric é uma distributed ledger technology (DLT) com arquitetura modular focado em prover redes blockchains para ambientes corporativos. Nesta tecnologia alguns componentes, como algoritmo de consenso, são módulos plugados que permitem flexibilidade de escolha e implementação do Fabric. A ferramenta permite a implementação de tokens e contratos inteligentes para atender regras de negócio.

O Fabric possui os recursos de canais privados nos quais somente os participantes dos canais possuem acesso às informações compartilhadas nos mesmos. Por conta dos canais privados, participantes da rede podem possuir visões diferentes do ledger, onde os não participantes dos canais privados não possuirão os dados respectivos a estes canais em seus ledgers. A funcionalidade dos canais privados garante maior privacidade no Fabric em relação a outras blockchains permissionadas, e permite que o Fabric seja uma alternativa de grande relevância para blockchains de consórcio entre empresas de competição em um mesmo setor ou ambientes nos quais é necessário a cooperação entre instituições que haja confiabilidade parcial, porém interesses conflitantes.

Os componentes fundamentais de uma rede Hyperledger Fabric consistem em nós, autoridades certificadoras (CAs) e o próprio livro-razão, todos essenciais para o funcionamento do blockchain. Esses elementos arquitetônicos desempenham papéis distintos na rede. Existem três tipos de nós: cliente (client), peer e nó de serviço de solicitação (orderer). Os clientes atuam como representantes dos usuários, transmitindo as transações para a rede. Os pares são responsáveis por manter uma cópia do livro-razão e do estado, e também podem servir como endossantes, validando as transações antes de sua inclusão no livro-razão. O serviço de pedidos inclui classificadores, que garantem que as transações sejam corretamente organizadas em blocos e distribuídas a todos os pares da rede.

No domínio da segurança e confiança da rede, as autoridades certificadoras desempenham um papel vital, fornecendo certificados X.509 que verificam identidades dentro da configuração do blockchain. Esses certificados servem como ferramentas cruciais para reconhecer afiliações organizacionais de componentes e validar transações. Eles garantem que apenas organizações autorizadas possam endossar transações antes de serem incorporadas ao livro-razão.

O próprio livro-razão é um componente importante, registrando todas as transações no blockchain. É mantido por pares, garantindo a integridade e o status do blockchain. O design do livro razão permite a reconstrução histórica do status das transações, proporcionando transparência e confiança nas operações da rede.

Para saber mais sobre esses elementos e suas interações em uma rede Hyperledger Fabric, a imagem abaixo demonstra o estado final de uma rede fabric, onde é possível

verificar a criação das organizações, os canais de comunicação, a integração por meio dos contratos, e os meios de ordenação da configuração da rede.

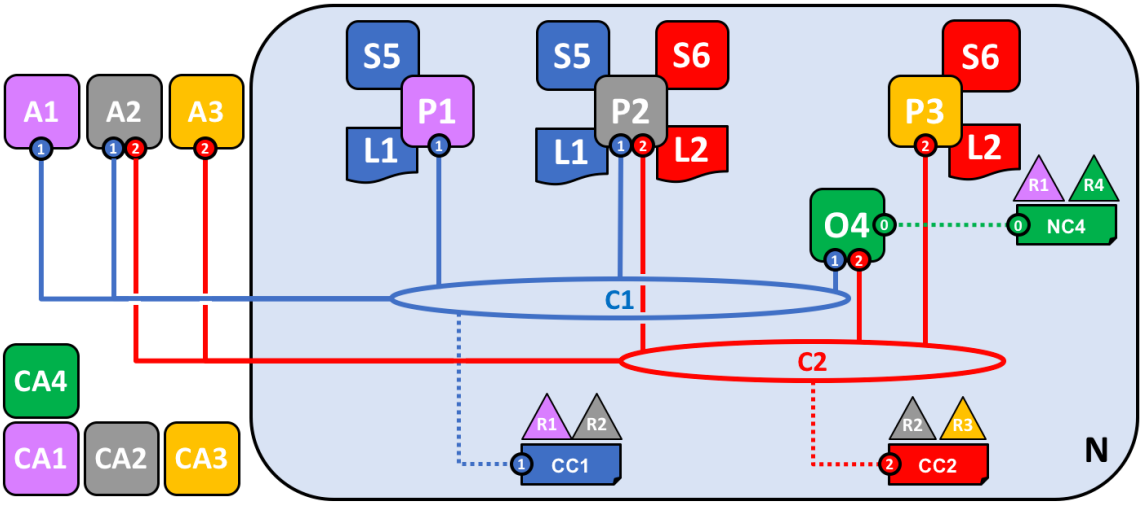


Figura 3-Rede Hyperledger Fabric. Fonte: Hyperledger Foundation, 2023.

Quatro organizações, R1, R2, R3 e R4, decidiram em conjunto formalizar um contrato onde irão configurar e explorar uma rede Hyperledger Fabric. O R4 foi designado para ser o criador da rede – ele tem a capacidade de configurar a versão inicial da rede. O R4 não tem intenção de realizar transações comerciais na rede. R1 e R2 precisam de uma comunicação privada dentro da rede geral, assim como R2 e R3. A organização R1 possui um aplicativo cliente que pode executar transações comerciais no canal C1. A organização R2 possui um aplicativo cliente que pode executar um trabalho semelhante nos canais C1 e C2. A organização R3 tem um aplicativo cliente que pode fazer isso no canal C2. O nó P1 mantém uma cópia do livro-razão L1 associada a C1. O nó P2 mantém uma cópia do razão L1 associada ao C1 e uma cópia do razão L2 associada ao C2. O nó P3 mantém uma cópia do razão L2 associada a C2. A rede é governada de acordo com as regras da política especificada na configuração de rede NC4, a rede está sob o controle das organizações R1 e R4. O canal C1 é governado de acordo com as regras da política especificada na configuração de canal CC1; o canal está sob o controle das organizações R1 e R2. O canal C2 é governado de acordo com as regras da política especificada na configuração do canal CC2; o canal está sob o controle das organizações R2 e R3. Há um serviço de ordem O4 que atua como um ponto de administração de rede para N e usa o canal do sistema. O serviço de ordem também suporta os canais de aplicativos C1 e C2, para fins de ordem de transações dos blocos para distribuição. Cada uma das quatro organizações possui uma Autoridade de Certificação preferida.

As políticas estabelecidas pelas organizações constituintes da rede, como determinar quais organizações têm autoridade para adicionar novos membros, regulam a infraestrutura que suporta a rede blockchain. Nesse contexto, você obterá informações

sobre como os aplicativos utilizam os serviços de contabilidade e contratos inteligentes oferecidos pela rede blockchain.

4.2.2. Hyperledger Besu

Desenvolvido dentro da estrutura Hyperledger, o Hyperledger Besu é um cliente Ethereum de código aberto baseado em Java que funciona perfeitamente em redes blockchain públicas e privadas. Ele suporta a rede pública Ethereum e também pode ser utilizado em redes privadas autorizadas, que são comumente empregadas para aplicações empresariais.

Besu oferece uma variedade de mecanismos de consenso, como Prova de Trabalho (PoW), Prova de Autoridade (PoA) e Tolerância a Falhas Bizantinas de Istambul (IBFT), que contribuem para sua adaptabilidade no atendimento a diversas necessidades e modelos de rede. Esses mecanismos desempenham um papel crucial no governo da rede e permitem que Besu atenda a diversas aplicações, incluindo transações públicas de criptomoedas e transações comerciais privadas e confidenciais.

A modularidade do Hyperledger Besu é uma característica proeminente que permite integração e atualização perfeitas de seus diversos componentes, incluindo o algoritmo de consenso e a camada de rede. Este design modular também promove a colaboração e facilita a integração com outros projetos dentro do ecossistema Hyperledger, aumentando o seu valor no desenvolvimento de soluções blockchain multiplataforma. Besu fornece aos programadores uma variedade de APIs robustas, incluindo JSON-RPC, GraphQL e WebSocket, permitindo interação perfeita com a rede Ethereum, implementação de contratos inteligentes e desenvolvimento de aplicativos descentralizados (DApps). Além disso, o Besu integra recursos avançados de permissão, garantindo que controles de acesso rigorosos sejam mantidos em ambientes empresariais.

Dentro desse contexto, e como dito anteriormente, é possível verificar duas variações e configurações de rede, como por exemplo redes públicas, que atua como cliente de execução em redes Ethereum públicas de prova de participação, como Ethereum Mainnet, Goerli e Sepolia. Que também pode executar o Besu usando prova de trabalho no Ethereum Classic (ETC) .

Na rede privada, na Besu é possível desenvolver aplicativos corporativos que exigem processamento de transações seguro e de alto desempenho em uma rede privada. Uma rede privada é uma rede não conectada à Ethereum Mainnet ou a uma rede de teste Ethereum. As redes privadas normalmente usam um ID de cadeia diferente e prova de consenso de autoridade (QBFT , IBFT 2.0 ou Clique). Também pode-se criar uma rede de desenvolvimento local usando prova de trabalho (Ethash). Besu oferece suporte a recursos empresariais, incluindo privacidade e permissão.

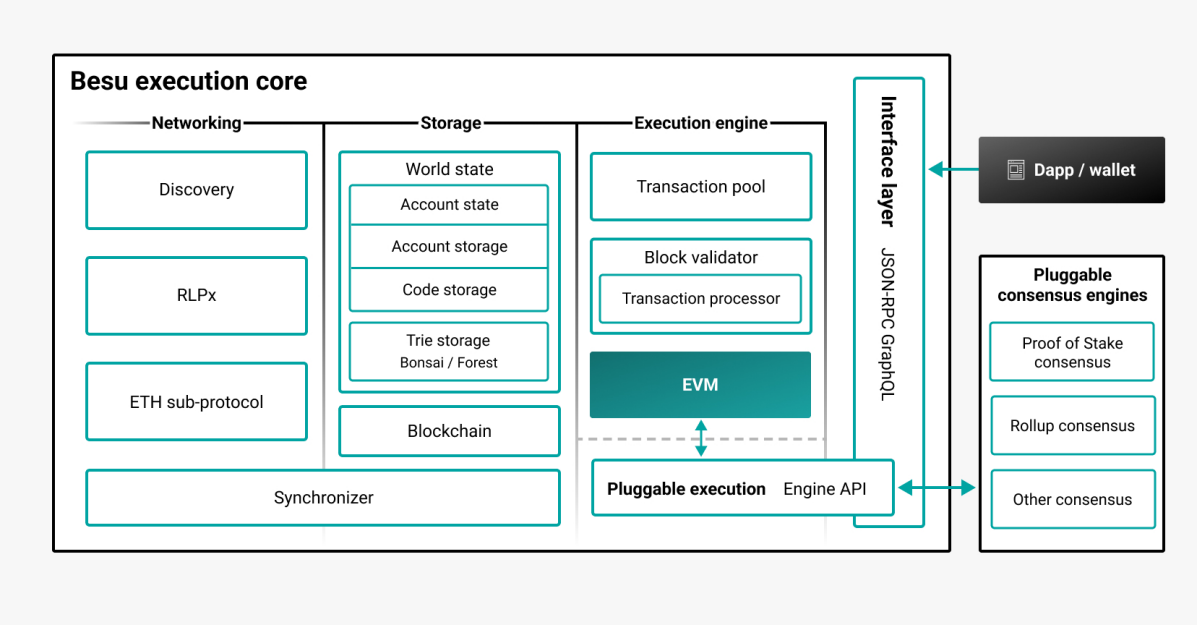


Figura 4-Diagrama de arquitetura da Rede Hyperledger Besu redes públicas. Fonte: Hyperledger Besu, 2023.

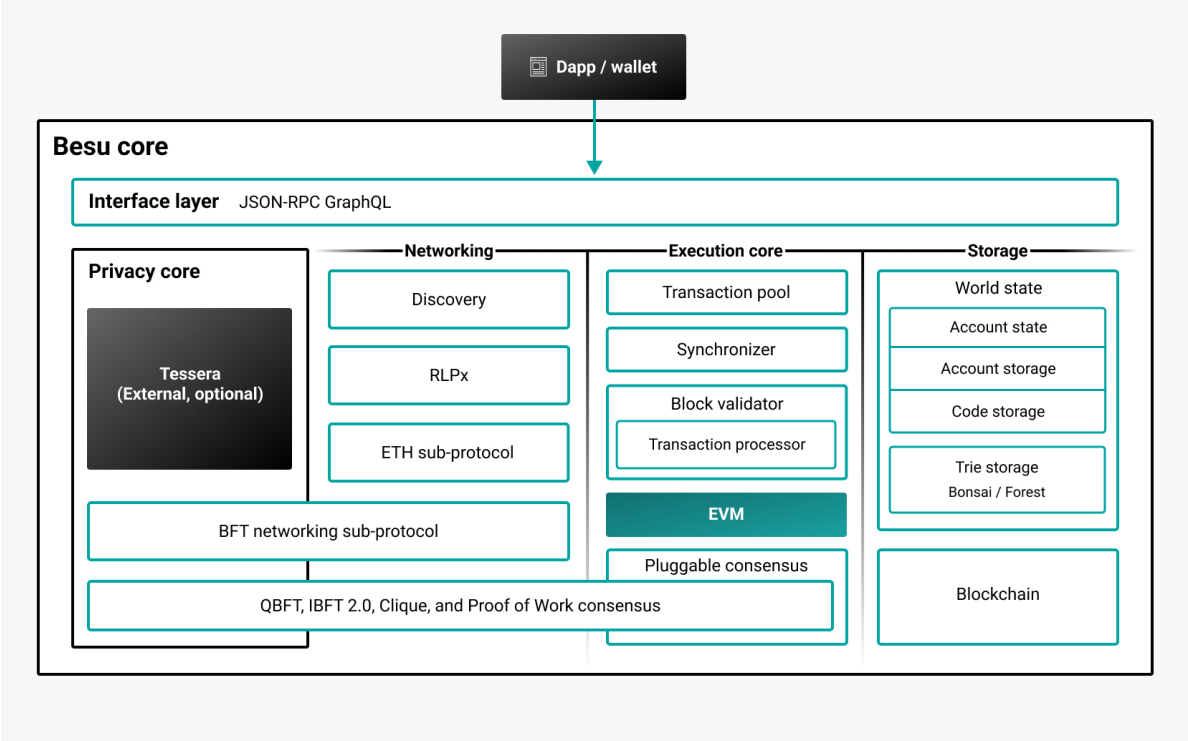


Figura 5-Diagrama de arquitetura da Rede Hyperledger Besu redes privadas. Fonte: Hyperledger Besu, 2023.

4.2.3. Hyperledger AnonCreds

AnonCreds é um novo projeto Hyperledger que permite credenciais verificáveis com privacidade aprimorada. A tecnologia em si não é nova, pois originalmente fazia parte do Hyperledger Indy, o projeto de registro de identidade digital. No entanto, agora ele foi

separado do Indy para que possa ser usado para credenciais verificáveis em ledgers como Hyperledger Fabric ou Hyperledger Besu baseado em Ethereum, ou outros.

O conceito central que sustenta AnonCreds, Indy e Project Aries é permitir que os usuários compartilhem dados de identidade com outras pessoas, mas apenas quando necessário. Por exemplo, em um bar, alguém pode provar que tem idade para beber e talvez compartilhar uma foto vinculada à credencial sem revelar seu nome e endereço.

