

Uma infraestrutura de experimentação para pesquisa e desenvolvimento em Blockchains e Web3

Luiz Eduardo Folly de Campos
luiz.campos@rnp.br
Rede Nacional de Ensino e Pesquisa (RNP)

Reinaldo César de Moraes Gomes
reinaldo.gomes@rnp.br
Rede Nacional de Ensino e Pesquisa (RNP)

ABSTRACT

Trust on the internet is an essential pillar for online interactions, and blockchain technologies offer a new paradigm of trust based on data integrity and decentralization, enabling innovative solutions such as the Web3 applications. This paper presents the experimental infrastructure for blockchain research and development currently being built within the ILIADA project at RNP, and its use for the development of new Web3 applications.

KEYWORDS

web3, blockchain, decentralization, dapps, self-sovereign digital identity, ssi, did

1 INTRODUÇÃO

Blockchain é atualmente uma tecnologia fundamental no contexto das aplicações Web3, oferecendo formas mais sofisticadas de garantir auditabilidade, rastreabilidade e integridade dos dados através do estabelecimento de confiança entre os pares, sem a necessidade de intermediários ou autoridades centrais certificadoras. Entretanto, o desenvolvimento de sistemas blockchain e web3 envolve a integração de diversas técnicas para prover escalabilidade, segurança, descentralização, auditabilidade e tolerância a falhas, assim como a aplicação de modelos de governança, negócios e gestão.

Diversas iniciativas internacionais têm explorado o potencial da tecnologia blockchain, com foco em segurança e auditabilidade. Uma delas é a EBSI [1], fruto da colaboração entre a Comissão Europeia e 29 países, que visa melhorar serviços e negócios por meio da tecnologia blockchain. Outro exemplo é a LACChain [4], liderada pelo Laboratório de Inovação do BID, oferecendo uma infraestrutura blockchain público-permissionada para apoiar governos, empresas e organizações no desenvolvimento de soluções descentralizadas. No Brasil, a RBB [6] reúne diversas instituições para construir uma infraestrutura tecnológica e de governança voltada à adoção da blockchain em aplicações de interesse público.

Se unindo a esses esforços temos o projeto ILIADA (Integrando Livros-razão/ledgers, Infraestrutura e Aplicações Descentralizadas), que é financiado pelo MCTI e coordenado pela Softex, tendo como executoras a RNP e o CPqD. As atividades planejadas visam estimular a pesquisa e desenvolvimento de artefatos tecnológicos, aplicações e plataformas computacionais baseadas em blockchain, para contribuir no amadurecimento dessa tecnologia no Brasil. Para tanto, uma das principais ações é a construção de uma estrutura de experimentação (chamada de *testbed*) para P&D em blockchain,

ofertando ambientes a pesquisadores que desejem usar tecnologias blockchain em suas pesquisas.

Ao simular condições próximas a ambientes reais de produção e possibilitando a integração com sistemas e serviços externos (i.e: outras blockchains, blockchains públicas, oráculos, sistemas de tokenização e armazenamento descentralizado), o testbed ILIADA possibilita a comparação de diferentes arquiteturas, a identificação das tecnologias mais adequadas para casos de uso distintos, bem como a validação de aspectos críticos de desempenho, segurança, escalabilidade e interoperabilidade das soluções em desenvolvimento.

2 O TESTBED ILIADA

2.1 Ambientes para Experimentação

Sendo uma infraestrutura dedicada para experimentação, o testbed ILIADA oferece ambientes controlados e flexíveis que possibilitam validar ideias inovadoras relacionadas a blockchains e soluções Web3 antes de sua adoção em escala, reduzindo riscos tecnológicos e acelerando os ciclos de desenvolvimento de forma segura através do suporte ao desenvolvimento de Provas de Conceito (PoCs) e de Produtos Mínimos Viáveis (MVPs) em um ambiente relevante.

A implementação de PoCs permite a validação de hipóteses e viabilidade técnica e funcional de soluções Web3, como aplicações descentralizadas (dApps), modelos de governança distribuída ou protocolos e soluções de identidade digital descentralizada (IDD). MVPs são fundamentais para transformar os conceitos validados em soluções funcionais que possam ser apresentadas a comunidades acadêmicas, ecossistemas de inovação ou potenciais investidores.

O projeto ILIADA também oferece suporte na instalação e uso das plataformas blockchain permissionadas Hyperledger Besu [2] e Fabric [3] dentro dos ambientes de experimentação. Essas plataformas são reconhecidas como padrões de plataformas blockchain de código aberto e mantidas pela Linux Foundation Decentralized Trust (LFDT) [5], entidade voltada a desenvolver e fomentar o uso de blockchains de código aberto para soluções corporativas.

