PROJETO ILÍADA

META 4 – PESQUISA E DESENVOLVIMENTO EM APLICAÇÕES DE BLOCKCHAIN EM ÁREAS ESTRATÉGICAS

Relatório da Atividade:
A4.3– Desenvolvimento de aplicações piloto

Blockchain em evolução.

Abril 2025

PROJETO ILÍADA
FASE 1

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

Sumário

1. Introdução

A Meta 4 do Projeto Ilíada (Integrando Livros-razão/ledgers, Infraestrutura e Aplicações Descentralizadas) visa estimular a pesquisa e desenvolvimento (P&D) em artefatos tecnológicos, aplicações e plataformas computacionais baseados em blockchain, visando contribuir para o amadurecimento da tecnologia no Brasil. Busca identificar aplicações estratégicas baseadas em tecnologia blockchain para o contexto científico, tecnológico e industrial brasileiro, além de levantar os requisitos mínimos de negócio e de desenvolvimento dessas aplicações.

Esses requisitos balizaram dois editais públicos que a Rede Nacional de Pesquisa (RNP) publicou para obter propostas de desenvolvimento das aplicações piloto a serem executadas na(s) rede(s) de experimentação resultantes da Meta 3. Um dos editais era direcionado à seleção de projetos acadêmicos e o outro voltado à seleção de empresas jovens (*startups*) para o desenvolvimento de protótipos funcionais de aplicações baseadas em tecnologia blockchain.

Para orientar os editais, as metas 4.1 e 4.2 traçaram um mapa do ecossistema atual de uso de blockchain no Brasil e definiram os setores mais estratégicos para o contexto científico, tecnológico e industrial brasileiro, de modo a sugerir os setores econômicos e os casos de uso de maior interesse para as chamadas públicas de propostas de implementações a serem feitas no âmbito do Projeto Ilíada.

Foram priorizados os seguintes setores econômicos: "agropecuário", "indústria de transformação", "água, esgoto, atividades de gestão de resíduos e descontaminação", "comércio e afins", "transporte, armazenagem e afins", "informação e comunicação", "financeiro", "administração pública, defesa e seguridade social", "educacional" e "saúde".

No que trata dos casos de uso, dos 36 descritos na tipologia adotada na Meta 4.1 foram priorizados 18 nas chamadas, a saber: "automatização de processos, contratos e transações", "identidades e credenciais digitais", "certificação", "tokenização de ativos", "criptomoedas", "gestão de ativos", "fracionamento de ativos", "transferências monetárias", "micropagamentos e microcrédito", "rastreamento de procedência", "rastreabilidade de cadeia", "prontuário médico digital", "receita digital", "economia do compartilhamento", "interoperabilidade", "governança e votação", "carteira digital" e "notarização".

Entre outras razões, optou-se também por incluir todos esses setores e casos de uso na chamada pública como uma forma de sondar a diversificação de iniciativas no ecossistema de blockchain no Brasil.

As propostas recebidas em resposta às duas chamadas públicas realizadas no âmbito do Projeto Ilíada (para grupos acadêmicos e para *startups*) mostraram uma razoável variedade de setores econômicos e casos de uso, o que, em certa medida, é indício de um ecossistema dinâmico e multifacetado. Nesse sentido, observou-se, também, uma diferença considerável nos níveis de maturidade aparente das propostas, o que pode sugerir que atuam no ecossistema atores com maior ou menor vivência com as tecnologias em questão.

Assim, nesta primeira versão do relatório da Meta 4.3 são apresentadas, de forma resumida, as propostas recebidas e selecionadas para execução durante o Projeto Ilíada. Como os desenvolvimentos ainda se encontram em fases iniciais, é apresentada aqui uma visão geral das aplicações que estão desenvolvidas e sua importância. Elas são descritas de forma detalhada, com destaque para suas funcionalidades principais e seus objetivos específicos, bem como detalhes técnicos (arquitetura, linguagens de programação, *frameworks* utilizados e outros aspectos relevantes).

1.1. Objetivos do relatório

No âmbito da Meta 4, a Atividade 4.3 tem o objetivo de mapear a descrição das aplicações selecionadas que serão desenvolvidas conforme os editais de chamada pública para Projetos de Pesquisa e Desenvolvimento (P&D) em Blockchain. A partir deles, foram selecionadas propostas de novas aplicações baseadas em blockchain, permitindo o amadurecimento do ecossistema blockchain no Brasil, a indução de construção de soluções para atendimento das demandas de governo e setor privado que auxiliem a transformação digital no país através da implantação e na promoção de serviços digitais mais confiáveis e de melhor qualidade para os cidadãos.

Este documento tem como objetivo principal fazer um relato inicial das frentes de desenvolvimento apoiadas pelo Projeto Ilíada e que se encontram nas primeiras fases de implementação. Em suas versões subsequentes, o relatório da Meta 4.3 trará mais informações sobre as implementações propriamente ditas.

1.2 Estrutura do relatório

O presente relatório está assim estruturado:

- Na Seção 2, descreve-se o processo de seleção de projetos de desenvolvimento das aplicações, tanto da academia quanto de *startups* e uma análise quantitativa dos projetos considerando a região à qual pertencem os proponentes, o setor econômico de adoção das aplicações propostas e as escolhidas;
- Na Seção 3, apresenta-se uma visão geral das aplicações que estão sendo desenvolvidas e sua importância. Além disso, apresentam-se duas listas de projetos selecionados (academia e *startups*) e uma descrição mais detalhada de cada um, incluindo os principais objetivos específicos, funcionalidades e detalhes técnicos das aplicações, tais como, arquitetura, linguagens de programação, *frameworks* utilizados, e outros aspectos relevantes;
- Na Seção 4 consta a documentação associada às aplicações, sejam manuais de usuário, guias técnicos e outros documentos relevantes e seus códigos fonte;
- A Seção 5 trata da análise do desempenho das aplicações, por meio de Indicadores (Key Performance Indicator - KPIs) relacionados ao funcionamento das aplicações. Além disso, apresenta-se a metodologia para coleta e análise dessas métricas de desempenho;
- Na Seção 6, são descritos os testes a ser realizados para validar as aplicações e os resultados, incluindo possíveis problemas identificados e soluções adotadas;
- Na Seção 7, apresentam-se as medidas de segurança implementadas, as vulnerabilidades identificadas e as medidas adotadas para mitigá-las;

- Na Seção 8, são identificados e descritos os desafios técnicos ou obstáculos enfrentados durante o desenvolvimento das aplicações e as estratégias empregadas para superá-los;
- A Seção 9 aborda a avaliação e discussão das inovações tecnológicas incorporadas às aplicações que estão sendo desenvolvidas, com ênfase nas tecnologias emergentes e nas abordagens pioneiras adotadas. Também são analisados o impacto dessas aplicações no contexto de sua utilização e os benefícios obtidos. Por fim, são apontadas possíveis melhorias futuras nas soluções apresentadas.
- Finalmente, na Seção 10, tem-se um resumo das conclusões extraídas do desenvolvimento das aplicações, bem como recomendações para otimizações ou expansões futuras.