AnonCreds, que significa Anonymous Credentials, usa criptografia Zero Knowledge Proof (ZKP) para permitir esses tipos de divulgações seletivas. O conceito pode funcionar bem para algumas aplicações e talvez menos para outras. Se um processo financeiro envolver a conformidade com o seu cliente, pode ser necessário compartilhar alguns dados e, certamente, seu nome.

No setor de identidade digital, o AnonCreds tem atraído um pouco de polêmica. AnonCreds é anterior ao padrão de credenciais verificáveis do W3C e não cumpre totalmente. Ele também usa criptografia que não é aprovada pelo NIST (não está sozinha). No entanto, algumas das críticas foram refutadas (e aqui). E o fato de haver 25 patrocinadores de projetos demonstra a extensão de seu apoio. Ao mesmo tempo, o projeto AnonCreds parece disposto a revisitar o esquema de assinatura (criptografia) e, no futuro, apoiar a apresentação de credenciais usando o modelo de dados W3C.

MOTIVAÇÃO

A motivação para criar o Hyperledger AnonCreds é extrair uma importante tecnologia de credencial verificável que protege a privacidade de ser explicitamente vinculada ao Hyperledger Indy e permitir seu uso com qualquer registro de dados verificável (VDR) apropriado. Embora o Hyperledger Indy seja uma plataforma fantástica para compartilhar objetos AnonCreds, não é o único, e essa transição do AnonCred para um projeto autônomo permite que usuários investidos em outras plataformas de armazenamento distribuído usem AnonCreds.

AnonCreds é importante porque se baseia em vários recursos importantes de proteção de privacidade baseados em ZKP que não estão atualmente disponíveis com outros tipos de credenciais verificáveis. Esses incluem:

O ato de apresentar reivindicações de credenciais verificáveis da AnonCreds não expõe identificadores correlativos para o titular. Isso é particularmente importante para alguns governos, pois significa que o uso de credenciais verificáveis do AnonCreds não requer a introdução de um novo identificador para indivíduos e a correspondente sobrecarga legislativa que isso cria. A não correlação de apresentações de detentores para verificadores aborda as crescentes tendências globais de regulamentação de privacidade, como GDPR .

A AnonCreds apóia a noção de um "segredo de link" baseado em ZKP que permite a vinculação de credenciais emitidas a um detentor e a vinculação de várias credenciais apresentadas juntas ao mesmo secretário/proprietário do link.

O AnonCreds permite a minimização do compartilhamento de dados, suportando tanto a divulgação seletiva (compartilhando apenas algumas declarações em uma credencial) quanto os predicados ZKP (comprovando uma expressão baseada em declaração, como "Tenho mais de 21 anos" com base na data de nascimento sem ter compartilhar a data de nascimento).

A apresentação verificável do AnonCreds pode incluir reivindicações derivadas de credenciais verificáveis de várias fontes, com uma vinculação provando que as credenciais foram todas emitidas para o mesmo titular.

As apresentações verificáveis usando AnonCreds são derivadas de suas credenciais verificáveis de origem e, portanto, o titular não está fornecendo ao verificador sua credencial verificável bruta/original.

Ao separar AnonCreds de Indy, uma adoção mais ampla de AnonCreds é permitida, pois os grupos que consideram o uso de AnonCreds não estariam limitados a uma implementação baseada em Indy. Com uma base de usuários mais ampla, surge um interesse adicional na evolução dos AnonCreds, e esperamos ver como resultado um interesse adicional de criptógrafos aplicados. Embora muitos tenham implantado com sucesso soluções baseadas em AnonCreds em todo o mundo, não é uma solução perfeita e precisa continuar a evoluir. A revogação nos AnonCreds de hoje é menos do que ideal. Outros esquemas de assinatura prometem AnonCreds "melhores e mais rápidos". Com o AnonCreds como um projeto autônomo, os esforços na próxima geração de AnonCreds serão um foco. Tais evoluções devem reter os recursos de proteção de privacidade dos AnonCreds, como não correlação, divulgação seletiva, predicados e de vinculabilidade.

As principais características do que faz um AnonCred existirem em dois níveis distintos:

- **Nível ledger:** O que deve ser escrito em um registro de dados verificável para que os AnonCreds sejam criados e funcionem na prática;
- **Nível de credencial e SDK:** Quais técnicas criptográficas devem ser empregadas em um SDK para fornecer aos AnonCreds seus recursos de preservação de privacidade.

Para a pilha AnonCreds existente, no Hyperledger Indy, esses dois níveis podem ser representados pela Figura abaixo:

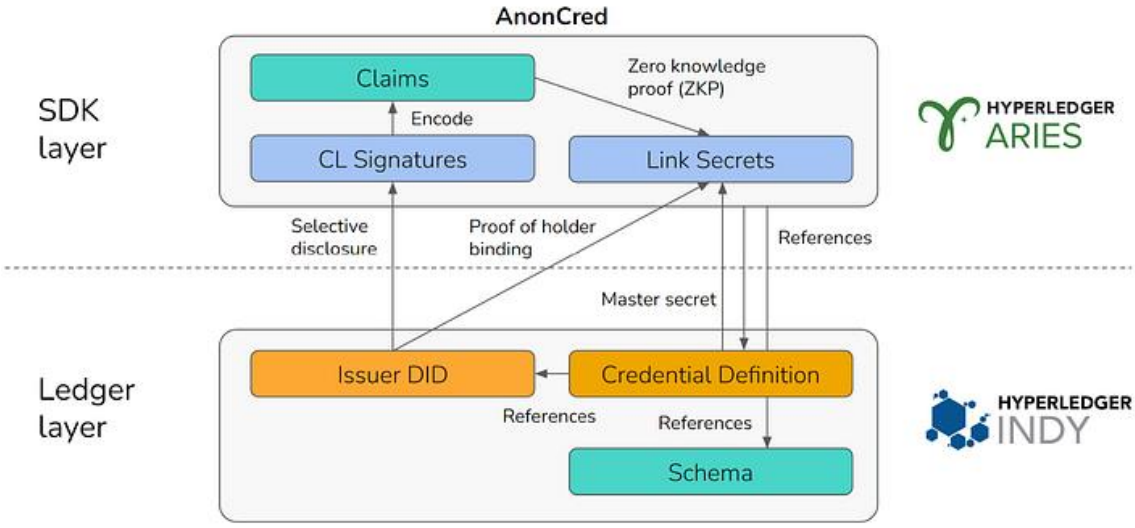


Figura 6-Arquitetura de comunicação Aries e Indy. Fonte: Hyperledger Foundation, 2023.

Hyperledger Indy é importante para AnonCreds, pois até o momento é a única blockchain de identidade que pode oferecer suporte nativo a transações de DIDs, esquemas, definições de credenciais (e registro de revogação opcional) gravadas no livro-razão. Os AnonCreds podem ser apresentados no formato padrão W3C VC Data Model, e as próximas etapas para o modelo incluem alcançar a conformidade com o W3C Verificable Credentials Data Model Standard.

ARQUITETURA

A seguir, mostramos como o componente AnonCreds irá interagir com os diversos componentes de um Agente SSI, o serviço de gerenciamento de chaves para um Agente, outros Agentes e Registros de Dados Verificáveis (VDRs). Observe os métodos AnonCreds Registrar e Resolver que definem o comportamento de gravação e leitura de AnonCreds para um VDR específico.

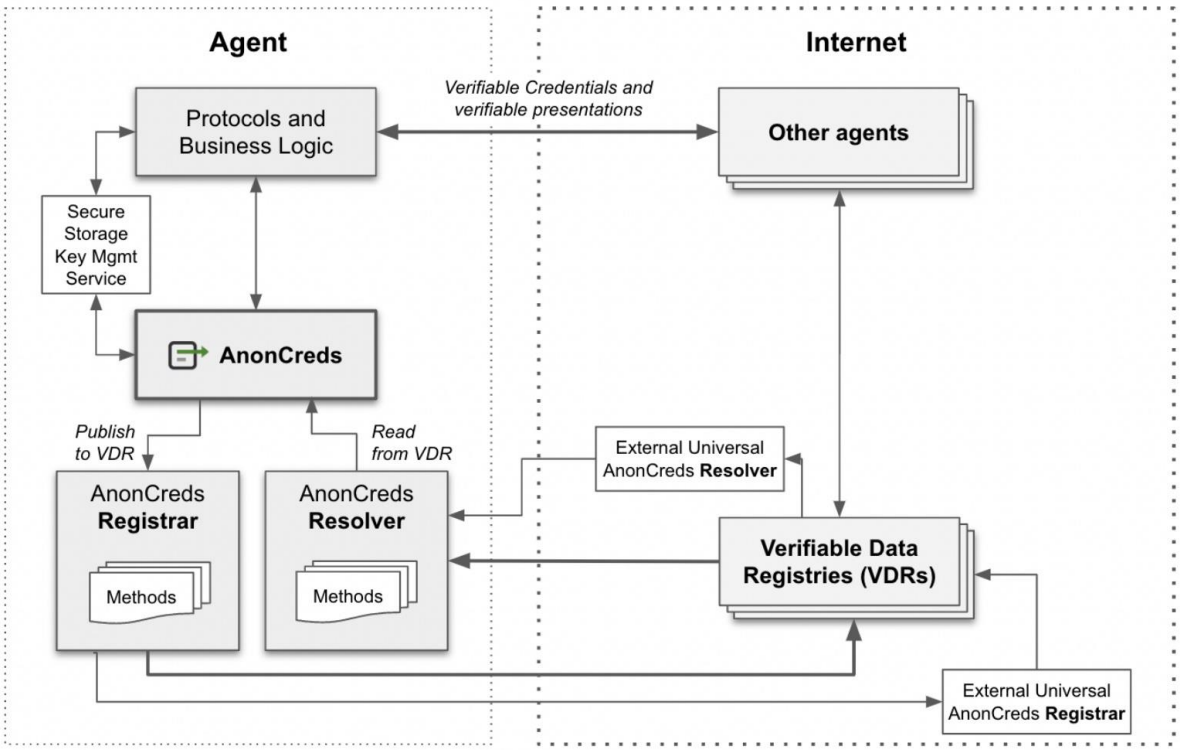


Figura 7-Interação componentes AnonCreds. Fonte: Hyperledger Foundation, 2022.

A arquitetura "to-be" é conceitualmente semelhante ao que temos hoje com o Hyperledger Indy, estendida separando AnonCreds em sua própria biblioteca e formalizando APIs independentes de razão entre AnonCreds e os métodos Registrar/Resolver. Conforme indicado pelo número de implementações independentes já criadas usando as bibliotecas AnonCreds existentes (6 e contando...), o ajuste das APIs é um esforço relativamente pequeno. É claro que, com a implementação de APIs de registrador/resolvedor, fica muito mais fácil usar VDRs além do Indy, especialmente para casos de uso somente de resolvedor (titular e verificador). Além de uma mudança nas dependências dentro do Aries Frameworks, deve haver pouco ou nenhum impacto no uso de AnonCreds pelas implementações existentes.

A comunidade mais ampla e o subsequente foco mais amplo no AnonCreds "Next" trarão melhorias significativas nas capacidades, especialmente nas áreas de revogação e esquemas de assinatura adicionais que retêm os recursos do AnonCreds.

4.2.4. Hyperledger Indy

Hyperledger Indy é um projeto de código aberto da Linux Foundation, sob o guarda-chuva do Hyperledger, focado em prover uma base para identidades digitais descentralizadas. Seu objetivo é criar uma infraestrutura que permita aos usuários terem controle total sobre suas identidades digitais, de forma segura e privada, sem a necessidade de uma autoridade central.

Indy oferece ferramentas e bibliotecas que permitem a emissão, posse, e verificação de credenciais digitais que são interoperáveis através de blockchains e outras infraestruturas. Isso facilita a construção de aplicações que requerem identidades confiáveis, como sistemas de votação, registros de saúde eletrônicos, e gerenciamento de identidades corporativas.

Um dos principais componentes do Indy é a utilização de tecnologia blockchain para criar um registro imutável de identidades, proporcionando segurança e transparência. Outro conceito central é o de "Self-Sovereign Identity" (SSI), ou Identidade Autossoberanas, que coloca os indivíduos no controle de suas próprias identidades digitais, permitindo-lhes compartilhar seletivamente partes de suas identidades com terceiros de maneira segura e verificável.

Hyperledger Indy usa uma abordagem descentralizada para resolver os desafios associados à gestão de identidades digitais, promovendo privacidade, redução de fraudes, e interoperação entre diferentes sistemas e organizações.

OPERAÇÃO DAS REDES

O gerenciamento de identidades digitais vem se modificando constantemente conforme a internet e suas tecnologias vão avançando e ganhando maior importância e criticalidade. A seguir é pontuado alguns desses principais modelos de gerenciamento de identidade relacionados a redes blockchains, além do processo de configuração de uma rede Hyperlegder Indy.

INDY DISTRIBUTED LEDGER

O Registro Distribuído Indy é formado por dois projetos: Indy-Node e Indy-Plenum, como mostrado na figura a seguir. Indy-Plenum é um Registro Distribuído de propósito geral, onde fica implementado o algoritmo de consenso, já o Indy-Node é uma especialização do Indy-Plenum, onde são implementadas as transações específicas relacionadas à identidade. Indy-Node implementa um plugin no Indy-Plenum que adiciona as transações específicas para o gerenciamento de identidade, fazendo com que seja possível a inserção de novos plugins(nodes-indy).

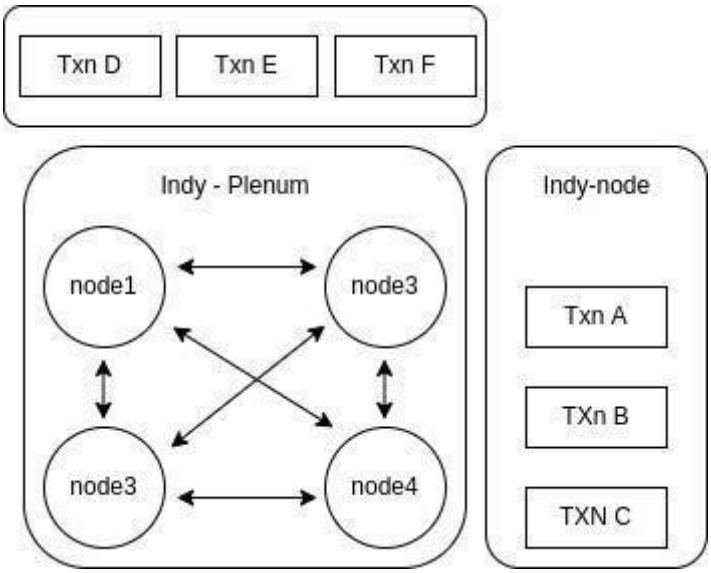


Figura 8-Hyperledger Indy é composto pelo Indy-Node e Indy-Plenum.

CONJUNTO DE NÓS

Existem dois conjuntos de nodos na implementação do hyperledger Indy, sendo eles o conjunto *Validators* e o conjunto *Observer*:

- O *Validator* é quem gerencia a escrita, são os nodos que de fato participam do protocolo de consenso;
- *Observer:* serve para gerenciar a leitura.

TIPOS DE REGISTROS DISTRIBUÍDOS

- **Config Ledger**

  Primeiro temos o Config Ledger, onde ficam registradas informações a respeito das validações de transações, políticas de autorização e etc. São informações/configurações que todos os nodos devem saber em consenso. Os nodos leem esse Registro para estar a par dessas configurações.