Redes blockchain permissionadas se destacam por oferecer ambientes controlados, com regras de governança e participação definidas de forma colaborativa entre participantes previamente autorizados. Elas permitem a implementação de mecanismos de confidencialidade, como transações privadas, canais restritos e controle de acesso, e geralmente oferecem desempenho superior devido ao uso de mecanismos de consenso mais eficientes que dispensam a competição intensiva por recursos ou o uso de criptomoedas para participação. Essas redes são particularmente adequadas a consórcios multi-institucionais, comunidades produtivas e ecossistemas acadêmicos e corporativos, nos quais há a necessidade de confiança mútua entre organizações, segurança e conformidade regulatória.

Redes públicas como a Ethereum e similares são suscetíveis a impactos de uso público, apresentando maior variabilidade de latência

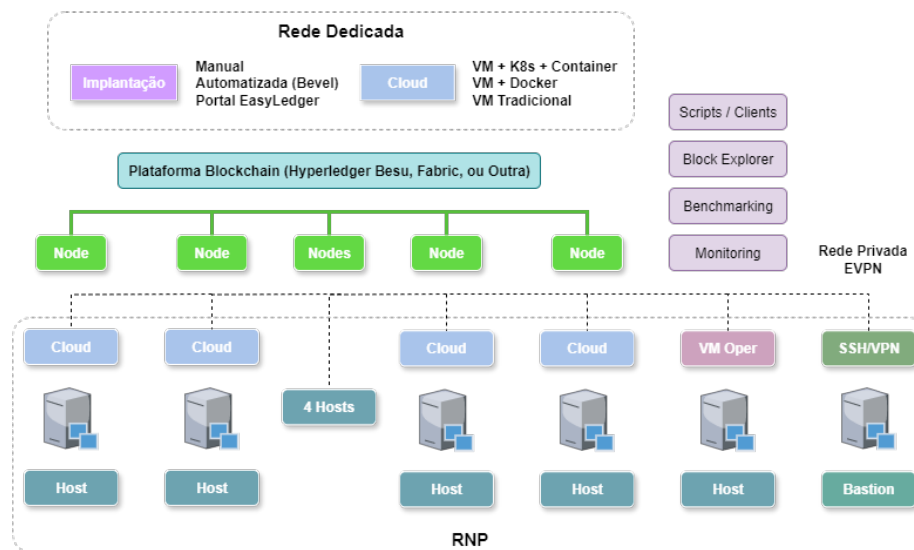


Figura 1: Arquitetura do ambiente para redes dedicadas

e custos de transação (ex.: *gas fees*), e uma menor previsibilidade de comportamento e desempenho, o que pode limitar sua adequação a cenários corporativos, regulados, ou de pequenas comunidades. Adicionalmente, um ambiente permissionado e dedicado reduz riscos associados a ataques externos comuns em *blockchains* públicas, como ataques Sybil e exploração de vulnerabilidades em consenso aberto, proporcionando maior segurança e confiabilidade.

O Testbed prevê dois tipos de ambientes para experimentação em *blockchain*: o das Redes Dedicadas e o das Redes Descentralizadas. O roadmap do testbed prevê a criação e uso de módulos para testes de desempenho e para monitoramento e coleta de métricas como, por exemplo, latência e tempo de execução de transações, TPS (transações/s), consumo de recursos (CPU, RAM e Disco), tamanho de blocos, blocos por nó, transações executadas por nó, etc.

2.2 Ambientes para Redes Dedicadas

Os ambientes de experimentação com redes blockchain dedicadas (Figura 1) oferecem uma infraestrutura de uso exclusivo para a implantação de redes blockchain personalizadas e flexíveis que permanecem sob controle e governança do usuário. Esse tipo de ambiente é implantado em infraestrutura fornecida pela RNP e planejado para pesquisadores que necessitam de autonomia na configuração, gestão e operação de todo o ciclo da infraestrutura de blockchain, e mantém-se isolado de outros ambientes, prevenindo interferências no desenvolvimento da pesquisa.