2. Processo de seleção das aplicações

As chamadas públicas tiveram como objetivo fomentar a implantação de tecnologia blockchain em soluções inovadoras para aplicação no mercado por *startups*. Nesta seção serão apresentados e justificados os critérios de avaliação das propostas recebidas. Em seguida, as propostas serão avaliadas em termos de sua diversidade geográfica e de setor econômico de aplicação. Por fim, são listadas as propostas selecionadas para implementação no âmbito do Projeto Ilíada.

2.1 Seleção dos projetos acadêmicos

A seleção dos projetos acadêmicos foi conduzida por um comitê avaliador composto por pesquisadores da RNP e do CPQD, bem como por especialistas de entes externos convidados, como o BNDES, ou da academia.

Todas as propostas receberam cinco avaliações: duas da RNP, uma do CPQD, e duas de especialistas convidados. Para tanto, todas as propostas submetidas foram analisadas por um avaliador da RNP e um dos especialistas convidados. Para a segunda avaliação da RNP, as propostas foram divididas entre dois avaliadores, enquanto que para a segunda avaliação dos especialistas as elas foram divididas entre três avaliadores. Por fim, o CPQD dividiu as avaliações entre seus representantes no comitê de avaliação. Cada proposta teve duas avaliações, uma da RNP e outra dos especialistas, e a média dessas avaliações foi calculada para se ter o mesmo peso da dos demais avaliadores.

As propostas passaram pelos critérios de avaliação mostrados nas Tabelas 1 e 2.

Tabela 1 - Critérios de avaliação para seleção das propostas da academia

Critério 1	**Experiência do grupo nos tópicos da chamada**: Analisa os currículos Lattes para avaliar a experiência geral dos membros da equipe, especialmente nas áreas de cibersegurança e desenvolvimento de aplicações no contexto de blockchain.
Critério 2	**Proposta de valor da aplicação**: Considera a forma como o produto ou serviço se diferencia da concorrência e que benefícios serão entregues aos potenciais usuários.
Critério 3	**Aderência Temática**: Verifica se a proposta é pertinente com os setores e tópicos de interesse priorizados na chamada.
Critério 4	**Viabilidade Técnica**: Avalia se é viável executar a proposta no prazo de nove meses.
Critério 5	**Qualidade da proposta**: Avalia a qualidade e a clareza da proposta enviada com relação aos seus objetivos e motivações, à complexidade da execução e aos resultados esperados.

Tabela 2 - Critérios auxiliares de avaliação para seleção das propostas da academia

Critério Auxiliar 1	**Indicação de ambiente de desenvolvimento e experimentação**: As aplicações a serem desenvolvidas devem, preferencialmente, fazer uso de um dos *frameworks* suportados pelo Projeto Ilíada. Também foi permitida a utilização de redes públicas, mas os custos dessa utilização ficariam a cargo dos proponentes.
Critério Auxiliar 2	**Indicação de responsável técnico**: Para viabilizar a adequada implementação da aplicação proposta a equipe executora deve contar com ao menos um membro com formação em computação e experiência técnica comprovada em blockchain.
Critério Auxiliar 3	**Avaliação Geral**: Nível de recomendação da proposta: 1: Rejeição Forte 2: Rejeição Fraca 3: Aceitação Fraca 4: Aceitação Forte

Como resultado dessa chamada de projetos de pesquisa e desenvolvimento em Blockchain, a RNP recebeu 14 projetos.

A Figura 1 mostra a distribuição geográfica das propostas recebidas. Nota-se uma predominância de propostas oriundas de instituições acadêmicas das regiões Sudeste e Nordeste. A região com menos propostas é a Centro-oeste.

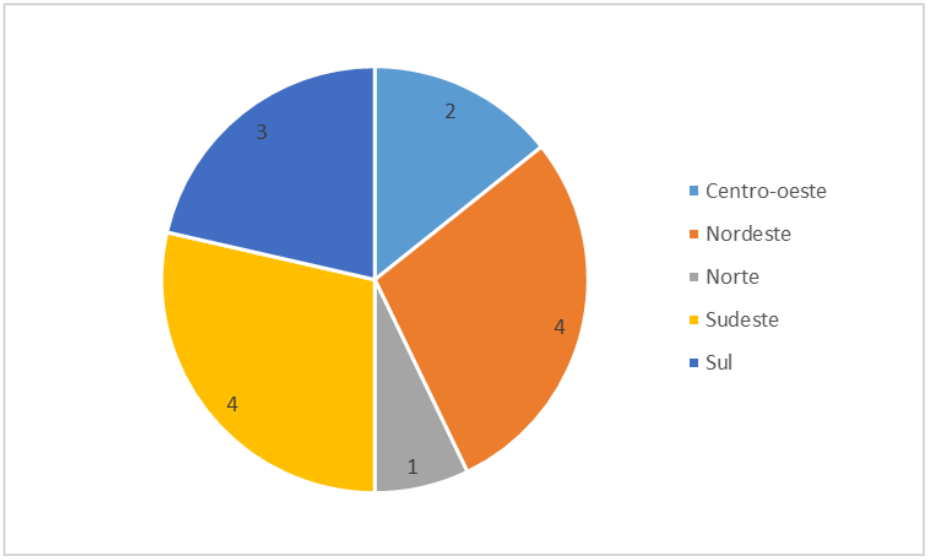

Figura 1 - Distribuição dos projetos por região geográfica do Brasil[1]

A Figura 2 analisa outro aspecto das propostas apresentadas, que é o setor econômico em que as aplicações estão inseridas, quais sejam: "Financeiro", "Comércio e afins", "Administração pública, defesa e seguridade social", "Saúde", "Agropecuária" e "Educacional ". Nota-se que o setor econômico com maior quantidade de propostas é o da Educacional (4 propostas), seguido da "Saúde" e "Agropecuária" (3 propostas cada) e "Administração pública, defesa e seguridade social" (2 propostas). Os demais setores mencionados contam com um proposta cada.