- **Pool Ledger**

  No Pool Ledger ficam registradas informações sobre o estado atual do Conjunto de Nodos – quem são os nodos, suas chaves públicas, ips e etc – Toda transação que adiciona, remove ou edita nodos é registrada aqui. Mais uma vez, todos os nodos da rede leem desse Registro para saberem quem são os outros nodos do Conjunto de Nodos e como se comunicar com eles. Esse Registro precisa de um "motor de arranque" que é o arquivo Gênesis. Como todas as informações sobre o Conjunto de Nodos estão armazenadas no próprio Pool Ledger, então, quando o Pool Ledger está em branco, iniciando do zero, ele não possui informação nenhuma sobre o Conjunto de Nodos. Não é possível saber quem faz parte do

pool, quais seus ips e etc. O arquivo Gênesis é esse "motor de arranque" que faz as primeiras transações no Pool Ledger – ao rodar pela primeira vez, ele lê o arquivo Gênesis e escreve no Pool Ledger. O arquivo Gênesis deve conter as informações iniciais do Conjunto de Nodos (quem são os nodos, quais seus ips, etc), assim quando um nodo roda pela primeira vez ele sabe onde conectar. O arquivo Gênesis é lido apenas na primeira vez que o Pool Ledger é executado. Após as transações iniciais do arquivo Gênesis, seguem no Pool Ledger todas as transações subsequentes referentes ao Conjunto de Nodos, como mostrado na Figura abaixo.

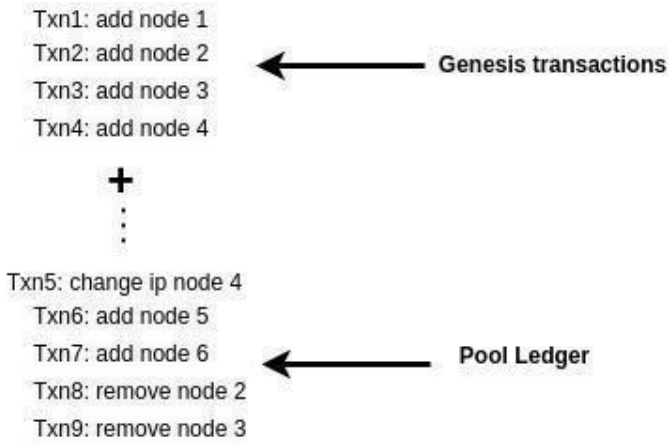


Figura 9 - Pool Ledger.

- **Domain Ledger**

  O Domain Ledger é o Registro principal, onde ficam as transações específicas de identidade e de aplicação. De forma análoga ao Pool Ledger, o Domain Ledger também precisa de um arquivo Gênesis. Para escrever no Registro é necessária uma identidade com papel/permissão de escrita, porém as informações sobre todas as identidades encontram-se no próprio Domain Ledger, se o Registro está em branco, não há como criar nenhuma identidade nova pois não existe autorização para escrever no Registro. Novamente o "motor de arranque" é necessário. O arquivo Gênesis escreve as primeiras transações no Registro, colocando algumas identidades que possuem papel que permitam a escrita – registra o usuário inicial que adicionar os outros. A Figura 3 representa o Domain Ledger. Na sequência às transações do arquivo Gênesis, seguem todas as transações subsequentes de identidade e de aplicação.

- **Audit Ledger**

  O Audit Ledger é o Registro responsável pela sincronização entre as diferentes Ledgers. Esse Registro monitora as outras Ledgers e ordena todas as transações de todas as Ledgers em uma sequência que representa todas as transações do

sistema de forma ordenada. Esse registro é utilizado para recuperação do sistema e também para auditorias externas, além de gerar controle e coesão interna para o sistema.

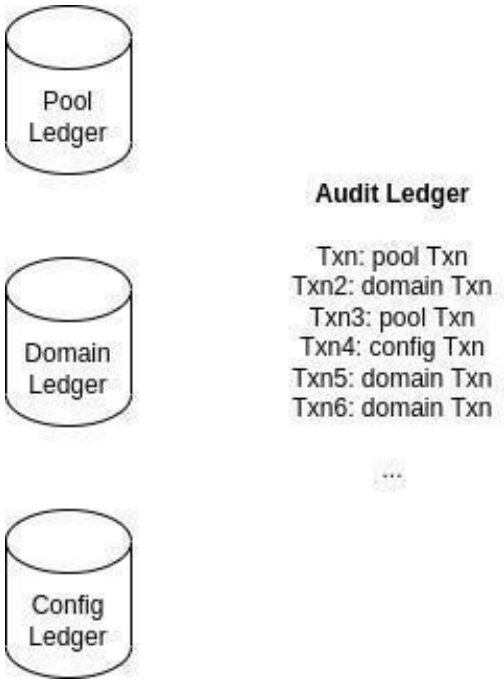


Figura 10-Audit Ledger.

4.3. Componentes Blockchain Modulares

Dentro do ecossistema Hyperledger, os módulos Hyperledger Aries e Hyperledger Ursa têm importância significativa, pois cumprem funções distintas no avanço de tecnologias blockchain seguras e eficientes para vários casos de uso.

O Hyperledger Aries serve como uma estrutura colaborativa que promove a transferência de dados criptografados no blockchain, fomentando o desenvolvimento e o controle de identidades digitais descentralizadas e compatíveis. Seu objetivo é estabelecer um meio de comunicação confiável e confidencial entre entidades digitais. Aries fornece uma plataforma não apenas para a troca de credenciais de identidade digital, mas também para facilitar diversas transações de dados entre os participantes, aproveitando a segurança e a confiabilidade da tecnologia blockchain.

Ursa, uma biblioteca colaborativa de criptografia, visa eliminar a necessidade de esforços redundantes de implementação e minimizar erros, incentivando a reutilização de código criptográfico comumente usados. Seu principal objetivo é oferecer aos desenvolvedores de blockchain uma variedade abrangente e confiável de ferramentas criptográficas e primitivas que priorizam segurança, flexibilidade e qualidade. Através da consolidação de funções criptográficas em uma única biblioteca, a Ursa agiliza auditorias de segurança, inspira confiança na implementação criptográfica e aumenta a eficiência do desenvolvimento de aplicações blockchain.

Resumindo, o principal objetivo do Hyperledger Aries é estabelecer e lidar com identidades digitais descentralizadas, permitindo interações seguras e verificáveis. Por outro lado, o Hyperledger Ursa fornece uma estrutura criptográfica forte que pode ser utilizada não apenas pelo Aries, mas também por outros projetos Hyperledger e comunidades de software. Seu objetivo é garantir a segurança das transações e dados no blockchain. Tanto Aries quanto Ursa são componentes vitais para melhorar a segurança, interoperabilidade e eficácia das soluções blockchain.

4.3.1. Hyperledger Ursa

A Hyperledger Ursa é uma biblioteca criptográfica compartilhada e usada para evitar a duplicação de códigos criptográficos. Ela é um repositório opcional voltado à implementação e ao uso de criptografia.

Está disponível no projeto Ursa uma abrangente biblioteca de assinaturas modulares e primitivas de chave simétrica, a fim de que os desenvolvedores possam inserir e excluir diferentes esquemas criptográficos, por meio da configuração, sem precisar modificar seu código. Além dessa biblioteca básica, a Ursa também inclui criptografia mais recente, tais como assinaturas agregadas, de limite e baseadas em pareamento. Além dessas assinaturas, também serão incluídas primitivas de conhecimento zero (Zero Knowledge Protocol - ZKP), incluindo SNARKs. O projeto Hyperledger Ursa identificou os seguintes benefícios:

- Evita a duplicação de solução de requisitos de segurança semelhantes em diferentes implementações de blockchain;
- As auditorias de segurança de operações criptográficas são mais simples de analisar quando o código é consolidado em um único local. Isso reduz os esforços de manutenção dessas bibliotecas e melhora os rastros de segurança para aqueles desenvolvedores que porventura tenham menos experiência com projetos de livro-razão distribuído;
- As revisões de especialistas ocorrem em todos os códigos criptográficos, a fim de reduzir a probabilidade de erros de segurança;
- A interoperabilidade entre plataformas que exigem verificação criptográfica melhora quando estas utilizam os mesmos protocolos de segurança;
- A modularidade de componentes comuns estabelece a estrutura para futuras plataformas de tecnologia de livro-razão distribuído modular que compartilham os mesmos componentes. Uma implementação de referência bem-sucedida de um componente comum, como segurança, cria oportunidades futuras;
- Novos projetos conseguem acelerar seu tempo de lançamento no mercado se um paradigma de segurança existente puder ser conectado, em vez de ser refeito em cada caso.

4.3.2. Hyperledger Aries

A biblioteca Aries possui uma camada de interface para criar, assinar e ler transações na blockchain. Fornece suporte para trocas e emissão de Credenciais Verificáveis, incluindo credenciais que utilizam as premissas de zero conhecimento, encontrados na biblioteca Ursa. Aries permite interações ponto-a-ponto baseado em identidades

descentralizadas, e suporta diversos registros distribuídos diferentes. Junto com Hyperledger Indy e Hyperledger Ursa, faz parte dos projetos Hyperledger voltados para implementação de sistemas de Identidade Auto-Soberana.

ARIES AGENT

Um Agente é uma peça de software com o propósito de interagir com outras entidades, via DIDs e também por outros meios. Uma instância de um Agente Aries é composta por duas partes, o agente e o controlador.

- Aries Agent é o responsável por gerir as funcionalidades principais do Aries (HYPERLEDGER, 2021), incluindo interação com outros agentes, gerenciamento de armazenamento seguro, além de troca de mensagens com o controlador;
- O controlador é quem provê a lógica de negócio, indicando como o agente deve responder a eventos. O Agente envia notificações de evento para o controlador, que por sua vez analisa a melhor resposta e envia mensagens administrativas para o Agente. A comunicação entre os dois é feita por meio de webhooks e chamadas HTTP.

Assim, para desenvolver projetos com o Aries, na maioria dos casos basta programar o controlador, que proverá a lógica de negócios. Na arquitetura de uma rede utilizando Hyperledger Indy e Hyperledger Aries, existem diversos agentes. Os agentes que se encontram nas "bordas" desta rede, são aqueles contidos em celulares, tablets, computadores, etc. Temos também os agentes na "nuvem" que oferecem roteamento de mensagens. Assim, geralmente, enquanto os agentes da "borda" são pessoas e organizações, os agentes da nuvem têm principalmente como lógica de negócio o roteamento de mensagens entre agentes. Mensagens enviadas entre dois agentes da borda são roteadas por agentes na nuvem.

COMUNICAÇÃO

A comunicação entre agentes acontece por meio de um mecanismo de mensagem chamado DIDcomm (DID Communication). DIDcomm permite uma troca segura e assíncrona de mensagens encriptadas ponto-a-ponto, que geralmente são roteadas por meio de agentes Aries intermediários. A criptografia é feita pela biblioteca Hyperledger Ursa.

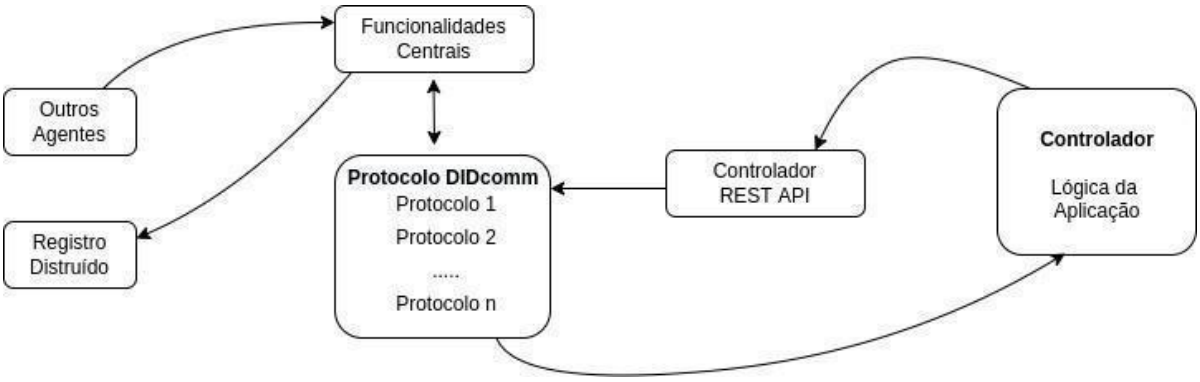


Figura 11 - Estrutura interna de um Agente Aries.

O mecanismo usa uma instância do método did:peer DID method, que faz uso de DIDs não publicados na blockchain, utilizados apenas de forma privada entre os dois agentes que se comunicam. Entre os protocolos padrões definidos, que configuram um conjunto de mensagens para realizar determinada tarefa, podemos destacar:

- O protocolo "estabelecer conexão" (establish connection) que permite a conexão de dois agentes por meio de um conjunto de mensagens: o convite, a requisição de conexão e a resposta de conexão;
- O protocolo "emitir credencial" (issue credential) que permite um agente emitir uma credencial para outro agente;
- O protocolo "apresentar prova" (present proof) permite que agentes façam requisições e recebam provas de outros agentes.

5. Arquitetura Blockchain e Infraestrutura de Computação

Em adição aos tipos de blockchain e das plataformas blockchain apresentadas na sessão anterior, nesta seção são apresentadas as opções gerais de arquitetura das principais plataformas quanto a mecanismos de consenso, tipos de nós, e quantidade de nó para cada organização participante, assim como seus requisitos de hardware.

Também serão apresentadas opções para a infraestrutura de software para suportar as redes blockchain e também algumas ferramentas de automatização dos processos de implantação e gerência de redes blockchain.

5.1. Algoritmos de consenso

Em geral, a definição do algoritmo de consenso depende da tecnologia que será implementada. Alguns *frameworks* possibilitam a escolha de um algoritmo dentre as possibilidades compatíveis com o *framework*, outras tecnologias possuem compatibilidade com apenas um algoritmo de consenso. As ferramentas da Hyperledger (Fabric e Besu) possuem compatibilidade com mais de um algoritmo de consenso.

Os algoritmos de consenso podem ser classificados de diversas maneiras, dentre elas o modo como o algoritmo previne ataque Sybil. Os algoritmos de prova de trabalho (*Proof of Work - PoW*) previnem ataque Sybil requerendo que um nó aplique esforço computacional para resolver um desafio criptográfico para ter o direito de adicionar o próximo bloco na cadeia. A classe de algoritmos de prova de participação ou participação detida (*Proof of Stake - PoS*) previne ataques Sybil bloqueando recursos do nó (normalmente token) temporariamente, até que o participante possa adicionar bloco na cadeia. Enquanto que a classe de algoritmos de prova de autoridade (Proof of Authority - PoA) previne ataque Sybil concedendo permissão para um nó, dentro de um grupo conhecido e pré-definido, para adicionar o bloco na cadeia. Os nós que possuem permissão de adicionar blocos na cadeia são conhecidos de validadores.

Algoritmos de consenso de prova de autoridade são em geral utilizados em blockchains privadas, permissionadas ou público-permissionadas, onde as instituições participantes da rede são conhecidas e existem requisitos legais de participação. Os algoritmos de prova de autoridade implementam variações de soluções para o problema dos generais bizantinos. Em geral os algoritmos com denominação *byzantine fault tolerance* em redes permissionadas são algoritmos de prova de autoridade.

Os algoritmos de consenso possuem o desafio do trilema blockchain: segurança, escalabilidade e descentralização. De acordo com o propósito da blockchain um destes itens terá mais foco enquanto o restante apresentará menos efetividade. Um exemplo é a rede Ethereum em que o consenso é adequado para prover boa descentralização, entretanto é pouco escalável ocorrendo até atrasos na rede por excesso de transações na fila. Por outro lado, os algoritmos de redes privadas de maneira geral possuem melhor performance e conseguem processar mais informações, porém essas redes geralmente apresentam um alto grau de centralização.