Esse ambiente é constituído por elementos voltados à comunicação interna e ao acesso dos usuários, como o **Bastion**, servidor de VPN que garante acesso seguro e isolado, e a **Rede Privada EVPN**, rede interna em camada 2 responsável por conectar de forma segura e isolada os elementos do ambiente. Inclui ainda elementos de suporte à pesquisa, como **VM(s) Oper**, máquinas virtuais destinadas a hospedar ferramentas de monitoramento, *benchmarking* e exploradores de blocos, além de possibilitar a instalação de aplicações

próprias dos pesquisadores. Os elementos de instalação das plataformas Blockchain são representados pelos componentes **Cloud**, uma infraestrutura de nuvem composta por VMs preparadas para execução em contêineres e clusters Kubernetes, com flexibilidade para personalização de software e quantidade de recursos computacionais. Cada VM possui um gateway próprio para acesso à Internet e uma interface conectada à Rede Privada EVPN para comunicação direta com as demais VMs do ambiente. Os **Hosts** representam servidores físicos distribuídos geograficamente, responsáveis pela execução da nuvem, das plataformas blockchain e das VMs Oper, tendo seus recursos compartilhados entre diferentes ambientes. Dessa forma, cada um desses ambientes é formado por uma VPN, sua rede privada, VMs Oper e VMs Cloud distribuídas nos Hosts.

2.2.1 Cenários de Instalação. A instalação das plataformas blockchain a serem utilizadas nos experimentos pode ser realizada diretamente pelo pesquisador em seu ambiente dedicado, ou pela equipe técnica do projeto ILIADA, de acordo com as necessidades de cada experimento, garantindo flexibilidade e agilidade na configuração do ambiente de testes, de acordo com duas opções de cenários:

- Cenário 1: Instalação de uma blockchain inteira, com todos os nós (Nodes) hospedados em um único Host, simplificando o gerenciamento e a configuração da rede, sendo ideal para experimentos que requerem menor complexidade.
- Cenário 2: Instalação de uma blockchain distribuída sobre múltiplos Hosts. Esse cenário é útil para simulações de redes reais, com distribuição geográfica e onde as organizações precisam interagir em um ambiente descentralizado.

2.2.2 Tipos de Instalação. As seguintes opções de instalação são consideradas para os Cenários 1 e 2:

- 1 Scripts e Containers: Abordagem simples, utilizando scripts automatizados e containers docker, permitindo replicabilidade do ambiente e implantação das redes de forma rápida, acessível e de fácil manipulação;

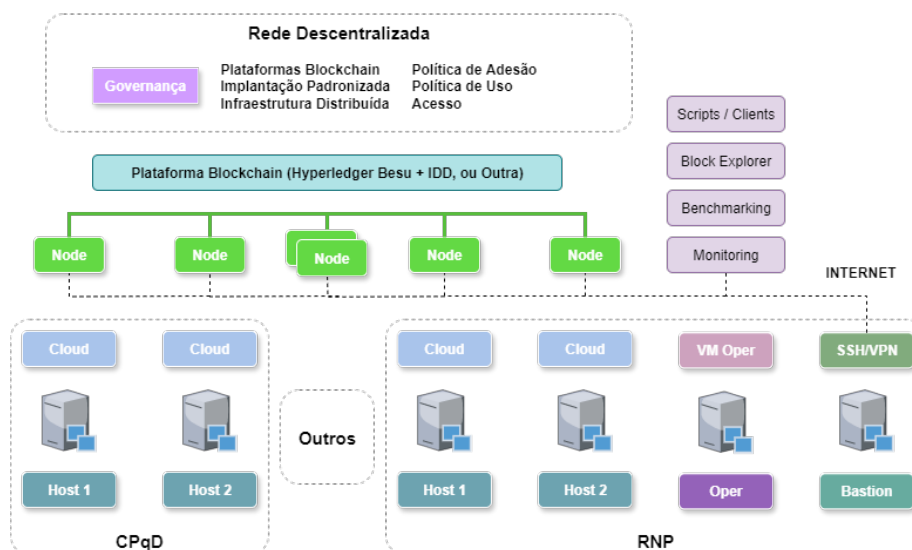


Figura 2: Arquitetura do ambiente para redes descentralizadas

- Cluster Kubernetes: Implantação da plataforma blockchain sobre Kubernetes, proporcionando um ambiente de orquestração de containers altamente escalável e resiliente, com suporte à distribuição e gestão automatizada de recursos;
- Hyperledger Bevel: Uso do framework para instalação modular e adaptável, alinhado às melhores práticas de implantação de plataformas Hyperledger e redes mais complexas;
- Portal blockchain EasyLedger: Plataforma modular e extensível desenvolvida dentro do projeto ILIADA, para a instalação automatizada e gerenciamento de redes blockchain Hyperledger, com uma interface gráfica web intuitiva, permitindo a implantação sucessiva de blockchains personalizadas e efêmeras sem a necessidade de manipulações complexas.