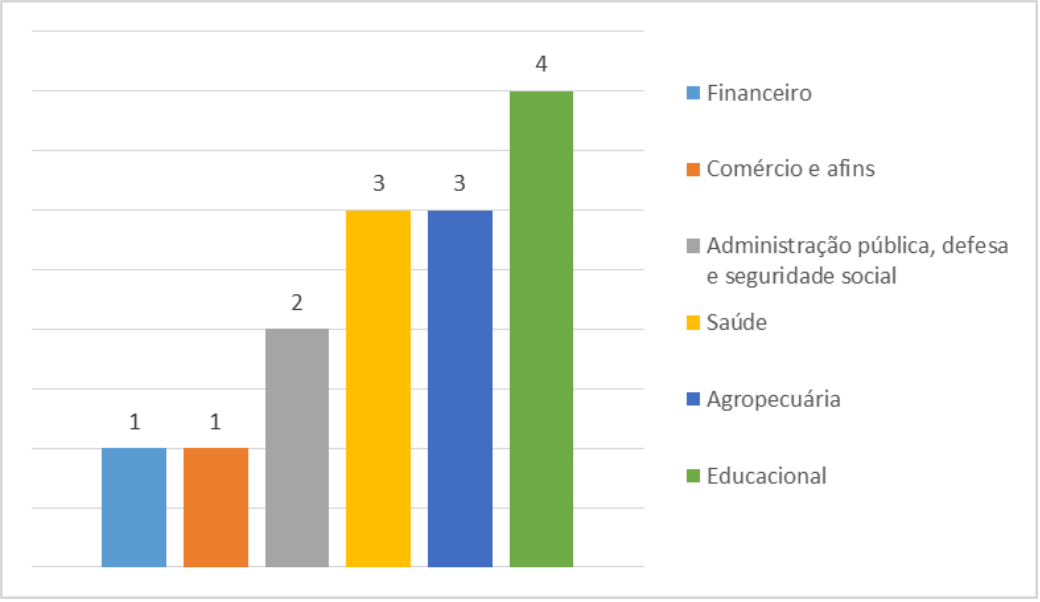

Figura 2 - Distribuição dos projetos por setor econômico[2]

A Tabela 3 apresenta a lista dos grupos de trabalho que foram selecionados com base nos critérios apresentados nas Tabelas 1 e 2, o nome do proponente principal e a

[1] Elaborada pelos autores do relatório.
[2] Elaborada pelos autores do relatório.

Instituição de Ensino Superior (IES) à qual pertencem. A lista está em ordem alfabética do título da proposta.

Tabela 3 - Grupos de trabalho selecionados

Projeto	Proponente Principal	IES
GT-CarbonID: Plataforma de Tokenização de Créditos de Carbono	Leobino N. Sampaio	UFBA
GT-ChainGuard: Proposta de desenvolvimento de cadeia de custódia de vestígios digitais utilizando a infraestrutura de blockchain	Renato Torres	UFPA
GT-Smart AgroRAF: Smart Contracts para Rastreamento da Agricultura Familiar	Rodrigo B. Mansilha	UNIPAMPA
GT-SWARM: Self-sovereign wi-fi Authentication Roaming	Carla M. Westphall	UFSC

2.2 Seleção dos projetos das *startups*

Assim como nos projetos acadêmicos, o processo de seleção dos projetos de *startups* foi conduzido por um comitê de avaliação composto por especialistas da RNP, do CPQD e do BNDES.

Todas as propostas receberam três avaliações: uma avaliação da RNP, uma do CPQD, e uma do BNDES. Enquanto os representantes da RNP e do BNDES no comitê avaliaram todas as propostas submetidas, os do CPQD dividiram entre si as avaliações.

No processo de avaliação foram considerados os seis critérios que compõem a média da nota de cada proposta, todos com o mesmo peso, como apresentados na Tabela 4. Além disso, adotou-se um critério de avaliação auxiliar, mostrado na Tabela 5.

Tabela 4 - Critérios de avaliação para seleção das propostas das *startups*

Critério 1	Experiência de mercado: Será avaliada a experiência de mercado da *startup*.
Critério 2	Experiência técnica: Avalia o conhecimento técnico da *startup* no desenvolvimento de soluções no setor escolhido e a capacidade de evoluir a solução existente para suportar o uso de blockchain.
Critério 3	Proposta de valor: Avalia os potenciais benefícios e diferenciais da solução proposta para o mercado, bem como ela pode auxiliar na consolidação da tecnologia blockchain no país.
Critério 4	Aderência temática: Verifica se a proposta é pertinente com os setores e tópicos de interesse priorizados na chamada.
Critério 5	Viabilidade tecnológica: Avalia a viabilidade da proposta considerando o prazo e o ambiente de desenvolvimento a ser adotado.
Critério 6	Qualidade da proposta: Avalia a qualidade da proposta enviada com relação à descrição da solução proposta, à clareza e objetividade das informações e aos resultados esperados com a adoção da tecnologia blockchain.

Também foi considerado o critério auxiliar, apresentado na Tabela 5.

Tabela 5 - Critérios de avaliação auxiliares para seleção das propostas das *startups*

Critério Auxiliar 1	Avaliação Geral: Recomendação da Proposta 1: Rejeição Forte 2: Rejeição Fraca 3: Aceitação Fraca 4: Aceitação Forte

Como resultado da chamada, foram recebidas 11 propostas, das quais nove foram consideradas aptas.

A Figura 3 mostra a divisão dos projetos de *startups* por região geográfica. Observa-se, nesse caso, que apenas houve submissões das regiões Nordeste, Sudeste e Sul (três propostas cada).

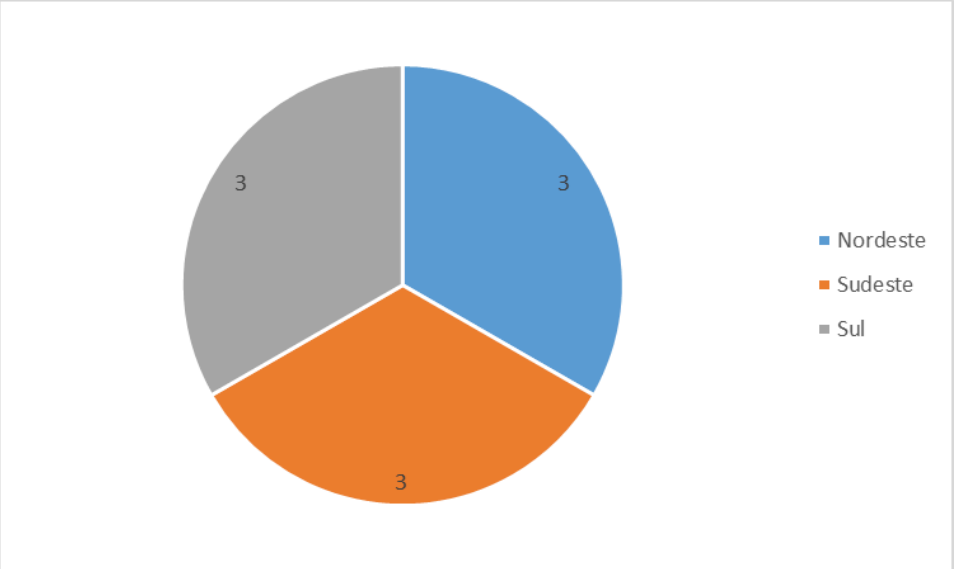

Figura 3 - Distribuição dos projetos de *startups* por região[3]

Já a Figura 4 traz a segmentação dos projetos por setor econômico, em que predominam as propostas dos setores "Educacional" e "Saúde" (duas propostas). Os setores "Administração pública, defesa e seguridade social", "Agropecuária", "Água, esgoto, gestão de resíduos e descontaminação", "Financeiro" e "Informação e comunicação" contaram com uma proposta cada.