O algoritmo de consenso escolhido também pode influenciar o número mínimo de nodes em uma rede blockchain. Abaixo será discutido o algoritmo de consenso das plataformas citadas anteriormente.

5.1.1. Hyperledger Besu

O Hyperledger Besu implementa os algoritmos de consenso de prova de autoridade IBFT2, QBFT, e Clique.

O Algoritmo IBFT2 é uma atualização do Instanbul Byzantine Fault Tolerance (IBFT) que por sua vez é inspirado no Pratical Byzantine Fault Tolerance. Este algoritmo possui o princípio de finalidade determinística, quando um bloco é adicionado na cadeia, este nunca será removido e forks da cadeia serão evitados, diferente de algoritmos de prova de trabalho em que a possibilidade de remoção de um bloco depende da quantidade de blocos posteriormente adicionados, e a medida que blocos são adicionados posteriormente, menor a probabilidade de matematicamente de sucesso em remover um bloco. Comparativamente, o IBFT2 previne mais rapidamente a alteração de dados da blockchain.

O IBFT2 corrige o problema do IBFT, no qual um validator não honesto pode criar mais de um grupo de validadores para adicionar novo bloco, com esta estratégia este validador pode adicionar dois ou mais blocos na cadeia com valores de height diferentes, pois na primeira versão do IBFT o consenso precisa somente de 2/3 (dois terços) do total de validadores confirmando para adicionar um novo bloco na cadeia. Em um caso hipotético em que haja 5 validadores, caso um validador desonesto seja escolhido para adicionar o próximo bloco, este pode criar dois grupos de 3 validadores para adicionar um novo bloco e adicionar blocos simultâneos com height diferentes, como mostra na Figura 14. Para solucionar este problema, o IBFT2 realiza consenso com 3/4 (três quartos) dos validadores para evitar que sejam criados dois grupos de adição de blocos.

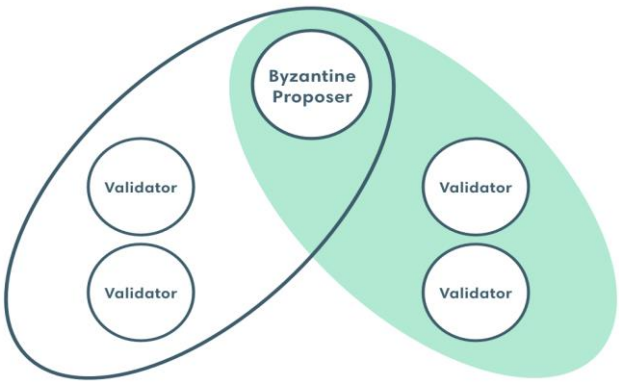


Figura 12- Mecanismo de validação protocolo IBFT. Fonte: Hyperledger Besu, 2023.

O algoritmo QBFT é uma proposta do Enterprise Ethereum Alliance (EEA) com intuito de apresentar uma alternativa de melhoria à primeira versão do IBFT. O QBFT utiliza os mesmos mecanismos do QBFT, porém com melhorias de velocidade e confiabilidade com poucos validadores, implementando o processo de validação com tolerância a falhas no qual é possível que até (n-1)/3 validadores possam ser maliciosos ou estejam com mal funcionamento. Mesmo neste cenário o algoritmo de consenso garante o princípio de finalidade determinística e previne forks da cadeia.

O Clique é um protocolo simples e indicado para blockchains permissionadas com foco em descentralização e redução da complexidade. Neste protocolo, validadores utilizam um sistema aberto de votação para adicionar um novo bloco na cadeia. Neste algoritmo de consenso vários blocos são propostos para serem adicionados na cadeia ao mesmo tempo. Em seguida os blocos candidatos passam por um processo de seleção em que o critério pode ser votação através do protocolo ghost ou pontuação do bloco, onde o bloco do líder da rodada possui maior pontuação. A seleção do bloco é necessária para resolver os forks na rede com múltiplos blocos candidatos. O algoritmo de consenso não apresenta validação, o bloco é adicionado na cadeia se for inserido por uma autoridade legítima. Entretanto, se um validador insere um bloco inválido, os outros validadores podem votar para suspender temporariamente o direito deste validador de adicionar blocos.

O algoritmo de consenso Clique não garante a prevenção de forks na cadeia, diferente dos anteriores no Clique é possível ter uma rede com apenas um validador, porém esta estratégia não garante redundância, e caso o validador esteja indisponível não haverá adição de blocos na cadeia. No aspecto de (vivacidade), Clique possui melhor tolerância a falhas que o IBFT e QBFT, pois basta que apenas um validador esteja disponível para que a rede continue produzindo blocos. No aspecto de segurança, o Clique apresenta uma vulnerabilidade, pois o algoritmo de consenso confia no pressuposto que haverá sempre a quantidade de nós honestos para manter a ledger segura.

5.1.2. Hyperledger Fabric

Hyperledger Fabric (HF) é um framework que possui a funcionalidade de algoritmo de consenso plugável, no qual é possível implementar ou utilizar algoritmos de consenso personalizados. Entretanto, é possível utilizar algoritmos de consenso padrão da ferramenta, atualmente na versão 2.5 por padrão é possível utilizar algoritmos Crash Fault Tolerance (CFT) ou Byzantine Fault Tolerance (BFT). O Fabric disponibiliza por padrão os algoritmos RAFT, Solo e Kafka. Porém os algoritmos Solo e kafka estão em desuso e estão sendo abandonados pela comunidade.

Algoritmos CFT são desenvolvidos para tolerar a falha ou indisponibilidade de nós, e continuidade dos serviços com ao menos um validador. Atualmente o HF suporta o algoritmo RAFT da classe CFT. Este algoritmo possui um mecanismo de líder e seguidor, no qual um líder é eleito por canal e suas decisões são replicadas para os seguidores. O líder também possui a responsabilidade de centralizar a troca de mensagens.

Em relação a algoritmos BFT, o HF disponibiliza por padrão algoritmo PBFT que funciona de maneira similar ao handshake do protocolo TCP. Inicialmente existe uma etapa de

preparação, em que um nó propõe (líder) a adição de novo bloco através de broadcasting para todos os outros validadores. Os outros validadores realizam a verificação do bloco proposto e retornam o aceite para a inclusão do bloco. Em seguida, após o líder receber uma quantidade suficiente de aceites do bloco, este envia para todos os validadores uma mensagem de commit do bloco. Cada bloco deve receber então uma quantidade suficiente de 2F+1[3] de commits.

Em aspecto geral os algoritmos de consenso utilizados no Hyperledger Fabric seguem o padrão de ordenar transações em um bloco, adicionar o bloco na cadeia e em seguida a confirmação de inserção do novo bloco.

5.1.3. Hyperledger Indy

Hyperledger Indy é um framework para blockchains focadas em identidade digital descentralizada que permite utilizar um algoritmo de consenso plugável. Semelhante ao Hyperledger Fabric, é possível utilizar consenso personalizado. Porém, é possível utilizar um algoritmo de consenso padrão disponibilizado pela ferramenta, RBFT. O (Robust Byzantine Fault Tolerance - RBFT) é uma variação da classe de algoritmos de consenso bizantinos tolerantes a falhas (BFT). No RBFT é necessário que o número de nós honestos seja 3 vezes mais um maior que o número de nós desonestos[4].

5.2. Quantidade de nós

Para definir a quantidade mínima de nós em cada rede é necessário observar as regras do mecanismo de consenso, pois cada mecanismo determina a quantidade de nós necessário para validação de bloco, adição e remoção de participantes[5]. Atender a quantidade mínima garante a continuidade de operação da blockchain, pois caso a quantidade de nós seja menor que o necessário, processos de votação ou validação de blocos podem entrar em loop aguardando atingir o consenso sem nunca conseguir alcançá-lo. Os cenários de loop são indesejáveis e devem ser evitados, pois, dependendo do caso a solução é desligar e ligar todos os nós, o que é inadequado e fere o princípio de disponibilidade dos dados em blockchain.

5.2.1. Hyperledger Fabric

Fabric permite implementar redes privadas com algoritmo de consenso RAFT, KAFKA e SOLO. Os algoritmos de consenso implementados no Fabric necessitam de apenas um nó orderer e um peer para gerar blocos e garantir o funcionamento da rede. Embora seja possível, este número não é adequado para uma rede blockchain e não garante tolerância a falhas. Para a rede do projeto Ilíada, é recomendado que os membros fundadores utilizem no mínimo 2 nós *orderers* e 2 nós *peers* cada. Os outros participantes como universidades, institutos de pesquisa e startups podem utilizar um

[3] 2F+1. Neste cálculo F é o número de nós maliciosos ou com mau funcionamento.

[4] O Algoritmo prevê que o número de nós honestos seja 3F+1 onde F é o número de nós desonestos.

[5] A votação para adição e remoção de participantes ocorre em redes blockchain permissionadas.

nó *peer*, e caso haja abertura nas regras de governança, podem implementar um nó *orderer.*

5.2.2. Hyperledger Besu

O Besu permite implementar redes permissionadas com algoritmos de consenso de prova de autoridade QBFT, IBFT e Clique. Estes algoritmos de consenso são baseados em algoritmos bizantinos de tolerância a falhas (Byzantine Fault Problem - BFT), garantindo o princípio de finalidade determinística. Em termos gerais, os algoritmos BFT necessitam de pelo menos 2/3 dos nós validando transação.

Para implementá-los em uma rede que garanta a disponibilidade dos dados, a resiliência e a tolerância a falhas, são necessários no mínimo três nós validadores. Entretanto, para garantir resiliência e tolerância a falhas são necessários mais nós. Desta forma, os membros fundadores da rede (RNP e CPQD) podem considerar um mínimo 2 boots e 2 validators em cada organização, pois mesmo que uma instituição apresente indisponibilidade em todos os seus nós o *ledger* será preservado até que estes voltem a funcionar normalmente. O restante dos membros da rede deve implementar nós *writers* para fazer execução de contratos inteligentes, porém pode ser adequado que algumas instituições participantes auxiliem no consenso e disponibilidade dos dados implementando-nos validadores melhorando aspectos de disponibilidade e tolerância a falhas da rede.

5.2.3. Hyperledger Indy

Existem dois conjuntos de nós na implementação do Hyperledger Indy, sendo eles o conjunto *Validators* e o conjunto *Observer*:

- O *Validator* é quem gerencia a escrita, são os nodos que de fato participam do protocolo de consenso;
- *Observer:* serve para gerenciar a leitura de dados da bockchain.

Para Hyperledger Indy é recomendado que RNP e CPQD implementem no mínimo 2 nós *validators* e dois nós *observers*. Instituições de ensino-pesquisa e startups podem instanciar nós *observers* e caso seja necessário, instanciar um nó *validator.*

5.3. Infraestrutura Lógica e Comunidades

Nesta seção serão apresentados os componentes lógicos que podem servir como base de infraestrutura de software para as redes blockchain do projeto Ilíada, assim como seus contextos e comunidades relacionadas. Serão relacionadas algumas das principais comunidades envolvidas com as ferramentas já citadas e com ferramentas e padrões que possam ser utilizados no projeto seguindo as recomendações definidas. Também serão relacionadas tecnologias adequadas para implementar, operar e manter as redes blockchain de forma eficaz, segura e eficiente. A seguir, são apresentados os critérios gerais não-mandatórios, porém recomendados para essas indicações:

- Arquitetura OpenSource
- Desenvolvimento ativo

- Comunidade ativa e reconhecida como referência
- Suporte a conteinerização
- Aplicações externas e funções conteinerizadas
- Orquestração de contêineres em múltiplos servidores
- Suporte a execução sobre plataforma de nuvem como Kubernetes
- Auto recuperação de nodes e aplicações no caso de falhas na infra
- Replicação e escalonamento automáticos
- Fatiamento da infraestrutura em espaços isolados (multi-tenancy)
- Possibilidade de uso por parte das aplicações: da rede, das funções externas, dos orquestradores adotados

5.3.1. Comunidades, iniciativas e projetos

A seguir, serão apresentadas comunidades ativas e reconhecidas como referências no desenvolvimento de ferramentas de arquitetura Open Source, com foco na infraestrutura de software necessária para a operação de redes blockchain e também em padrões blockchain, que se encontram em constante desenvolvimento e podem contribuir com o projeto Iíada.

5.3.2. Ethereum Foundation

A Ethereum Foundation é uma organização sem fins lucrativos dedicada ao desenvolvimento e à promoção da plataforma Ethereum. Fundada em 2014, a fundação é responsável pelo desenvolvimento dos protocolos fundamentais da Ethereum, como a camada de consenso e o Ethereum Virtual Machine (EVM). Além disso, eles oferecem suporte a toda comunidade Ethereum e seus utilizadores e desenvolvedores.

A fundação promove a interoperabilidade entre diferentes implementações de clientes Ethereum e define padrões e melhores práticas para o desenvolvimento de contratos inteligentes, DApps e linguagens relacionadas, como a Solidity. A Ethereum Foundation também desempenha um papel na governança do protocolo Ethereum, facilitando discussões entre os principais interessados e participando de processos de atualização do protocolo. Ela explora e desenvolve continuamente temas como escalabilidade, segurança e privacidade.

Acompanhar a Ethereum Foundation pode ser interessante para garantir conformidade com as melhores práticas e padrões estabelecidos, bem como para permanecer informado sobre os desenvolvimentos mais recentes no ecossistema Ethereum. Além disso, aproveitar os recursos e o suporte oferecidos pela comunidade pode ser vantajoso para facilitar a correta utilização das tecnologias e ferramentas relacionadas à plataforma Ethereum e outras plataformas relacionadas, como a Hyperledger Besu.

5.3.3. Linux Foundation (LF)

A Linux Foundation (LF) desempenha um papel fundamental no avanço da tecnologia blockchain, apoiando e hospedando vários projetos blockchain sob o guarda-chuva Hyperledger. A iniciativa inclui múltiplas estruturas e ferramentas de blockchain projetadas para apoiar setores que vão desde finanças até saúde, todos construídos

com base nos princípios colaborativos de código aberto que são fundamentais para a missão da Linux Foundation.

Lançado pela Linux Foundation, o Hyperledger é um projeto importante que ressalta o compromisso de promover soluções blockchain escaláveis e interoperáveis. Inclui várias estruturas, como Hyperledger Fabric, Besu e Sawtooth e etc., cada uma das quais atende a necessidades diferentes, mas unifica seu objetivo principal de aumentar a adoção e funcionalidade do blockchain em todos os setores.

O suporte da Linux Foundation faz mais do que apenas fornecer um local para esses projetos. Contribuímos ativamente para a construção de um ecossistema robusto de treinamento, programas de certificação e eventos que ajudam os profissionais a obter o conhecimento necessário para implementar soluções blockchain de maneira eficaz. Esta abordagem holística garante que os desenvolvimentos da tecnologia blockchain se alinhem com as necessidades da indústria e permaneçam na vanguarda da inovação tecnológica.