Essa variedade de opções atende às diferentes necessidades dos pesquisadores, permitindo a escolha do método mais adequado conforme os requisitos de cada experimento e o nível de complexidade desejado. O testbed busca garantir um ambiente adequado para cada projeto de pesquisa, oferecendo desde redes simples e localizadas até redes complexas e distribuídas geograficamente.

2.3 Ambientes para Redes Descentralizadas

Os ambientes para Redes Descentralizadas são ambientes multi-institucionais, servindo como infraestrutura para redes blockchain sob governança colaborativa entre a RNP e outras instituições participantes das redes em execução, sendo estas implantadas de forma distribuída, onde cada organização contribui com a manutenção de 2 ou mais nós “validadores” para cada rede em que ela é participante.

Essa abordagem tem o intuito e a vantagem de oferecer um cenário de blockchain descentralizada próximo a um ambiente de produção real, onde questões relacionadas à governança, disputas entre pares, permissionamento de nós e contas, assim como processos e procedimentos síncronos entre instituições participantes, podem ser corretamente percebidos, analisados, modelados e testados em um ambiente de testes que é próximo aos ambientes

corporativos reais. Múltiplas redes blockchain podem ser executadas simultaneamente sobre a mesma infraestrutura computacional, e instituições de ensino e pesquisa podem se tornar participantes desse ambiente, contribuindo com sua infraestrutura.

A primeira rede descentralizada implantada (Figura 2) usa a plataforma Hyperledger Besu, visando principalmente a experimentação em IDD (Identidade Digital Descentralizada), tendo algumas funcionalidades extras implantadas para esse fim.

Esse tipo de ambiente é constituído pelos mesmos elementos presentes os ambientes para redes dedicadas. Cada instituição participante, além da RNP é responsável por manter elementos **Cloud**, que representam a infraestrutura de nuvem utilizada para prover os recursos computacionais necessários à execução de seus nós blockchain, bem como os elementos **Hosts** correspondentes a eventuais equipamentos. A implantação segue modelos de pilha de software e configurações definidas pelo grupo de governança da rede, formado pelos participantes. A responsabilidade e o acesso aos equipamentos e VMs são exclusivos do respectivo participante proprietário, e cada conjunto de VMs pode suportar uma ou mais plataformas blockchain, seguindo a definição estabelecida pela governança. A comunicação entre os nós das redes descentralizadas ocorre via **Internet**, protegida por firewalls nas instituições, e o acesso aos nós blockchain pode ser realizado por meio da VM Oper na RNP ou diretamente pela internet, conforme acordado na governança.

3 CASOS DE USO EM WEB3

Dentre os casos de uso para experimentação estão assuntos como Identidade Digital Descentralizada (IDD), Criptomonedas para comunidades, Tokenização de ativos, NFTs (Non-Fungible Tokens), e plataformas para Organizações Autônomas Descentralizadas (DAOs).

Ao longo do projeto ILIADA, Grupos de Trabalho foram selecionados através de chamadas públicas para desenvolver pesquisas apoiadas pelo testbed. A seguir, são apresentados alguns casos de uso aderentes ao paradigma de soluções Web3.

3.1 Gestão de Identidade

A utilização de identidades digitais é um dos pilares da Web3, mas uma série de desafios podem ser destacados para a sua adoção: padronização de identidades, resistência das big techs a perder a posse das identidades dos usuários, conscientização dos usuários da sua responsabilidade como detentores de sua identidade digital, usabilidade das carteiras, interoperabilidade entre sistemas, etc.

Buscando entender diversos desses aspectos e construir novas soluções para a gestão de identidades digitais descentralizadas, exemplos de ações de pesquisa realizadas no Projeto ILIADA são:

- Portabilidade de identidade de sistemas Web 2.0 para Web3: estudo de viabilidade e desenvolvimento de uma plataforma de identidade digital descentralizada baseada em blockchain para garantir segurança, privacidade e interoperabilidade das identidades digitais com sistemas de autenticação federada, provendo uma solução robusta de autenticação e autorização através da convergência da segurança e privacidade da Web3 com a confiabilidade dos sistemas convencionais;
- Identidade digital para autenticação e autorização: algumas das pesquisas desenvolvidas consideram o uso mais "convencional" de IDD em Web3, através de AAA com credenciais verificáveis. Nessas situações, usuários devem apresentar suas credenciais, que são validadas por uma entidade verificadora, garantindo sua autenticidade e integridade, e passando os atributos necessários para que os sistemas realizem as operações de acordo com o perfil do usuário.