[3] Elaborada pelos autores do relatório.

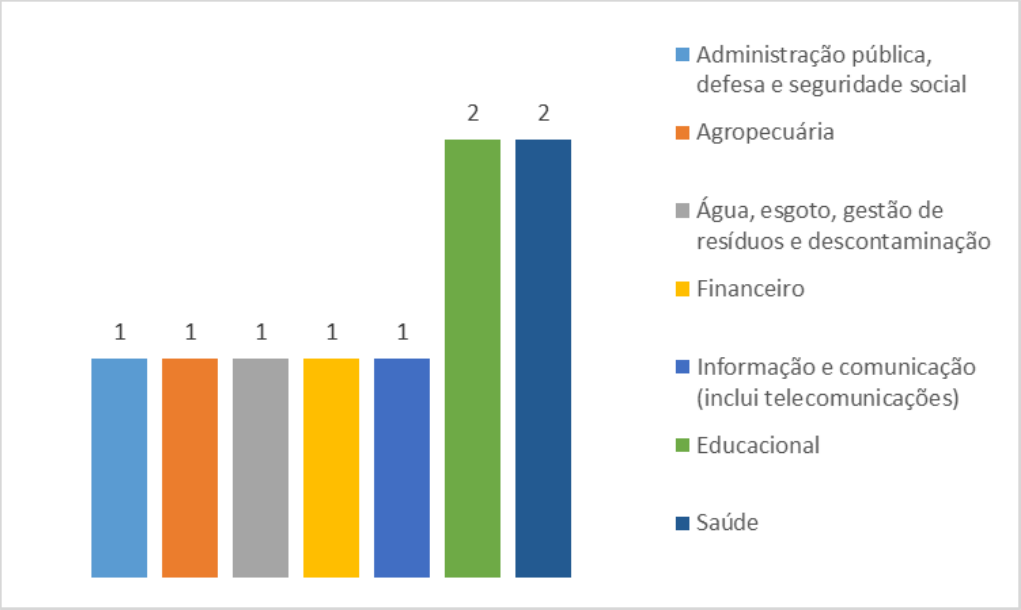

Figura 4 - Distribuição dos projetos de *startups* por setor econômico[4]

A Tabela 6 apresenta, na ordem alfabética do título da proposta, a lista das *startups* selecionadas.

Tabela 6 - Propostas de *startups* selecionadas

Proposta	Proponente principal	Empresa
DAIESEB: Digitalização do acervo acadêmico de instituições de ensino superior com base em inteligência artificial e blockchain.	Rafael Escrich	Certisecure
Levery: Plataforma de carteira digital e negociação de ativos tokenizados	Cristiano Policarpo	Wire Labs
Modelagem de aplicações piloto baseadas em NFTs de ciclo preditivo utilizando a plataforma Ledger NFT	Caio S. Florentino	Ledgertec
Rastreabilidade química inteligente: agricultura na era da blockchain	Mônica Vianna	Sollytch

3. Descrição das aplicações a serem desenvolvidas e sua importância

Nesta seção, apresenta-se para cada uma das aplicações que estão desenvolvimento:

- **Visão geral das aplicações desenvolvidas** e sua importância (proposta de valor);
- **Listagem** dos projetos e **descrição detalhada** de cada aplicação que está sendo desenvolvida;

[4] Elaborada pelos autores do relatório.

- **Funcionalidades principais**, **objetivos específicos** e **detalhes técnicos** de cada aplicação, incluindo arquitetura, linguagens de programação, *frameworks* utilizados, e **outros aspectos relevantes**.

Além disso, são destacados o(s) responsável(is) pela execução das atividades previstas no desenvolvimento das aplicações, equipe executora e, quando aplicável, consultores. São primeiramente descritos os projetos acadêmicos e, em seguida, os das *startups*.

3.1 Projetos acadêmicos

Os projetos acadêmicos selecionados são os seguintes:

- GT-CarbonID - Plataforma de tokenização de créditos de carbono
- GT-ChainGuard - Proposta de desenvolvimento de cadeia de custódia de vestígios digitais utilizando a infraestrutura de blockchain
- GT-SWARM - Self-sovereign wi-fi authentication roaming
- GT-Smart AgroRAF - Smart contracts para rastreamento da agricultura familiar

A seguir, apresenta-se o detalhamento de cada um dos mencionados projetos.

3.1.1 GT-CarbonID - Plataforma de tokenização de créditos de carbono

A plataforma de tokenização de créditos de carbono (GT-CarbonID) tem como tópicos de interesse identidade digital descentralizada (IDD), certificação, tokenização de ativos e como principal setor econômico de aplicação a Agropecuária.

O desenvolvimento da aplicação está sendo coordenado pelo Prof. Leobino Nascimento Sampaio, da Universidade Federal da Bahia (UFBA). Integram a equipe os colaboradores apresentados na Tabela 7.

Tabela 7 - Equipe de Colaboradores do GT-CarbonID

Nome do colaborador	Instituição	URL do currículo Lattes
Prof. Leobino N. Sampaio	UFBA	http://lattes.cnpq.br/1952937182023132
Prof. Alan S. dos Santos	IFBA	http://lattes.cnpq.br/8254119995385483
Prof. Anderson da S. Carvalho	UFBA	http://lattes.cnpq.br/9225499996748414
Daniel A. de Oliveira Neves	UFPA	https://lattes.cnpq.br/1844593396780142
Osvaldo L. Santana Filho	UFBA	http://lattes.cnpq.br/9205720021595816
Silvio José de Queiroz Pereira	Smart Trends	https://lattes.cnpq.br/0793061929576345

3.1.1.1 Visão geral do GT-Carbon ID e sua importância

O projeto CarbonID nasce como uma resposta às fragilidades identificadas no mercado voluntário de créditos de carbono no Brasil, como a inexistência de regulamentação e de padrões, a baixa credibilidade e transparência, a falta de mecanismos confiáveis de auditoria, custos potencialmente altos de associados à verificação, à certificação e a transações de créditos de carbono, o que reduz os benefícios financeiros para os participantes, além do risco de dupla contagem de emissões. Diante desse cenário, o projeto CarbonID propõe desenvolver uma plataforma baseada em blockchain e IDD para criar um ambiente seguro, transparente e auditável de registro e gestão de créditos de carbono.