5.3.4. Cloud Native Computing Foundation (CNCF)

Conhecida como guardiã de tecnologias de nuvem escaláveis, como Kubernetes, a Cloud Native Computing Foundation (CNCF) desempenha um papel no espaço blockchain, principalmente por meio da integração e gerenciamento de tecnologias nativas de nuvem e sistemas blockchain. O CNCF permite que as arquiteturas blockchain sejam dimensionadas e se adaptem com mais eficiência em ambientes de nuvem, promovendo um ecossistema que aproveita contêineres, microsserviços e sistemas coordenados dinamicamente.

As aplicações Blockchain se beneficiam muito do foco da CNCF em melhorar a escalabilidade, confiabilidade e flexibilidade de seus serviços de contêiner. Por exemplo, os nós blockchain implantados em um cluster Kubernetes são mais robustos e fáceis de gerenciar, consistentes com a natureza descentralizada e robusta da tecnologia blockchain.

Embora o próprio CNCF não gerencie diretamente projetos de blockchain, suas ferramentas e estruturas ajudam a construir infraestrutura que pode executar aplicativos de blockchain de maneira mais eficaz, especialmente em ambientes corporativos que exigem alta disponibilidade e ampla escalabilidade. Esta integração demonstra como os princípios tradicionais nativos da nuvem podem ser aplicados para inovar e apoiar o ambiente de tecnologia blockchain em rápido crescimento.

5.3.5. Linux

Linux e blockchain são duas tecnologias poderosas que estão sendo cada vez mais integradas para criar sistemas poderosos e eficientes para uma variedade de aplicações, desde criptomoedas até soluções de negócios.

Linux é o sistema operacional preferido para blockchain e é amplamente reconhecido por sua estabilidade, segurança e desempenho, que são atributos essenciais para executar uma rede blockchain. Sua flexibilidade de customização permite adaptá-lo a

necessidades específicas, como otimizar o desempenho dos nós do blockchain. Isso torna o Linux o sistema operacional preferido para muitas aplicações blockchain.

Às aplicações blockchain se beneficiam dos recursos robustos do Linux, incluindo seus fortes mecanismos de segurança, que ajudam a proteger contra acesso não autorizado e outras ameaças cibernéticas. Os recursos avançados de rede do Linux também suportam a escalabilidade das redes blockchain, essencial para lidar com grandes volumes de transações típicas de muitos casos de uso de blockchain.

Muitas plataformas blockchain, especialmente aquelas projetadas para uso empresarial, como Hyperledger Fabric e Ethereum, são comumente implementadas em servidores Linux. Essas implantações geralmente aproveitam tecnologias de conteinerização, como o Docker, que é executado nativamente no Linux, para aumentar a eficiência e a escalabilidade da implantação.

Concluindo, a integração do Linux e do blockchain aproveita os pontos fortes de ambas as tecnologias – criando sistemas que não são apenas mais seguros e estáveis, mas também escaláveis e eficientes. Esta sinergia é crucial à medida que a tecnologia blockchain continua a evoluir e a expandir-se para novas indústrias e aplicações.

5.3.6. Docker

Docker é um ecossistema capaz de encapsular um aplicativo e seu ambiente em um pacote isolado, chamado container. Isso permite que o aplicativo seja executado de maneira consistente, independentemente do sistema host subjacente. Em outras palavras, Docker pode criar um ambiente virtualizado para o aplicativo, incluindo todas as dependências necessárias, como bibliotecas e configurações. Isso torna fácil implantar e escalar aplicações em diferentes ambientes, sem a necessidade de configurar novamente os servidores ou as máquinas virtuais, e também permite que diferentes versões das aplicações e suas dependências coexistam pacificamente em um mesmo sistema. A tecnologia Docker é especialmente útil para aplicativos que exigem uma configuração específica ou que precisam ser executados em um ambiente próprio isolado. O Docker permite que os desenvolvedores usem esses ambientes isolados para testar suas aplicações, antes de implantá-las em produção.

Dentro do ecossistema docker existem também algumas ferramentas úteis como o docker-compose, uma aplicação simples que permite a orquestração rápida de aplicações compostas por vários contêineres em um único ambiente. Ele fornece uma maneira fácil de gerenciar as dependências entre os contêineres, garantindo que todos estejam funcionando corretamente juntos. A estrutura da aplicação e seu ambiente, incluindo os serviços, redes e volumes necessários, ficam descritos em arquivos YAML ou JSON, que são posteriormente usados para instanciar estes ambientes de uma forma fácil se comparada à maneira tradicional, principalmente no caso de aplicações complexas que dependem de múltiplos serviços e dados.

Docker e blockchain são uma combinação poderosa que é particularmente benéfica para o desenvolvimento e para o ambiente operacional de arquiteturas blockchain. Abaixo segue o detalhamento das vantagens de uso desse ecossistema:

Consistência ambiental: os containers Docker encapsulam os aplicativos da arquitetura blockchain e seu ambiente, garantindo que ele seja executado da mesma maneira, independentemente do sistema host subjacente. Essa consistência é crítica para aplicações blockchain, e diferenças no ambiente podem causar sérios problemas no processamento de transações.

Configuração e escalabilidade simplificadas: o Docker simplifica o processo de configuração de nós e redes de blockchain, empacotando aplicativos em contêineres fáceis de implantar e escalar. Isto é particularmente útil para gerenciar infraestruturas de blockchain complexas e de grande escala, como aquelas que envolvem vários nós e serviços.

Desenvolvimento e testes: o Docker é ideal para criar ambientes isolados que imitam sistemas de produção, permitindo aos desenvolvedores testar aplicações blockchain sob condições controladas. Isso ajuda a detectar bugs e problemas no início do ciclo de desenvolvimento, reduzindo assim o risco antes da implantação.

Interoperabilidade: Ao usar o Docker, as redes blockchain podem ser facilmente integradas a outros sistemas e tecnologias. Esta interoperabilidade é crítica tanto em ambientes de desenvolvimento quanto de produção, onde a blockchain precisa interagir com bancos de dados, aplicações e sistemas existentes.

Essencialmente, o Docker não apenas simplifica a implantação e o gerenciamento de redes blockchain, mas também oferece suporte a um ciclo de vida de desenvolvimento robusto para aplicações blockchain, tornando-o uma ferramenta indispensável no ecossistema blockchain.

5.3.7. Kubernetes

Kubernetes, também conhecido como K8s, é uma plataforma de nuvem desenvolvida e mantida pela Linux Foundation, com o objetivo de ser uma solução avançada de orquestração de contêineres sobre *clusters* de servidores, transformando-os em uma infraestrutura de nuvem capaz de automatizar a implantação, o dimensionamento e o gerenciamento de aplicações conteinerizadas. Os servidores de um cluster Kubernetes podem ser físicos ou virtuais (*baremetal* ou *virtual machines*), e podem estar alocados em uma nuvem pública, privada ou híbrida. Kubernetes é uma plataforma adotada atualmente em larga escala em ambientes de produção, sendo inclusive oferecida como serviço na maioria das plataformas de nuvem pública.

A configuração das aplicações é feita através de arquivos YAMLs similares aos utilizados no docker-compose. Nesses arquivos são definidos parâmetros da aplicação como variáveis de ambiente, parâmetros de rede, volumes de armazenamento, etc. Vale ressaltar que o Kubernetes traz de forma nativa verificação do estado da aplicação através de probes (liveness e readiness). Além disso, Kubernetes possui uma forte ferramenta para escalabilidade, chamada escalonamento horizontal, que auxilia fortemente no desempenho das aplicações.

5.3.8. Helm

Helm é um gerenciador de pacotes para Kubernetes, um sistema popular de orquestração de contêineres usado para implantar e gerenciar aplicativos em contêineres. Helm Charts são pacotes de recursos pré-configurados do Kubernetes que podem ser usados para implantar aplicativos complexos, compostos por vários microsserviços, bancos de dados e outros recursos, de forma reprodutível e automatizada.

Helm Charts são arquivos YAML que descrevem o estado desejado dos recursos do Kubernetes, incluindo implantações, serviços, configmaps, segredos e muito mais. Esses recursos são organizados em uma estrutura de diretório que define as dependências e os relacionamentos entre eles. Os gráficos do Helm têm versões e podem ser facilmente instalados, atualizados e desinstalados usando a CLI do Helm.

5.3.9. KVM

KVM (Kernel-based Virtual Machine) é uma infraestrutura de virtualização de kernel Linux ideal para executar ambientes virtualizados nos quais você pode configurar e gerenciar nós de blockchain. A integração do KVM com a tecnologia blockchain oferece benefícios como maior isolamento, gerenciamento de recursos e escalabilidade, que são essenciais para manter a segurança e a eficiência das redes blockchain. Ao usar KVM, os ambientes blockchain se beneficiam de um espaço virtual robusto e isolado que permite que múltiplas instâncias de blockchain sejam executadas simultaneamente em um único host físico. Isto é especialmente útil para fins de desenvolvimento e teste, onde diferentes configurações de blockchain podem ser testadas sem interferência. Além disso, o KVM pode aumentar a segurança dos aplicativos blockchain, separando o tráfego de rede e os processos de computação de máquinas virtuais, minimizando o risco de contaminação cruzada e ataques externos. No geral, o KVM fornece uma plataforma poderosa, eficiente e segura para implantação e gerenciamento da tecnologia blockchain, aproveitando os benefícios inerentes da virtualização para melhorar o desempenho e a confiabilidade dos sistemas blockchain.

5.3.10. Vagrant

O Vagrant é uma aplicação de código aberto para construção e gerenciamento de ambientes de máquinas virtuais, e é particularmente útil no contexto do desenvolvimento de blockchain porque permite criar um ambiente de desenvolvimento virtualizado e consistente.

O Vagrant permite que os desenvolvedores configurem e desmontem rapidamente ambientes de trabalho reproduzíveis e portáteis, perfeitos para testar e desenvolver aplicativos blockchain em uma variedade de plataformas. A ferramenta simplifica o gerenciamento de máquinas virtuais por meio de uma interface de linha de comando simples e funciona com uma variedade de plataformas de virtualização, incluindo VirtualBox, VMware e Hyper-V.

Para desenvolvedores de blockchain, o Vagrant oferece uma maneira simplificada de configurar esses ambientes com precisão e garantir que todos os membros da equipe

trabalhem na mesma configuração do sistema, reduzindo inconsistências e problemas de compatibilidade. Essencialmente, o Vagrant fornece uma camada de infraestrutura crítica para projetos de blockchain que exigem um ambiente de testes rigoroso antes da implantação, tornando-o uma ferramenta valiosa para desenvolvedores que buscam melhorar a eficiência e a consistência de seus fluxos de trabalho.

5.3.11. Aplicações de suporte

Além dos componentes citados anteriormente, é interessante para o projeto a prospecção e utilização de aplicações de suporte para ambientes de experimentação em blockchain. Isto pode incluir aplicações de monitoramento centralizado, tanto de métricas de hardware dos servidores quanto de métricas das camadas lógicas e da própria blockchain, *dashboard* ou *block explorer* centralizado, gerenciamento de logs centralizado, gerenciamento de imagens de *container* centralizado, armazenamento centralizado, e eventualmente um portal centralizado para acesso dos experimentadores. O termo "centralizado" indica que estas ferramentas serão implantadas fora das redes blockchain, servindo como suporte ao ambiente de experimentação como um todo, e podendo acessar ou serem acessadas pelos nós das redes blockchain em operação.

5.4. Soluções de implantação e gerência de plataformas blockchain

A implantação de uma blockchain envolve várias etapas técnicas, desde o design inicial até a manutenção contínua da rede. Diversas ferramentas têm sido desenvolvidas para simplificar esse processo, tornando a tecnologia blockchain mais acessível a desenvolvedores e organizações. Essas ferramentas reduzem significativamente a complexidade associada ao desenvolvimento e implantação de redes blockchain, permitindo que as organizações se concentrem na criação de soluções inovadoras. Ao oferecerem recursos que vão desde a simplificação da codificação de contratos inteligentes até a gestão eficiente da infraestrutura de rede, elas desempenham um papel crucial em tornar a tecnologia blockchain mais prática e acessível para uma ampla variedade de casos de uso.

Neste contexto, essa seção apresenta um levantamento de soluções para implantação e operação de redes blockchain. A tabela a seguir apresenta esta listagem de soluções, as plataformas blockchain suportadas por cada solução (entendemos que quanto maior a quantidade de plataformas suportadas por uma solução maior é o valor desta poiś atenderia diferentes cenários), a infraestrutura computacional (docker ou um cluster kubernetes), o foco da solução (teste/aprendizado e Produção) e o estado de cada projeto.

Nome	Plataformas blockchain suportadas	Infraestrutura esperada	Foco de Uso	Estado do Projeto
Bevel	Hyperledger Fabric, Hyperledger Indy, Hyperledger, Besu Quorum and R3 Corda	kubernetes	Produção	Ativo
Fablo	Hyperledger Fabric	Containers	Implementações Limitadas/Produção	Ativo
Fabric-samples	Hyperledger Fabric	Containers	Desenvolvimento e aprendizado	Ativo
Fabric operator	Hyperledger Fabric	Kubernetes	Implantação, gerenciamento e operação de redes Hyperledger Fabric	Ativo
Fabric Ansible Collecion	Hyperledger Fabric	Containers Kubernetes	Produção	Ativo
Fabric-Test	Hyperledger Fabric	Containers Kubernetes	implantação, espécie de monitoramento da rede com o PTE e testes.	Ativo
Indy Node Container	Hyperledger Indy	Containers	Implantação, operações de redes, desligamento de rede exclusão de dados da rede	Ativo
MinIndy	Hyperledger Indy	Containers	Implantação, operações de redes, desligamento de rede exclusão de dados da rede	Inativo
VON Network	Hyperledger Indy	Containers	Implantação, operações de redes, desenvolvimento, testes, visualização de processos da rede, desligamento de rede, exclusão de dados da rede.	Ativo
Nephos	Hyperledger Fabric	Kubernetes	Implantação, desenvolvimento de testes, produção.	Inativo (arquivado)

Tabela 4 -Ferramentas de implantação e gerência de redes blockchain.

5.4.1. Hyperledger Bevel

O Hyperledger Bevel[6] é um acelerador que permite aos desenvolvedores configurar e implantar rapidamente redes DLT seguras e escaláveis, prontas para produção. Ele simplifica a integração de novas organizações à rede e permite que os desenvolvedores concentrem-se na construção de aplicativos blockchain, sem se preocupar com o ambiente ou escalabilidade da rede. Ele suporta plataformas como o Hyperledger Fabric, Hyperledger Indy, Besu Quorum e R3 Corda. O Bevel utiliza tanto o Docker quanto o Kubernetes para sua infraestrutura, oferecendo flexibilidade de implementação. Seus pontos fortes incluem uma documentação clara e fácil configuração do ambiente de desenvolvimento, além de recursos avançados de segurança, como controle de acesso granular e criptografia robusta. No entanto, seus requisitos significativos de recursos de hardware e software e seu status de projeto incubado podem representar desafios para algumas organizações. Em resumo, o Hyperledger Bevel é uma excelente escolha para ambientes de produção que valorizam a segurança e a escalabilidade, mas pode exigir investimentos substanciais em recursos de infraestrutura.

5.4.2. Fablo

O Fablo[7] é uma ferramenta que facilita a criação, implantação e gerenciamento de redes Hyperledger Fabric. Ele automatiza tarefas complexas, tornando-o ideal para iniciantes e especialistas em blockchain; Ela tem suporte a Hyperledger Fabric e utiliza Containers Docker. Sua indicação é para equipes de desenvolvimento, empresas que desejam integrar o blockchain em seus processos, estudantes e profissionais de TI que desejam aprender sobre Hyperledger Fabric. Dos pontos positivos do Fablo, destacam-se: facilidade de uso, automatização de tarefas complexas, flexibilidade para diferentes configurações de rede, recursos amigáveis para desenvolvimento e atualizações frequentes com novos recursos. Porém, ele possui suporte limitado a recursos avançados, isso faz com que algumas funcionalidades possam exigir uso de outras ferramentas. Conhecimento técnico básico em Hyperledger Fabric e conceitos de blockchain são recomendados. Suporte ao Kubernetes ainda está em desenvolvimento.