3.2 Cadeia de Custódia de Vestígios Digitais

A cadeia de custódia consiste em um conjunto de procedimentos que permitem documentar de forma sistemática e cronológica, todas as ações realizadas em um vestígio, desde sua identificação e coleta inicial até seu descarte final. Esse processo visa garantir a rastreabilidade da posse e manuseio da evidência, assegurando que ela permaneça íntegra e confiável ao longo de toda a investigação.

Ao término da cadeia, é essencial que se comprove que o conteúdo não sofreu nenhuma alteração durante o curso da investigação, preservando sua autenticidade como fonte de prova. Qualquer quebra de conformidade nesse processo compromete a credibilidade da evidência, podendo torná-la inadmissível judicialmente, assim como invalidar outras provas que tenham relação com ela.

Diante dos desafios de manter esse nível de controle e transparência, a tecnologia blockchain tem sido explorada por suas características de imutabilidade, descentralização e auditabilidade. A pesquisa em curso utiliza uma infraestrutura de blockchain para registrar e verificar a integridade dos vestígios durante todas as etapas da cadeia de custódia, garantindo a confiabilidade dos vestígios digitais para todos os entes envolvidos, como Polícias, Ministérios Públicos Estaduais e Federal e Seccionais da OAB.

3.3 Rastreabilidade de Cadeia Produtiva para Agricultura

A rastreabilidade da produção agrícola é um processo importante para garantir a origem dos produtos, bem como o atendimento a restrições e características específicas e, por isso, deve garantir a integridade, imutabilidade e disponibilidade das informações. Neste contexto, está sendo desenvolvida uma aplicação descentralizada

(Decentralized Application - DApp) voltada à rastreabilidade da cadeia produtiva de alimentos provenientes da agricultura familiar através da utilização de blockchain.

A solução visa assegurar transparência, segurança e auditabilidade dos participantes envolvidos no consumo, distribuição e auditoria (agricultores, cooperativas, consumidores, órgãos de fiscalização, etc.), promovendo maior controle e confiança nas informações compartilhadas entre os diversos atores envolvidos. A arquitetura da aplicação se baseia em tecnologia blockchain para a persistência das informações dos produtos/lotos, integrando contratos inteligentes (smart contracts) e tokens digitais como mecanismos para garantir a integridade, imutabilidade e disponibilidade dos dados.

3.4 DLT para gestão de recursos compartilhados

Um problema que diversos setores apresentam é a necessidade de compartilhamento de informações entre competidores para viabilizar a reserva e utilização de recursos.

Com o crescimento esperado da utilização de drones e veículos aéreos urbanos, uma situação trabalhada nas pesquisas do projeto ILIADA é voltada para a gestão eficiente do espaço aéreo, que será realizada por um conjunto de provedores de serviço concorrentes. Esses provedores serão responsáveis por funções como desconfito de rotas, roteamento e previsão meteorológica.

Todo esse gerenciamento se baseia em um serviço conhecido como Discovery and Synchronization Service (DSS). O DSS é um serviço descentralizado que permite a sincronização de informações críticas entre diferentes provedores de serviços, permitindo o compartilhamento seguro de dados, como planos de voo e restrições de espaço aéreo, garantindo que todos os participantes tenham acesso às informações mais atualizadas e consistentes. Entretanto, as atuais implementações de referência empregam um banco de dados distribuído convencional, não oferecendo imutabilidade, rastreabilidade e descentralização dos dados como seria possível com a adoção da tecnologia blockchain.

4 CONCLUSÃO

Soluções Web3 representam uma grande mudança no modo como sistemas digitais são concebidos e governados. Este artigo apresentou a estrutura de experimentação para P&D do projeto ILIADA, um projeto que está construindo um ambiente inovador para viabilizar o desenvolvimento de pesquisas baseadas em tecnologia blockchain, como sistemas Web3. O testbed permite uma alta personalização da infraestrutura de experimentação, oferecendo a oportunidade de explorar uma diversidade de tecnologias e configurações para o desenvolvimento de aplicações inovadoras e descentralizadas.

REFERÊNCIAS

- [1] EBSI 2025. European Blockchain Services Infrastructure. Acessível em: <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI>.
- [2] <https://www.lfdecentralizedtrust.org/projects/besu> [n. d.]. Hyperledger Besu.
- [3] <https://www.lfdecentralizedtrust.org/projects/fabric> [n. d.]. Hyperledger Fabric.
- [4] LACChain 2025. LACChain. Acessível em: <https://www.lacchain.net/home>.
- [5] LFDT 2025. Linux Foundation Decentralized Trust. Acessível em: <https://www.lfdecentralizedtrust.org/>.
- [6] RBB 2025. Rede Brasileira de Blockchain. Acessível em: <https://github.com/RBBNet/rbb>.