Inspirado na experiência da equipe com a plataforma ChainID, o CarbonID busca combinar blockchain, armazenamento descentralizado e IDD para criar um ambiente para armazenamento rastreável de dados, multi-inquilino (*multi-tenant*). O uso de IDD garante rastreabilidade, integridade e descentralização das informações, agregando confiabilidade a um mercado ainda carente de mecanismos robustos de governança.

Além de atender diretamente o mercado de créditos de carbono, a plataforma CarbonID também se propõe a ser adaptável a uma gama de outras aplicações que demandam processos confiáveis de certificação, rastreamento e validação.

A importância estratégica do projeto vem do fato de que sua implementação consolida a posição do Brasil como líder no mercado global de créditos de carbono, cuja previsão de movimentação ultrapassa os US$ 300 bilhões até 2050. Ao solucionar problemas estruturais de governança, auditabilidade e confiança, a plataforma contribui para evitar práticas de fraude ambiental (*greenwashing*), fortalecer a integridade das transações e estimular a entrada de novos participantes — inclusive pequenos produtores e investidores.

O projeto também se alinha com os recentes esforços legislativos para regulamentar o mercado nacional de carbono, antecipando as necessidades tecnológicas que a nova regulação exigirá. Com sua abordagem, o CarbonID oferece um modelo de governança descentralizada que aumenta a transparência e a segurança de todo o ecossistema.

Embora o foco inicial da CarbonID seja o mercado de créditos de carbono, a plataforma foi projetada para ser adaptável a uma ampla gama de indústrias que demandam alta confiabilidade e rastreabilidade, como:

- Alimentos e bebidas: Rastreabilidade da cadeia de produção para certificações de qualidade e origem;
- Indústria farmacêutica: Monitoramento de insumos e controle de conformidade sanitária;

- Moda e vestuário: Verificação de práticas sustentáveis e origem de materiais;
- Tecnologia e eletrônicos: Garantia de procedência e conformidade de componentes;
- Varejo e distribuição: Logística e monitoramento de cadeia de suprimentos;
- Órgãos governamentais e reguladores: Fiscalização e conformidade em processos regulatórios.

Cada setor apresenta desafios específicos que podem ser mitigados pela adoção da CarbonID como solução para transparência, segurança e governança de dados.

Assim, o CarbonID se propõe não apenas a impulsionar a eficiência e credibilidade do mercado de carbono no Brasil, como também abrir caminho para modelos de negócios sustentáveis e inovadores, promovendo a transformação digital em setores que dependem de transações de alto grau de confiança.

Adicionalmente, provê um repositório de dados e metadados como serviço que permite rastreabilidade com confiabilidade, privacidade e segurança. Como características tecnológicas, a solução de tokenização não apenas utiliza a blockchain Ethereum e o padrão ERC-721 [1] para criar *tokens* não fungíveis (NFTs) que representam créditos de carbono, mas também integra o potencial das identidades digitais descentralizadas. Isso permite uma certificação digital autêntica, transparente e verificável, em que as entidades certificadoras podem validar projetos de mitigação de carbono de forma segura e eficiente. Com o armazenamento descentralizado de metadados, a plataforma assegura a rastreabilidade completa e a transparência das transações.

Por fim, a interface de usuário intuitiva facilita a criação, gerenciamento e certificação de *tokens*, enquanto a conformidade com regulamentações ambientais globais garante a legitimidade dos *tokens* emitidos. Isso simplifica o acesso ao mercado de carbono e promove a sustentabilidade e a responsabilidade ambiental de forma escalável e segura, aproveitando o poder das identidades digitais descentralizadas para aumentar a confiança, a auditabilidade e a eficiência do sistema como um todo.

3.1.1.2 Descrição detalhada do GT-Carbon ID

A CarbonID busca resolver os problemas de rastreabilidade, segurança e transparência em cadeias de produção e suprimentos — com foco inicial no mercado de créditos de carbono, mas com potencial de aplicação em outros setores industriais.

Para tanto, a arquitetura foi projetada de forma *multi-tenant*, permitindo que múltiplas organizações utilizem a mesma infraestrutura de maneira independente, com espaço de dados próprio, preservando a privacidade e a integridade das informações.

A solução integra:

- Hyperledger Besu: para garantir a imutabilidade dos registros e a criação de contratos inteligentes;
- Arweave: para o armazenamento descentralizado, assegurando que dados e documentos estejam permanentemente disponíveis e sem adulterações;
- ChainID: para gestão de IDD, aumentando a confiança entre participantes ao permitir autenticação e verificação de identidade sem intermediários centrais.

A Figura 5 apresenta a plataforma, suas tecnologias e o ecossistema envolvido. Como pode ser observado, a solução de rastreabilidade *multi-tenant* poderá atender a uma ampla gama de indústrias que exigem sistemas robustos para garantir transparência, segurança e conformidade regulatória em suas cadeias de suprimentos. Cada setor enfrenta desafios únicos que podem ser mitigados pela adoção de uma plataforma de rastreabilidade integrada e segura, com um ambiente de validação e experimentação no *testbed* do Projeto Ilíada.