5.4.3. Fabric Ansible Collection

O FAC[8] (Fabric Ansible Collection) permite automatizar a construção de redes Hyperledger Fabric e permite construir, operar, governar e expandir redes blockchain corporativas; Ela tem suporte a Ethereum, Hyperledger Fabric, Corda R3, EOSIO e Tezios; e utiliza Docker e kubernetes para oferecer portabilidade e consistência na implantação desses componentes em diferentes ambientes de computação. É possível destacar a sua segurança e facilidade de instalação, mas sua documentação é limitada. Ele possui o foco de uso em produção e o estado do projeto se encontra ativo.

[6] https://github.com/hyperledger/bevel

[7] https://github.com/hyperledger-labs/fablo

[8] https://github.com/hyperledger-labs/fabric-ansible-collection

5.4.4. Indy Node Container

O Indy Node Container[9] é uma ferramenta para fornecer containers (conteinerização de nós) de fácil utilidade com mínima utilização de recursos para executar nós de rede Indy. Ela tem suporte ao Docker e utiliza imagens de sistema operacional Linux, como Ubuntu 18 e Debian 11. Sua indicação é para ambientes que buscam uma maneira conveniente e escalável de implantar nós da rede Hyperledger Indy em containers Docker. Podemos destacar como pontos fortes a facilidade de configuração e a documentação detalhada. No entanto, seus pontos fracos incluem a necessidade de conhecimento especializado na plataforma do Hyperledger Indy e em conteinerização com Docker.

5.4.5. VON Network

A VON Network[10] é uma ferramenta de desenvolvimento de redes Indy, parte da Rede de Organizações Verificáveis (Verifiable Organizations Network - VON). Ela tem suporte ao Orquestrador Docker e é indicada para ambientes de desenvolvimento e testes. Podemos destacar como pontos fortes a inicialização facilitada de rede Indy e o oferecimento do Ledger Browser (Exemplo: http://greenlight.bcovrin.vonx.io/), que fornece informações das transações e status dos nós da rede. No entanto, seus pontos fracos incluem não ser adequada para uso em produção, pois não possui recursos e proteções necessárias para uma rede de produção, além de exigir conhecimento especializado em infraestrutura de rede Indy.

5.4.6. Fabric-Test

O Fabric-Test[11] é um projeto relacionado ao Hyperledger Fabric que fornece um conjunto de recursos para testar e validar diferentes aspectos do Hyperledger Fabric. Ele é usado para testar a funcionalidade, desempenho e robustez do Hyperledger Fabric em vários cenários, como redes de vários nós e casos de uso específicos. O Fabric-Test é composto por duas ferramentas: Operator, utilizado para implementar redes Hyperledger Fabric, e o PTE (Performance Traffic Engine), utilizado para invocação e consulta do *chaincode* através da rede implementada. A infraestrutura da ferramenta requer Go Lang 1.18 ou superior, Node 16 ou superior, Java 8 ou superior, Docker, Docker Compose, Curl, Make e um cluster Kubernetes. Fabric-Test é adequado para implantação, verificação de características da rede com o PTE e desenvolvimento de testes. Seus pontos fortes incluem documentação detalhada e recurso de verificação de desempenho da rede. Por outro lado, seus pontos fracos são a presença de muitas tecnologias na composição da ferramenta, o que pode resultar em uma curva de aprendizado menor e o fato de que a ferramenta pode não ser recomendada para produção devido à sua ênfase em testes.

[9] https://github.com/hyperledger/indy-node-container

[10] https://vonx.io

[11] https://github.com/hyperledger/fabric-test

5.4.7. Hyperledger Fabric Operator

O Hyperledger Fabric Operator[12] é uma ferramenta de código aberto projetada para simplificar a implantação e operação de redes Hyperledger Fabric na nuvem. Com uma interface intuitiva e recursos avançados, capacita os usuários a executarem tarefas repetitivas e configurações detalhadas de forma eficiente. Além disso, o operador oferece funcionalidades abrangentes para implantação, escalonamento, monitoramento e atualização das redes Fabric. Atualmente, pode ser implementado utilizando Kubernetes ou Docker, sendo mais recomendado o uso do Kubernetes, já que para o contexto do Docker ainda se encontra em processo de desenvolvimento. A ideia central do Fabric Operator é abstrair camadas e configurações complexas, permitindo que o administrador da rede se concentre em questões mais relacionadas ao negócio (Hyperledger Labs). Por outro lado, a curva de aprendizado da ferramenta pode representar um desafio para sua utilização.

5.4.8. Hyperledger Fabric-samples

O Hyperledger Fabric-samples[13] tem como público alvo desenvolvedores que desejam começar a trabalhar com o Hyperledger Fabric de forma rápida e eficiente. Ela tem suporte para a plataforma blockchain Hyperledger Fabric e utiliza a infraestrutura Docker. Sua indicação é para ambientes de desenvolvimento e aprendizado em blockchain. Podemos destacar seus pontos fortes, como acessibilidade, praticidade, diversidade e progressão no aprendizado, porém, é importante mencionar suas limitações, como a dependência de ambientes pré-configurados e a necessidade de conhecimentos prévios em blockchain para aproveitar totalmente suas funcionalidades.

O levantamento realizado e condensado na tabela 4 apresenta 10 soluções das quais 2 estão inativas. Entre os projetos ativos e voltados para produção (que é o foco das redes que serão implantadas no Iliada) o Bevel é a solução que apresenta maior número de plataformas suportadas e pode atender a maioria dos cenários blockchain identificados na seção de levantamento de aplicações blockchain na academia.

[12] https://github.com/hyperledger-labs/fabric-operator

[13] https://github.com/hyperledger/fabric-samples

6. Projeto de Implantação do primeiro ambiente

6.1. Definições da primeira rede blockchain

Abaixo são apresentadas as definições iniciais para o projeto da primeira rede do ambiente distribuído Ilíada:

1. As redes blockchain implementadas devem atender às necessidades dos projetos desenvolvidos por CPQD, RNP e possíveis interessados em participar do projeto Ilíada, como *Startups* e instituições de ensino e pesquisa. No âmbito da RNP existem projetos em Hyperledger Fabric e Hyperledger Besu. No âmbito do CPQD existem projetos em Hyperledger Fabric, Hyperledger Besu e Hyperledger Indy. O Besu é utilizado na RBB, e o Indy é utilizado nos projetos de Identidade digital descentralizada com SouID. O Fabric também está sendo utilizado em projetos no CPQD e na RNP, e possui grande apelo na comunidade acadêmica com diversos artigos de blockchain publicados utilizando Hyperledger Fabric.
2. O objetivo da implantação da primeira rede de experimentação deve ser o atendimento a alguma das demandas de pesquisa em assunto do tema Blockchain já previstas dentro do projeto Ilíada. A rede deverá incluir nós tanto na RNP quanto no CPqD, e sua arquitetura e configuração devem atender aos requisitos informados pela equipe desenvolvedora da pesquisa em questão. Para atender a essa demanda deve-se escolher a plataforma blockchain (*framework blockchain)* mais adequada dentre as já discutidas anteriormente neste relatório, pois cada uma apresenta características específicas com propósito de atender demandas especializadas. Aplicações de identidade digital descentralizada podem ser instanciadas usando as plataformas Indy ou Besu, enquanto que aplicações que necessitam de recursos EVM como NFT podem ser instanciadas na Besu. Por fim, aplicações de consórcio ou que necessitam de canais privados de comunicação podem ser instanciadas com a plataforma Fabric.
3. A primeira rede blockchain implantada no ambiente pode seguir um modelo simplificado de arquitetura e configuração, sem onerar o objetivo inicial de atender à demanda de execução de smart contracts dos projetos de pesquisa de forma básica. O projeto também deve considerar a evolução da rede inicial para uma arquitetura mais complexa, ou a inclusão de um modelo mais complexo paralelamente à rede inicial, que possa ser evolutivo.
4. O projeto não precisa considerar funcionalidades de alta disponibilidade em todas as camadas da rede inicial, devendo incluir esse requisito como recomendado nas próximas redes e versões.

Dentre as plataformas blockchain consideradas para o ambiente distribuído, foi definida a plataforma Hyperledger Besu como a plataforma da primeira rede a ser implantada. A escolha do Besu é justificada pelos motivos apresentados abaixo:

1. A plataforma terá como objetivo atender à necessidade da Meta 5, de pesquisa e desenvolvimento em Identidade Digital Descentralizada (IDD), servindo como rede distribuída para esta Meta desde o início do ambiente.
2. Em relação à plataforma Indy: apesar da plataforma Indy ser focada no gerenciamento de identidades descentralizadas, a plataforma Besu também

atende às demandas referentes a identidades descentralizadas através da implementação de funções agregadas do Hyperledger AnonCreds e do Hyperledger Aries. Como mostrado anteriormente neste relatório, o CPqD já possui experiência com esse tipo de implementação. Por outro lado, o padrão Indy foi projetado para funcionar em conjunto com outro sistema ou blockchain que possa prover a aplicação usuária das identidades descentralizadas, Assim, a Indy não suporta a execução de smart contracts de forma nativa, sendo necessária a implantação de uma outra blockchain paralela para este fim. Diferentemente, o padrão Besu já consegue atender a todos os requisitos em uma só rede, sem a necessidade de ter plataformas distintas para contratos inteligentes e para identidades.

3. A plataforma Besu já demonstrou sua viabilidade em ambientes de aplicações reais, sendo também a plataforma blockchain adotada pela RBB (Rede Blockchain Brasil), e também pelo DREX (Real Digital), uma CDBC brasileira desenvolvida e controlada pelo Bacen (Banco Central).
4. Já existe um conhecimento da equipe envolvida na Meta 3 a respeito do funcionamento do Besu, visto que ambas RNP e CPqD atuam ativamente como partícipes da RBB, e é possível aproveitar esse conhecimento para as redes Besu do ambiente distribuído Ilíada.
5. Ainda não há uma definição clara de demandas provenientes das Metas 4 e 2.2, assim como demandas provenientes de outras instituições que venham a fazer parte das redes do ambiente. Todos poderão adicionar suas demandas posteriormente, a partir do momento em que os requisitos puderem ser dimensionados.
6. Em relação à plataforma Fabric, a plataforma Besu apresenta diferenças quanto às funcionalidades de privacidade. O padrão Hyperledger Fabric possui suporte nativo a criação de canais privados, enquanto que o Besu possui a possibilidade de execução de contratos e transações de forma privada por meio da integração de ferramentas adicionais como a Orion. Quanto ao padrão de smart contracts, Fabric utiliza linguagens como Go, Java ou Node.js para elaboração de chaincodes, enquanto que a Besu utiliza linguagens como Solidity e Vyper seguindo o mesmo padrão utilizado na blockchain pública da Ethereum. Como o primeiro ambiente não necessita de controles rigorosos quanto a privacidade e permissão, a Besu também se mostra a escolha mais adequada para a primeira rede, quando comparada ao Fabric.
7. Foi verificado que a maioria dos trabalhos de pesquisa em blockchain utilizam o padrão da rede Ethereum. Sendo a plataforma Besu compatível com a rede Ethereum, estima-se que essa plataforma consiga atender a grande parte da demanda dos projetos de pesquisa na área de blockchain, principalmente para os casos de uso de redes privadas e/ou permissionadas.
8. Finalmente, o padrão Besu possui compatibilidade com a grande maioria das ferramentas e DApps utilizadas na rede Ethereum, o tornando uma ótima opção para desenvolvedores que desejam construir aplicações descentralizadas, além de implementar mecanismos de consenso do tipo PoA (Proof of Authority), ideais para uso em redes privadas-permissionadas de produção.

Portanto, a primeira rede será voltada a atender demandas de pesquisa em Identidade Digital Descentralizada, tendo seu escopo limitado a este atendimento e não será

necessária a configuração de tokens ou contratos inteligentes que não estejam associados a esta demanda.

6.2. Plataforma e arquitetura

Para a primeira versão das redes os nós serão instanciados utilizando containers *docker*, podendo ser executados via scripts docker-compose. Essa escolha proporciona as vantagens do isolamento das aplicações de forma auto-contida e da reutilização de recursos, já informadas anteriormente, através de uma plataforma de containers prática e bem conhecida.

Sendo o ambiente em sua versão inicial, pode-se assumir uma quantidade reduzida de hosts físicos dedicados, de nós da rede blockchain, e de organizações participantes da rede. Neste caso os primeiros participantes seriam RNP e CPqD.

6.2.1. Rede Besu em docker

A Figura 15 apresenta a primeira versão de uma rede Besu com RNP e CPqD utilizando docker para implantação de aplicações, e a possibilidade de participação de uma ou mais Instituições de Ensino e Pesquisa na primeira versão da rede.

Os nós da rede podem ser executados em containers docker isolados, e poderão ser do tipo *boot*, *validator* ou *writer*. As funções de boot e validator são mandatórias e poderão ser agregadas em um mesmo nó. Assim, uma arquitetura simples poderia utilizar 2 nós boot-validator por instituição, cada uma podendo ter nós writer opcionais. Todos nós dentro de uma mesma organização deverão se comunicar através da rede interna da própria organização, enquanto que a comunicação externa entre nós de organizações distintas deverá ser feita apenas entre os nós *boot-validator*, que deverão se conectar a outros nós *boot-validator* presentes nos ambientes dos outros participantes da rede. Os nós serão instanciados em containers docker com a possibilidade de utilização da ferramenta docker-compose para instalação dos containers dentro de uma mesma organização.

Deve ser garantido também a segurança dos nós através da utilização de mecanismos com firewall e configurações internas de segurança dos nós, como permissionamento local e lista de *static nodes*.