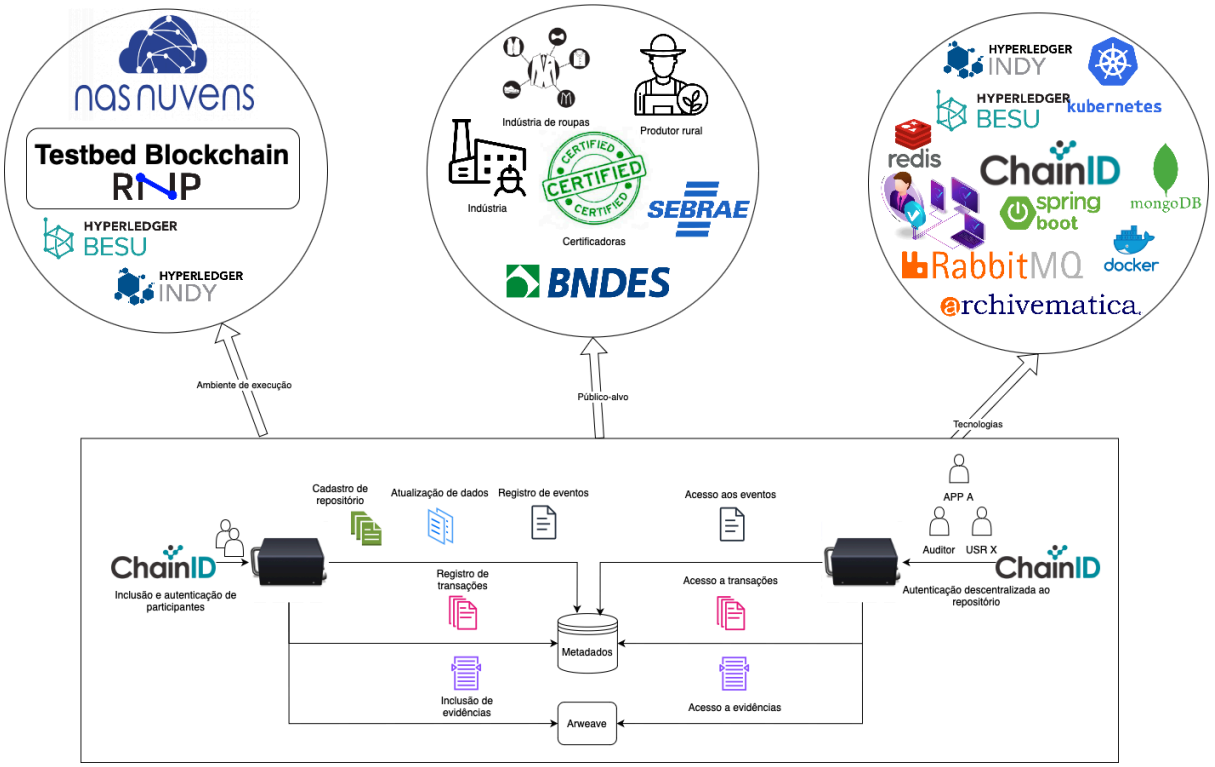

Figura 5 - Ecossistema da Solução da Plataforma CarbonID[5]

O projeto ainda prevê a criação de um ciclo de vida completo dos *tokens* de carbono, da submissão do projeto, passando pelas etapas de revisão, certificação, construção, e chegando à publicação e validação dos créditos de carbono.

3.1.1.3 Principais funcionalidades, objetivos específicos e detalhes técnicos do GT-CarbonID

A solução CarbonID baseia-se no conceito de "sem código" (do inglês, *no-code*) e nos princípios de experiência do usuário (UX) e usabilidade para abstrair a complexidade do

[5] Extraída da proposta apresentada à RNP em resposta aos Editais.

mercado voluntário e facilitar a criação dos *tokens*. Utilizará também IDD a fim de alavancar a identificação dos participantes e tirar proveito das características da tecnologia blockchain assegurando auditabilidade, transparência, segurança e confiança em todas as transações realizadas.

Um dos principais fundamentos da solução será a utilização do Hyperledger Besu, voltado para assegurar a integridade e a imutabilidade dos dados. Todos os eventos e transações serão registrados na blockchain, tornando as informações invioláveis e auditáveis. Essa abordagem protege contra fraudes e alterações indevidas, garantindo que os dados se mantenham precisos e confiáveis ao longo do tempo.

Além disso, a transparência oferecida pela blockchain permitirá rastrear toda a cadeia de suprimentos, proporcionando às partes interessadas acesso a informações claras e confiáveis em todas as etapas do processo.
Para o armazenamento de documentos, a solução adota o Arweave, uma plataforma de armazenamento descentralizado que assegura a permanência e a proteção dos dados. O Arweave armazenará documentos relevantes, como certificados e registros de transações, os quais permanecerão acessíveis e seguros contra perdas ou alterações. O hash desses documentos será registrado na blockchain, possibilitando a verificação da integridade dos arquivos a qualquer momento. Essa estratégia de armazenamento descentralizado eliminará a dependência de servidores centralizados e reforçará a resiliência do sistema frente a possíveis falhas.

A integração da IDD, por meio da plataforma ChainID, acrescentará à solução uma camada de segurança e autenticidade assegurando que todas as transações e usuários sejam validados de forma confiável, prevenindo acessos não autorizados e garantindo a integridade das operações. Além disso, a interoperabilidade do IDD com outros sistemas permitirá que as identidades sejam reconhecidas e validadas em diferentes plataformas e organizações ao redor do mundo, favorecendo uma integração segura e harmoniosa em um ecossistema global e ampliando a adaptabilidade da solução a diversas necessidades e contextos.

A automação dos processos de rastreabilidade é outro elemento essencial da solução. A plataforma automaticamente registra eventos e transações, reduzindo intervenções manuais e erros humanos. Essa automação melhora a eficiência operacional, como também contribui para a redução de custos relacionados ao monitoramento e à manutenção de registros. Além disso, a plataforma assegura conformidade com normas internacionais reconhecidas, como GS1 [2], ISO 22005 [3] e ISO 14064 [4], facilitando sua adoção por empresas que precisam atender a exigências regulatórias rigorosas. Em síntese, a solução apresenta uma abordagem integrada, segura e eficiente para a rastreabilidade, atendendo diferentes setores e promovendo transparência e confiança em cadeias de suprimentos e outros mercados.

Adicionalmente, a integração da CarbonID ao ambiente de experimentação do *testbed* do Projeto Ilíada potencializa a pesquisa, a experimentação e o desenvolvimento contínuo de inovações na área de rastreabilidade baseada em blockchain. Essa iniciativa fortalece o ecossistema de testes, criando um espaço para inovação e

aperfeiçoamento constante, onde desenvolvedores e pesquisadores podem testar e validar novas funcionalidades. Isso garante que a plataforma permaneça alinhada às melhores práticas e às tecnologias emergentes.

Linguagens de programação e *frameworks*

Conforme apresentado na Figura 5, as principais tecnologias envolvidas são:

- **Hyperledger Indy** é utilizado para a gestão de IDDs, oferecendo uma infraestrutura robusta e segura para a criação e verificação de identidades. É essencial para assegurar a autenticidade dos produtores rurais e das entidades certificadoras, garantindo que todos os participantes da plataforma sejam quem dizem ser. A opção pelo Hyperledger Indy se deu em função de sua especialização em identidade descentralizada e sua capacidade de proteger a privacidade dos usuários;
- **MongoDB** é um banco de dados NoSQL altamente escalável e flexível, é utilizado para armazenar grandes volumes de dados estruturados e semiestruturados. No contexto da plataforma CarbonID, o MongoDB armazena informações detalhadas sobre os participantes dos processos, incluindo dados dos produtores, produtos, consumidores, logística, assim como metadados e registros de transações. A escolha do MongoDB é devido à sua flexibilidade em lidar com diferentes tipos de dados e sua escalabilidade horizontal;
- **Redis** é utilizado para caching e como forma de notificação de comunicação entre APIs usando chamadas assíncronas implementadas com filas no RabbitMQ. Esse banco de dados em memória permite acessos rápidos e eficientes, melhorando a performance da plataforma ao armazenar sessões de usuário e dados temporários durante processos de verificação. O Redis é utilizado devido à sua velocidade e eficiência em operações de leitura e escrita, além de sua capacidade de suportar comunicação em tempo real. O Redis, além de ser usado para caching, será usado na comunicação entre APIs, implementando chamadas assíncronas com filas no RabbitMQ para garantir eficiência e rapidez no processamento das validações;
- **RabbitMQ** é um sistema de mensagens que facilita a comunicação entre diferentes componentes da plataforma, gerenciando filas de mensagens e garantindo a entrega confiável de dados. Ele é essencial para coordenar tarefas assíncronas, como a verificação de identidades e o processamento de transações de NFTs. O RabbitMQ foi escolhido pela sua robustez e capacidade de garantir a entrega de mensagens em sistemas distribuídos, essencial para a nossa arquitetura assíncrona;
- **Arweave** é uma tecnologia de armazenamento descentralizado que utiliza um modelo de pagamento único para garantir a preservação permanente de dados. Diferente de outras soluções, Arweave oferece um armazenamento imutável e resistente à censura, utilizando uma estrutura de blockchain-like para garantir que os dados armazenados sejam seguros e acessíveis indefinidamente. Na solução da plataforma CarbonID, Arweave é aplicado para assegurar o armazenamento permanente e seguro de documentos, registros digitais, fotos e vídeos, permitindo que esses dados sejam auditáveis e verificáveis a qualquer momento. Essa capacidade é crucial para manter a integridade e a

confiabilidade dos registros de rastreabilidade, garantindo que todas as transações e evidências associadas permaneçam acessíveis e inalteradas ao longo do tempo, facilitando a conformidade regulatória e a transparência nas operações;

- **Plataforma Hyperledger Besu** é uma plataforma de blockchain empresarial de código aberto projetada para ser altamente flexível, permitindo a implementação tanto em redes públicas quanto privadas de Ethereum. No contexto da plataforma CarbonID, Hyperledger Besu é utilizado para registrar de forma imutável todos os eventos e transações, garantindo a integridade e a transparência dos dados. Ele oferece suporte a contratos inteligentes, permitindo a automação segura de processos de negócios e a verificação de transações. Sua arquitetura robusta e compatibilidade com ferramentas empresariais fazem dele a escolha ideal para assegurar que todos os registros na plataforma de rastreabilidade sejam confiáveis e auditáveis, promovendo a confiança entre todas as partes envolvidas;
- **Plataforma Ethereum** é utilizada para a criação e gestão de NFTs, oferecendo um ambiente seguro e transparente para a emissão e negociação de créditos de carbono tokenizados. Os contratos inteligentes (smart contracts) em Ethereum garantem que os NFTs sejam criados de acordo com padrões específicos (ERC-721/ERC-1155), assegurando sua integridade e rastreabilidade. A opção pela Ethereum se deve à sua ampla adoção, segurança comprovada e capacidade de suportar contratos inteligentes complexos;
- **Spring Boot** é um *framework* Java que facilita a criação de aplicações robustas e escaláveis, utilizado para desenvolver os serviços backend da plataforma CarbonID. Ele fornece um ambiente de desenvolvimento rápido e produtivo, permitindo a construção de APIs RESTful que suportam a interação entre os diversos componentes da plataforma. O Spring Boot foi escolhido em função de sua robustez, facilidade de configuração e ampla comunidade de suporte.

A solução proposta baseia-se em tecnologias consolidadas e desenvolvimentos anteriores da equipe, operando em ambiente *cloud*. Ela oferece serviços de registro, recuperação e atualização de dados para setores que precisam de rastreabilidade em suas cadeias de produção ou suprimentos. O diferencial da plataforma está na tokenização de créditos de carbono utilizando blockchain Ethereum e o padrão ERC-721 para criar NFTs (*tokens* não fungíveis), integrando identidades digitais descentralizadas (IDD) para garantir certificação digital autêntica e transparente.

Com armazenamento descentralizado, a plataforma assegura rastreabilidade e transparência das transações. Sua interface intuitiva facilita a criação e certificação de *tokens*, enquanto a conformidade com regulamentações ambientais globais garante sua legitimidade. Essa abordagem promove a sustentabilidade, a responsabilidade ambiental e a confiança no mercado de carbono, tornando o sistema mais eficiente e seguro.

3.1.2 GT-ChainGuard - Proposta de desenvolvimento de cadeia de custódia de vestígios digitais utilizando a infraestrutura de blockchain

A Proposta de desenvolvimento de cadeia de custódia de vestígios digitais utilizando a infraestrutura de blockchain (GT-ChainGuard) tem como tópico de interesse a trilha de auditoria e como principal setor econômico de aplicação a Administração pública.

O desenvolvimento desta aplicação está sendo coordenado pelo Prof. Renato Hidaka Torres da Universidade Federal do Pará (UFPA). Formam a equipe de trabalho os colaboradores apresentados na Tabela 8.

Tabela 8 - Equipe de Colaboradores do GT-ChainGuard

Nome do colaborador	Instituição	URL do currículo Lattes
Prof. Renato Hidaka Torres	UFPA	http://lattes.cnpq.br/7469949213441010
Prof. Roberto S. dos Santos Araújo	UFPA	http://lattes.cnpq.br/6894507054383644
Fernanda dos Santos Borges	UFPA	http://lattes.cnpq.br/2487637732739787
Christian Amarildo Amorim Morais	UFPA	http://lattes.cnpq.br/7795948249534200
João Samuel Dias Santos	UFPA	http://lattes.cnpq.br/1763125013579875
Sainy Gabriel Rosa Dias Antonio	UFPA	http://lattes.cnpq.br/8584884245613422

3.1.2.1 Visão geral do GT-ChainGuard e sua importância

O projeto ChainGuard propõe a criação de uma rede blockchain dedicada ao registro da cadeia de custódia de evidências digitais, garantindo a segurança, autenticidade, rastreamento e imutabilidade de todo o processo, desde a coleta das evidências até sua apresentação em julgamento.

A solução utiliza a tecnologia blockchain para manter um livro-razão imutável e atualizado, onde todas as ações relacionadas às evidências são registradas de maneira transparente e auditável.

Com a implementação da ChainGuard, procedimentos que atualmente dependem de processos manuais ou sem padronização poderão ser automatizados e supervisionados dentro da rede, com políticas claras de endosso e controle de acesso. A utilização de identidades digitais únicas para cada participante da rede — garantidas por certificados de autenticação — assegura que todos os acessos e alterações no sistema sejam identificáveis e rastreáveis.

A importância do ChainGuard reside principalmente na elevação da confiabilidade jurídica de provas digitais em processos judiciais. Ao registrar de forma imutável cada etapa da cadeia de custódia, o projeto visa mitigar a anulação e a inadmissibilidade de provas por falhas processuais ou suspeitas de manipulação. Além disso, a rede

blockchain proporciona segurança reforçada contra acessos não autorizados e ataques cibernéticos, fortalecendo a preservação de informações sensíveis.