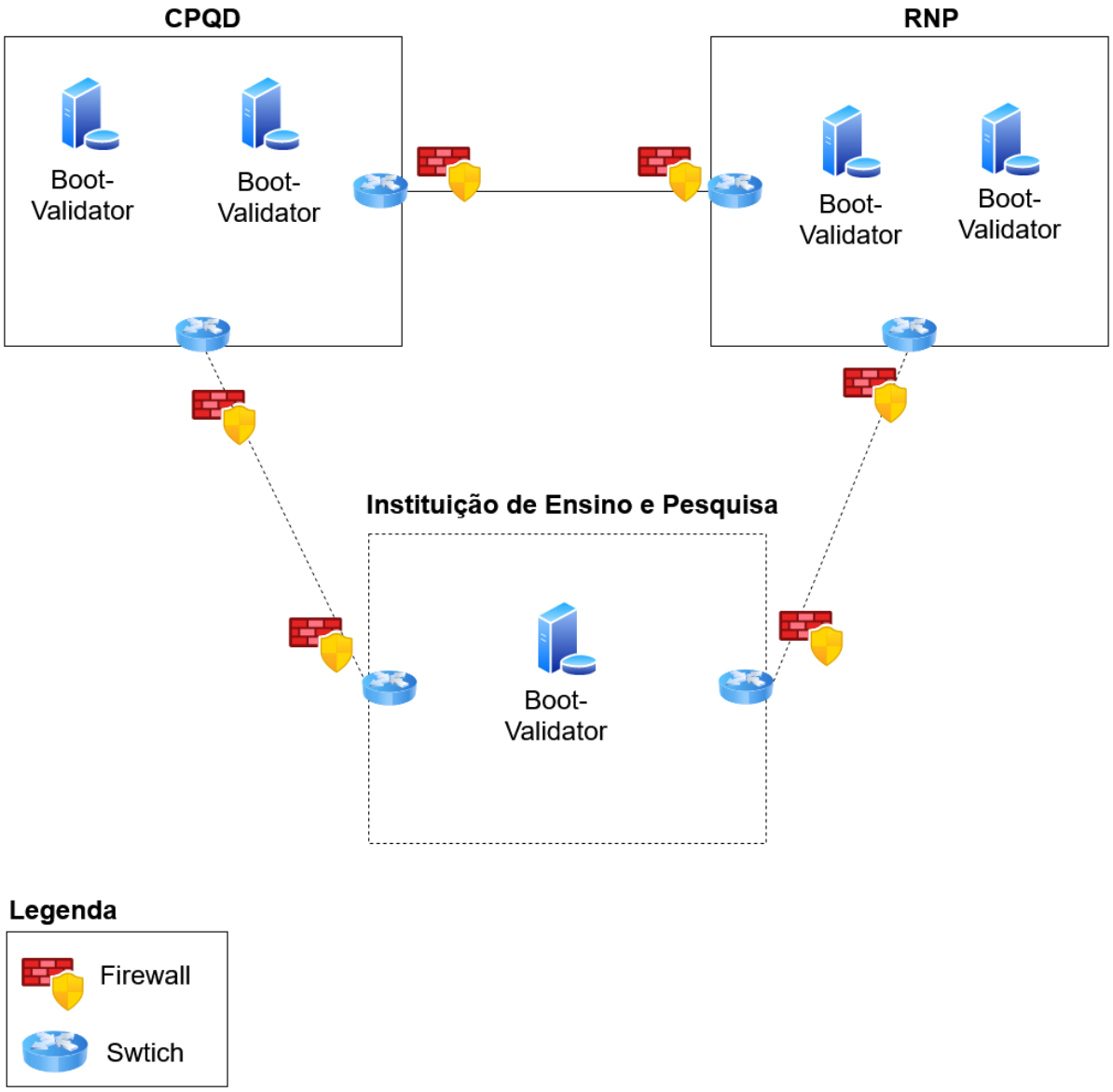


Figura 13 -Diagrama da Rede Hyperledger Besu para Ilíada.

6.2.2. Rede Fabric em docker

A Figura 16 apresenta a primeira versão de uma rede Fabric com nós instanciados na RNP e CPqD, utilizando docker para implantação de aplicações, e a possibilidade de uma instituição de Ensino e pesquisa instanciar nós na rede.

Cada participante da rede deverá ter uma autoridade certificadora para permitir a emissão local de certificados e chaves para os próprios nós, um nó do tipo *peer* com banco de dados *couchdb* para confirmar e armazenar transações, além de um nó do tipo *orderer* para ordenar as transações e os blocos. Cada instituição utiliza componentes de rede com switch para direcionamento do tráfego de rede entre os parceiros, bem como a utilização de firewall para proteger as conexões e os nós da rede de cada participante. Os nós serão instanciados em containers docker com a possibilidade de utilização da

ferramenta docker-compose para instalação dos containers dentro de uma mesma organização.

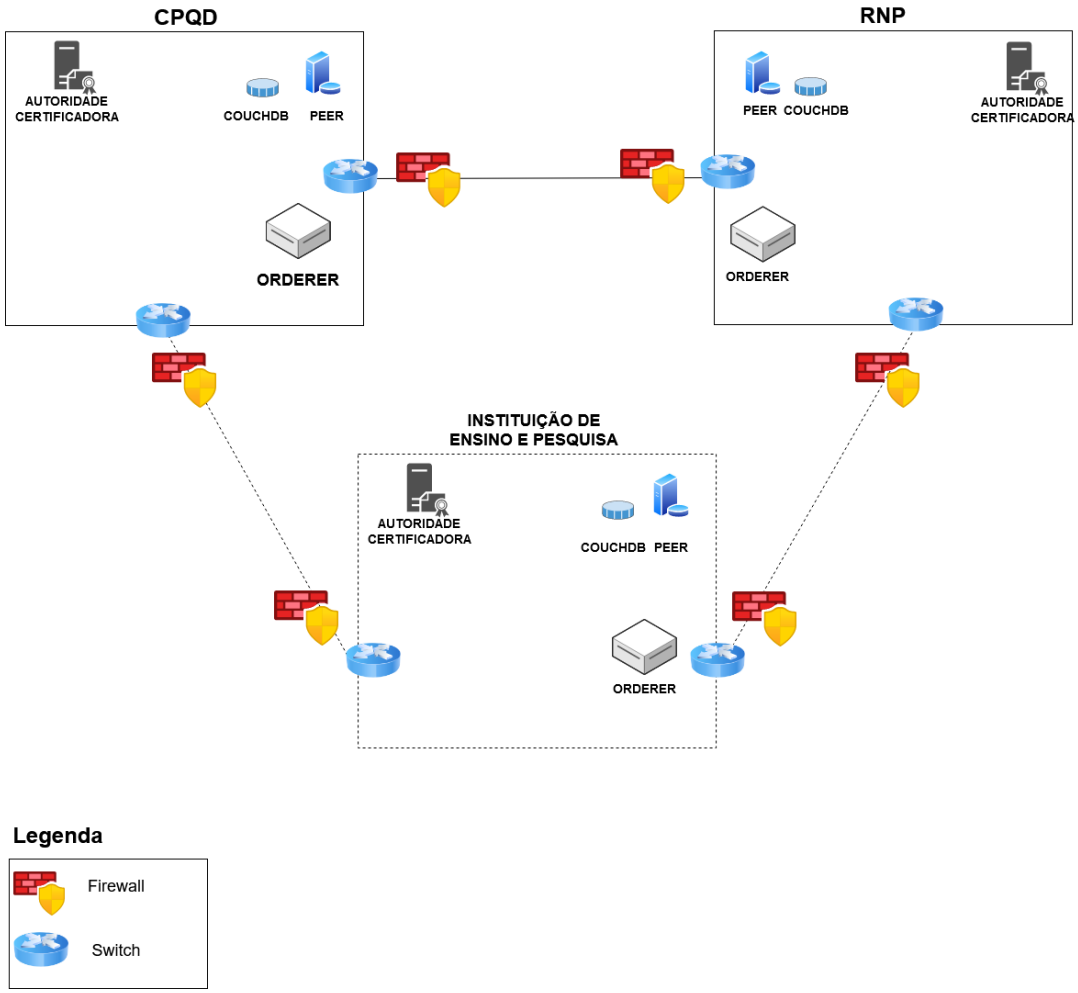


Figura 14 -Diagrama Rede Hyperledger Fabric para Ilíada.

6.2.3. Rede Besu inicial

A definição de quantidade de nós de uma blockchain depende de alguns fatores como escolha do algoritmo de consenso, tipo de rede (permissionada ou não-permissionada), governança e expectativa de adoção. Existem algoritmos de consenso que são restritivos em relação à quantidade mínima de nós necessários para a operação da rede, alguns algoritmos podem exigir apenas um nó para a operação da rede[14], enquanto outros podem exigir minimamente pares de nós para que a rede possa funcionar de maneira adequada. Entretanto, para garantir os benefícios da blockchain como redundância de armazenamento, disponibilidade de dados, tolerância a falhas é

[14] No aspecto técnico blockchain como uma rede de armazenamento descentralizado de dados não deve ter apenas um nó.

necessário que a quantidade de nós seja maior que o mínimo permitido, pois quanto maior a quantidade de nós melhor a *blockchain* responderá a falhas ou indisponibilidade de nós, garantindo a resiliência da rede.

Besu oferece suporte para uma variedade de protocolos de consenso, incluindo PoW, PoA e IBFT, tornando-o adaptável a diferentes configurações de rede. Esse recurso é particularmente valioso para organizações que operam em ambientes regulamentados ou que necessitam de redes autorizadas para garantir segurança e conformidade. Para a primeira rede, será definido o uso do protocolo de consenso QBFT, recomendação geral da Hyperledger para redes privadas.

Como cliente Ethereum, Besu tem capacidade de funcionar em redes públicas e privadas, garantindo compatibilidade com a rede principal Ethereum. Esta flexibilidade permite que as organizações explorem as possibilidades da infraestrutura pública, ao mesmo tempo que mantêm a opção de realizar determinadas operações em redes privadas. Essa flexibilidade é essencial para empresas que desejam utilizar a blockchain para diversas aplicações, mantendo a compatibilidade com o ecossistema Ethereum mais amplo.

Besu fornece um sistema de plugins que permite aos usuários personalizar o cliente de acordo com suas necessidades específicas, ao mesmo tempo que mantém intacto o código-fonte principal. Junto com esse recurso, Besu também oferece APIs JSON-RPC, WebSocket e GraphQL, que simplificam muito o processo de integração com sistemas e redes externas. Esta comunicação e troca de dados contínuos entre várias plataformas tornam-se facilmente alcançáveis.

A versatilidade da rede Besu é particularmente evidente na sua capacidade de se fundir perfeitamente com sistemas corporativos estabelecidos, concedendo às empresas a liberdade de decidir entre operar em redes privadas ou públicas, ou mesmo num híbrido de ambas.

Promover a integração perfeita com sistemas existentes e outras redes blockchain é de extrema importância em ambientes empresariais, especialmente para plataformas como Hyperledger Besu. A interoperabilidade é um recurso fundamental que o Hyperledger Besu oferece, reconhecendo sua importância.

Ao aderir aos padrões da Enterprise Ethereum Alliance (EEA), Besu incorpora efetivamente as especificações da EEA, que são projetadas para estabelecer interfaces universais entre projetos de código aberto e fechado no ecossistema Ethereum. Essa abordagem evita o problema de dependência do fornecedor e promove a interação perfeita entre várias implementações de blockchain que aderem a esses protocolos padronizados.

Um atributo notável do Hyperledger Besu são suas estruturas de permissão abrangentes, especificamente adaptadas para utilização em consórcio, tornando-o uma opção excepcional para organizações que buscam regular com eficácia controles de acesso complexos. Além disso, oferece recursos de monitoramento de nível empresarial por meio de ferramentas como o Prometheus, bem como APIs extensas projetadas para atender às necessidades dos desenvolvedores.

A primeira rede estará utilizando um ambiente distribuído inicial simples. Isso significa que poderá estar executando mais de 1 nó da rede blockchain em um mesmo servidor físico. Cada localidade deverá executar ao menos 2 nós *boot-validator*, chegando a um total de 4 nós. Inicialmente não serão usados nós *writer* ou *observer*. Todos os nós deverão ser executados em containers docker, sem a necessidade de estarem sobre Kubernetes.

Será confirmado com os integrantes da Meta 5 todos os requisitos para uma rede ideal de experimentação em Identidade Descentralizada. Em um segundo momento, após o primeiro padrão de implantação estar validado, esses requisitos e configurações necessárias serão implementadas na rede inicial.

Em um terceiro momento, podem ser agregados novos servidores a cada localidade, e poderá ser analisada a melhor forma de utilizar uma solução de orquestração de containers como o Kubernetes.

Posteriormente poderá ser implantada uma segunda rede blockchain em outro padrão Hyperledger, executando seus nós paralelamente aos nós da primeira rede, nos mesmos servidores físicos.

A Figura 15 abaixo apresenta a primeira versão da rede Besu definida como a plataforma inicial do ambiente distribuído.

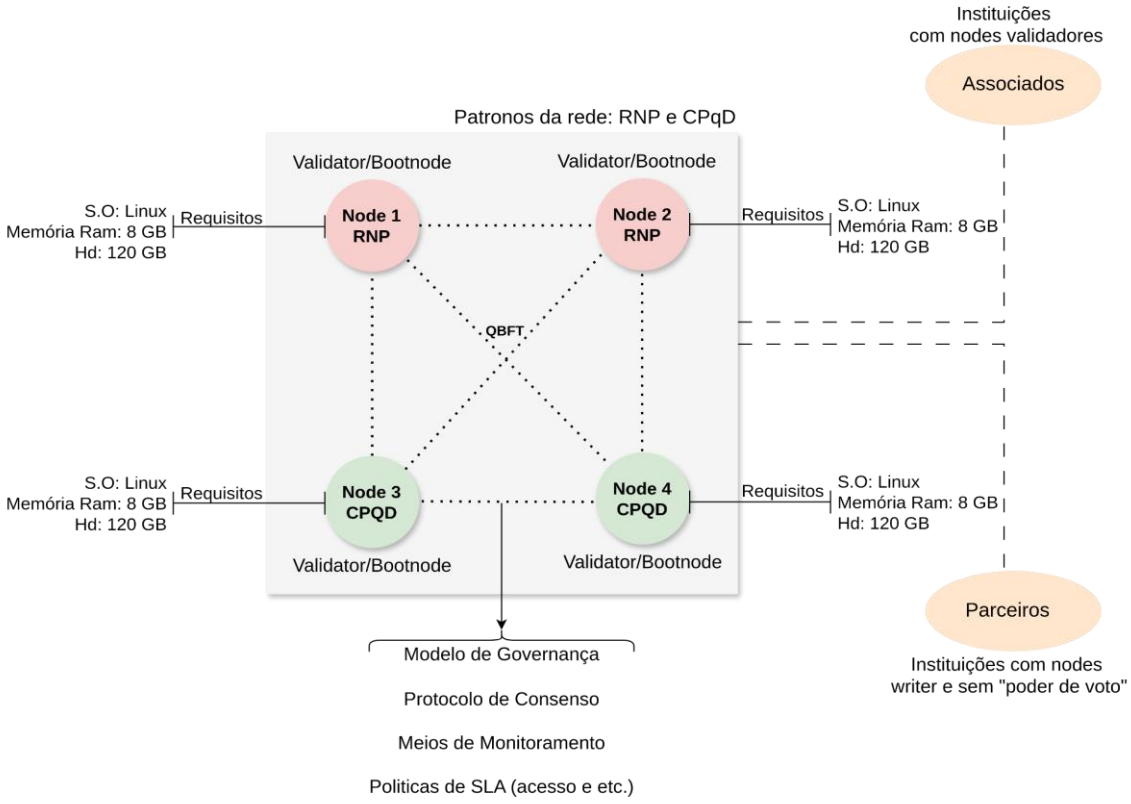


Figura 15 - Topologia inicial da primeira rede.

6.3. Requisitos de computação

Para realizar o deploy da rede é necessário atender requisitos mínimos de recursos computacionais para executar nós e garantir o consenso, principalmente em termos de Memória RAM, Armazenamento e Cores de CPU. A Memória RAM e os Cores CPU são utilizados de forma constante com picos intermitentes ao longo do ciclo de vida da rede blockchain, enquanto que o armazenamento é utilizado de forma incremental, sendo sua demanda estimada proporcionalmente ao período de tempo em que a rede estará funcionando. Foi considerada a experiência adquirida no projeto RBB para a definição da alocação de armazenamento, sendo definido o uso de 100 GBytes por nó ao longo de 1 ano de funcionamento. Esta definição foi estendida também aos padrões Fabric e Indy, por questões de facilidade, podendo ser revistos após o monitoramento das redes Ilíada ao longo de seu ciclo de vida e em uso por seus projetos.

Para redes privadas Hyperledger Fabric é recomendada a alocação mínima de 4 Gigabytes de memória RAM, 100 Gigabytes de armazenamento SSD e 2 cores de CPU, para cada nó.

Para redes privadas Hyperledger Besu é recomendada a alocação mínima de 8 Gigabytes de memória RAM, 100 Gigabytes de armazenamento SSD e 2 cores de CPU, para cada nó.

Para redes privadas Hyperledger Indy é recomendada a alocação mínima de 4 Gigabytes de memória RAM, 100 Gigabytes de armazenamento SSD e 4 cores de CPU, para cada nó.

Para a primeira rede, poderá ser utilizado um mesmo servidor físico para a instanciação de todos os nós de uma mesma instituição. Cada organização prevê a instanciação de 2 nós assumindo o papel de boot-validator cada um, em uma rede Besu. Os requisitos mínimos para um servidor único em cada organização participante para atender a essa demanda são apresentados abaixo:

- Memória RAM: 16 GB
- Armazenamento SSD: 200 GB
- CPU: 8 Cores ou vCPUs

Considerando que o ambiente poderá evoluir incluindo novas redes blockchain em paralelo assim como novas plataformas de blockchain, é recomendado que sejam alocados servidores com capacidade de hardware superior aos requisitos mínimos indicados acima, principalmente em termos de Memória RAM e Armazenamento, de forma que o ambiente possa ser estendido posteriormente com a evolução de todo o ambiente.

Para uma rede com 1 nó de cada uma das 3 plataformas blockchain Besu, Fabric e Indy, em cada servidor físico alocado, os requisitos mínimos para cada servidor único em cada organização participante são apresentados abaixo:

- Memória RAM: 16 GB
- Armazenamento SSD: 300 GB
- CPU: 8 Cores ou vCPUs

6.4. Rede

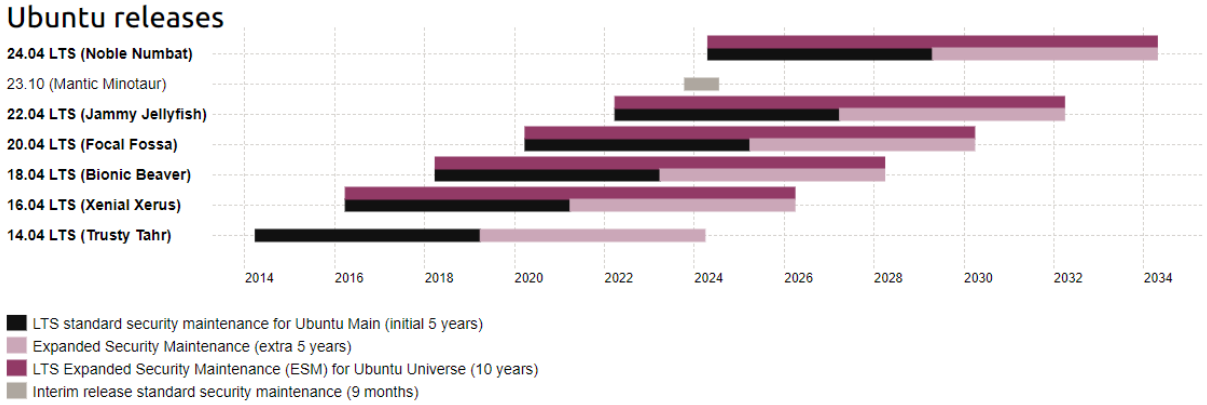
Para a conexão entre as diferentes instituições, inicialmente será utilizada conexão via Internet e IPs públicos. Futuramente, a conexão entre RNP e CPqD poderá utilizar link dedicado caso este cenário se mostre vantajoso do ponto de vista da demanda dos pesquisadores usuários. Cada conexão deve suportar uma velocidade mínima de 1 GBps, seja entre nós de uma mesma instituição, ou seja, entre diferentes instituições.

Cada instituição participante deve-se utilizar um Firewall de perímetro que proteja os próprios servidores, devendo-se liberar apenas as comunicações externas necessárias com outras instituições. Adicionalmente, também deve-se utilizar Firewall de host em cada servidor, de forma que estes tenham sua proteção individual, devendo-se liberar entre os nodes apenas as comunicações necessárias da rede blockchain e aplicações de suporte.

Deverá ser implementada uma conexão em arquitetura *full-mesh* (todos-para-todos) entre todos os *validators* da rede. Para futuras topologias, nós que não sejam *validators* podem se conectar ao nó *boot* de sua própria instituição, de forma local, não necessitando de conexões externas com outros nós de outras instituições.

6.5. Pilha de software

Como sistema operacional para a pilha de software foi definido o uso da distribuição Ubuntu, por se tratar de uma distribuição Linux bem conhecida e amplamente utilizada no meio acadêmico e científico, bem como por possuir alta estabilidade, suporte de 5 anos e uma boa frequência de atualizações, sendo bi-anual para novas versões LTS da distribuição e semestral para novas versões do kernel Linux. A versão a ser instalada nos servidores iniciais da ambiente Ilíada será a Ubuntu 22.04 LTS (Jammy Jellyfish), que teve seu lançamento em abril de 2022 e possui suporte padrão até abril de 2027, de acordo com as versões apresentadas na imagem oficial abaixo. Esta versão se mostra ideal para o projeto, por se tratar de uma versão não tão antiga, sem suporte oficial e sem riscos de não atender a dependências das aplicações atuais, e também não tão nova, se tratando de uma versão com bugs já descobertos e corrigidos, e sem o risco de ainda estar sem suporte a aplicações atuais. A escolha adequada da versão também é fundamental do ponto de vista de segurança, pois sistemas muito antigos podem ter vulnerabilidades que já não são mais corrigidas pela equipe oficial desenvolvedora do sistema, assim como versões muito novas podem conter vulnerabilidades que ainda não foram descobertas.



	RELEASED	END OF STANDARD SUPPORT	END OF UBUNTU PRO SUPPORT
24.04 LTS (Noble Numbat)	Apr 2024	Apr 2029	Apr 2034
23.10 (Mantic Minotaur)	Oct 2023	Jul 2024	
22.04 LTS (Jammy Jellyfish)	Apr 2022	Apr 2027	Apr 2032
20.04 LTS (Focal Fossa)	Apr 2020	Apr 2025	Apr 2030

Figura 16 -Ciclo de vida e suporte de sistemas Ubuntu atuais.

Os nós e as aplicações relacionadas à rede blockchain deverão ser instanciadas utilizando containers docker, com a possibilidade de se utilizar kubernetes posteriormente em futuras versões da rede para orquestração do ciclo de vida dos containers.

6.6. Aplicações de suporte a experimentação

Para a primeira versão do ambiente, também é recomendada a instalação de algumas aplicações de suporte a experimentação, que envolvam o monitoramento das redes blockchain e seus hosts, assim como ferramentas de acesso e interação com a primeira rede blockchain. Abaixo são apresentadas algumas ferramentas que poderão ser utilizadas para este fim:

- **netdata** - Ferramenta para monitoramento do total de recursos e nível de utilização em cada servidor, com baixo impacto e métricas a cada segundo ("tempo-real").
- **Prometheus + Grafana** - Conjunto de ferramentas para o monitoramento dos nodes e de métricas das redes blockchain. A plataforma Besu tem métricas nativas para servir a um monitoramento Prometheus.
- **Loki + Grafana** - Conjunto de ferramentas para a agregação centralizada de logs, com filtros de busca e interface amigável.
- **Sirato Block Explorer** - Ferramenta exploradora de blocos compatível com a plataforma Besu, provendo a visão geral de toda a rede, incluindo informações e metadados dos blocos, tokens, contratos inteligentes, transações, e nós, assim como interação básica com contratos inteligentes.

As aplicações a serem implantadas devem seguir a recomendação do uso de containers docker, podendo ser instanciadas em um servidor separado para este fim. Cada instituição poderá implantar ferramentas de forma separada caso seja de seu interesse, para obtenção de informações úteis aos projetos de pesquisa usuários da rede distribuída.

6.7. Processo de implantação

O processo de implantação da primeira rede e dos demais componentes do ambiente será desenvolvido ao longo das atividades da meta 3.2, sendo descritos no relatório dessa submeta, incluindo informações como o cronograma de atividades, a documentação técnica, e os critérios de aceitação e validação do ambiente como um todo, assim como todos os recursos que serão efetivamente alocados ou adquiridos para a composição do ambiente distribuído. A governança das redes de experimentação também será definida ao longo das atividades da meta 3.2, em que RNP e CPqD definirão os tipos de participantes a serem aceitos neste ambiente e os papéis e deveres de cada um.

7. Conclusão

Este relatório apresentou algumas das iniciativas em andamento envolvendo o tema Blockchain, tanto por parte da RNP quanto da parte do CPqD, como a RBB e o projeto de pesquisa de Identidade Descentralizada (IDD), que utilizam a plataforma Hyperledger Besu. também foi apresentado um levantamento inicial de trabalhos acadêmicos de pesquisa em temas de blockchain, ressaltando o uso de redes e plataformas como Ethereum, Fabric e Indy. Em seguida, foi apresentada uma visão geral de plataformas específicas de rede blockchain, ferramentas de implantação de blockchains, comunidades relevantes para acompanhamento, e aplicações de infraestrutura lógica de suporte, que poderiam ser considerados na implantação do ambiente de experimentação da rede distribuída do projeto Ilíada. Por fim, foi definida a plataforma e arquitetura geral da primeira rede do ambiente e as motivações para essa escolha, tendo como base o atendimento das demandas de pesquisa de IDD, assim como o dimensionamento inicial dos primeiros servidores e da infraestrutura necessária para a implantação do ambiente.

8. Referências

Allen, Cristopher (2016). "**The Path to Self-Sovereign Path to Self-Sovereign IdentityThe IdentityThe Path to Self-Sovereign Identity**". Disponível em: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html>. Acesso em: 08/05/2024.

FALAZI, Graheeb. **Process-Based Composition of Permissioned and Permissionless Blockchain Smart Contracts**. Paris, França. 2019. Disponível em: https://ieeexplore.ieee.org/document/8945020. Acessado 22 de Fevereiro de 2023.

GONCALVES, G. D. ; COUTINHO, E. ; FREITAS, A. E. S. . **Um Panorama da Pesquisa em Blockchain no Brasil.** SBC Horizontes, 26 maio 2022. Acessado 01 de Maio de 2024.

Hyperleger Besu. Hyperledger Besu for private networks. Disponível em: <https://besu.hyperledger.org/private-networks>. Acesso em: 19 fev. 2024.

Hyperledger Indy. Type: Distributed ledger software. Disponível em: <https://www.hyperledger.org/projects/hyperledger-indy>. Acesso em: 10 fev. 2024

Hyperledger Cacti. Type: Tool. Disponível em: <https://www.hyperledger.org/projects/cacti>. Acesso em: 10 fev. 2024

Hyperledger Bevel.automation framework for rapidly. Disponível em: <https://www.hyperledger.org/projects/bevel>. Acesso em: 16 jan. 2024

Hyperledger Fabric. A Blockchain Platform for the Enterprise. Disponível em: <https://hyperledger-fabric.readthedocs.io/en/release-2.5/>. Acesso em: 19 fev. 2024

Rede Blockchain Brasil. Disponível em: https://github.com/RBBNet/rbb. Acesso em: 29 fev. 2024.

SALTINI, R.; HYLAND-WOOD, D. **IBFT 2.0: A Safe and Live Variation of the IBFT Blockchain Consensus Protocol for Eventually Synchronous Networks**. [s.l: s.n.] Disponível em: <https://arxiv.org/pdf/1909.10194.pdf >. Acesso em: 09 abr. 2024.

ENTETHALLIANCE. **QBFT Blockchain Consensus Protocol Specification v1**. [*S. l.*], 17 jan. 2023. Disponível em: https://entethalliance.org/specs/qbft/. Acesso em: 10 abr. 2024.

CHAALS. **EEA Publishes QBFT Blockchain Consensus Protocol**. Disponível em: <https://entethalliance.org/23-01-qbft-spec-version-1-released/>. Acesso em: 9 abr. 2024.

ISLAM, M.; MWAMBA MERLE, M.; PETER IN, H. **A Comparative Analysis of Proof-of-Authority Consensus Algorithms: Aura vs Clique.** In: 2022 IEEE International Conference on Services Computing (SCC), Barcelona, Spain. Disponível em: <https://ieeexplore.ieee.org/document/9860157>. Acesso em: 9 abr. 2024.

BAINS, A. **A Comparative Analysis of Proof-of_authority Consensus Algorithm: Aura vs Clique,** 2023. Disponível em: < https://www.ccn.com/education/a-comparative-analysis-of-proof-of-authority-consensus-algorithms-aura-vs-clique/ > Acesso em: 09 abr. 2024.

The Ordering Service — hyperledger-fabricdocs master documentation. Disponível em: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/orderer/ordering_service.html>. Acesso em: 09 abr. 2024.

TRIPATHI, Shivani. Hyperledger Fabric Consensus Mechanisms: Exploring the Options. *In*: **Hyperledger Fabric Consensus Mechanisms**: Exploring the Options. [*S. l.*], 14 jul. 2023. Disponível em: https://www.spydra.app/blog/hyperledger-fabric-consensus-mechanisms-exploring-the-options. Acesso em: 10 abr. 2024.

GEEKSFORCE. Consensus in hyperledger fabric. *In*: **Consensus in Hyperledger Fabric**. [*S. l.*], 18 out. 2023. Disponível em: https://www.geeksforgeeks.org/consensus-in-hyperledger-fabric/. Acesso em: 10 abr. 2024.

SHARMA, Nirshal. Comparing Byzantine Fault Tolerance Consensus Algorithms. *In*: **Comparing Byzantine Fault Tolerance Consensus Algorithms**. [*S. l.*], 30 maio 2023. Disponível em: https://blog.web3labs.com/web3development/comparing-byzantine-fault-tolerance-consensus-algorithms. Acesso em: 10 abr. 2024.

ANCEAUME, E. et al. **On finality in blockchains**. OPODIS 2021 - 25th Conference on Principles of Distributed Systems, Dec 2021, Strasbourg, France. cea-03080029v5. Disponível em: <https://cea.hal.science/cea-03080029/document>. Acessado em: 23 abr. 2024.

Nakamura, E., Marino, F.C., Formigoni Filho, J.R., Ribeiro, S.L. e Oliveira, V.P. **Identidade Digital Descentralizada: Conceitos, aplicações, iniciativas, plataforma de desenvolvimento e implementação de caso de uso**. Minicurso do SBSeg 2019. Disponível em: <https://sbseg2019.ime.usp.br/minicursos.pdf>. Acesso em: 08/05/2024.

PENNEC, Guénolé Le. Choosing a Distributed Ledger Technology: **Looking at the Popularity and Activity of Major Players Report.** Available in: https://www.blockchainresearchlab.org/wp-content/uploads/2020/05/BRL-Report-No-5-DLT-Popularity.pdf, 2020.

Sovrin Foundation (2018**). "A Protocol and Token for SelfSovereign Identity and Decentralized Trust**". Disponível em: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf. Acesso em: 08/05/2024.

W3C (2021). "**Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations".** Disponível em: <https://www.w3.org/TR/did-core/#introduction>. Acesso em: 10/04/2022.

W3C (2022). "**Verifiable Credentials Data Model v1.1".** Disponível em: <https://www.w3.org/TR/vc-data-model/>. Acesso em: 10/04/2022.