O projeto também promove a transparência e a confiança entre diferentes autoridades e órgãos envolvidos na custódia de provas digitais, aumentando a segurança jurídica e favorecendo um tratamento mais imparcial e eficiente das evidências. Em resumo, o ChainGuard se apresenta como uma inovação crucial para modernizar, proteger e dar mais credibilidade ao processo de gestão de provas digitais no contexto jurídico.

3.1.2.2 Descrição detalhada do GT-ChainGuard

A cadeia de custódia passou a ter previsão expressa no ordenamento jurídico brasileiro com a promulgação da Lei nº 13.964/2019 [5], conhecida como Pacote Anticrime. Essa legislação inseriu os artigos 158-A a 158-F no Código de Processo Penal, estabelecendo e tornando obrigatório o procedimento de preservação de vestígios. Conforme o artigo 158-A, a cadeia de custódia compreende o conjunto de práticas destinadas a preservar e registrar toda a trajetória de um vestígio, desde o momento em que é identificado até seu descarte, garantindo o rastreamento cronológico de sua posse e manipulação.

O processo deve assegurar que o vestígio permaneceu intacto ao longo de toda a investigação, garantindo a integridade e a confiabilidade da prova. Caso os procedimentos adequados não sejam seguidos — caracterizando a quebra da cadeia de custódia —, torna-se impossível comprovar que os vestígios mantêm sua condição original, o que pode levar à exclusão dessas provas e de todas as provas delas derivadas no processo judicial.

Vale destacar que, embora a legislação tenha detalhado o tratamento de provas físicas e materiais, ela ainda carece de regulamentação específica para a preservação e custódia de vestígios digitais.

O ciclo de vida da prova digital é um aspecto essencial no processo forense, devido à sua natureza dispersa, volátil e suscetível a alterações, sejam elas acidentais ou intencionais [6]. Por essa razão, o projeto ChainGuard propõe o uso da tecnologia blockchain aliado às normas internacionais, como a ABNT NBR ISO/IEC 27037 [7], para nortear suas práticas. Essa norma estabelece que as evidências digitais devem obedecer a três princípios centrais: relevância, confiabilidade e suficiência. Para assegurar a confiabilidade, todos os procedimentos de manipulação das evidências digitais precisam ser auditáveis e passíveis de reprodução. Além disso, recomenda-se que a cadeia de custódia seja preservada durante todo o ciclo de vida da evidência e por um período adicional após o término da investigação.

O objetivo principal do registro da cadeia de custódia é permitir a rastreabilidade de acessos e movimentações da evidência digital em qualquer momento. Assim, o registro pode se materializar em mais de um documento, como, por exemplo, um documento que registre a aquisição de dados digitais de determinado dispositivo, além de documentos posteriores que documentem a movimentação desse dispositivo ou a criação de cópias e extratos para análises.

Dessa forma, o projeto ChainGuard se apresenta como uma proposta promissora para estabelecer um modelo nacional para o tratamento de evidências digitais.

A principal vantagem do uso da tecnologia blockchain na gestão da cadeia de custódia está na garantia de disponibilidade e confiabilidade no armazenamento e rastreamento de evidências digitais. Devido à sua natureza descentralizada, a blockchain reduz o risco de falhas em servidores únicos ou de ataques maliciosos concentrados em um único ponto, o que poderia comprometer a integridade das informações em sistemas convencionais de gestão de provas.

Além disso, a utilização da blockchain no projeto permite auditorias contínuas dos registros. Sua transparência e acessibilidade asseguram que todas as operações e alterações sejam facilmente verificáveis. No contexto da cadeia de custódia, isso implica que, uma vez registrado um vestígio digital na blockchain, ele é validado e armazenado de maneira permanente, prevenindo questionamentos futuros sobre sua integridade — um fator essencial em processos criminais, onde a autenticidade das provas é frequentemente contestada.

Outro diferencial importante da solução é o uso de assinaturas digitais e criptografia de dados. Cada ação ou registro relacionado a uma evidência é autenticado com uma assinatura digital exclusiva e protegido por criptografia, garantindo tanto a integridade quanto a privacidade das informações. Essa proteção extra dificulta o acesso não autorizado ou a alteração dos dados, fortalecendo a defesa contra fraudes e vazamentos de informações sensíveis.

A blockchain também oferece flexibilidade para a validação de registros por múltiplas autoridades, conforme políticas de endosso predefinidas. Em vez de centralizar essa função em um único órgão, o sistema permite que diferentes partes possam autenticar e validar os dados, promovendo um ambiente de governança colaborativa e aumentando a confiança entre os envolvidos.

Com a estrutura proposta, é possível manter um registro imutável da cadeia de custódia, contendo informações essenciais como: identificador único da evidência; registros de quem acessou a evidência, o local e o momento do acesso; dados sobre inspeções internas e externas realizadas nas instalações de preservação, os responsáveis e os motivos; além de eventuais alterações necessárias feitas nas evidências digitais, identificando o responsável e a justificativa para tais modificações.

Assim, o ChainGuard surge como uma solução inovadora para suprir a falta de um sistema informatizado que permita o compartilhamento de informações com o órgão central de perícia, viabilizando o mapeamento completo do ciclo de vida dos vestígios — desde a coleta até o descarte. Essa carência foi apontada como uma das maiores fragilidades do sistema de justiça brasileiro no relatório "Diagnóstico e Proposição de Modelo sobre Cadeia de Custódia no Brasil: estudo preliminar em cinco capitais representantes das cinco regiões brasileiras", divulgado pelo Ministério da Justiça e Segurança Pública em 2023.

Por se tratar de uma estrutura distribuída e descentralizada, o uso da tecnologia blockchain favorece a consolidação do Sistema Único de Segurança Pública (SUSP), estabelecido pela Lei no 13.675/2018 [8]. A proposta permite que diversas organizações atuem como nós da rede blockchain, armazenando evidências digitais de maneira colaborativa e consensual, o que facilita a integração entre as instituições por meio da criação de um repositório compartilhado de evidências.

Nesse ambiente comum, cada autoridade teria funções e níveis de acesso específicos, possibilitando que os participantes registrem informações de maneira segura e transparente, enquanto outros validam e consultam os dados em tempo real. Como exemplo prático, é possível idealizar uma rede blockchain que reúna a Polícia Civil, a Polícia Científica e o Ministério Público, atuando de forma integrada.

O desenvolvimento e a aprimoramento do ChainGuard têm o potencial de servir como base para integrar e compartilhar ativos de informação provenientes de diferentes fontes (órgãos), com o objetivo de aumentar a eficácia das investigações e acelerar os processos judiciais. O Ministério Público do Estado do Pará (MP-PA) atuará como fornecedor das informações necessárias para o projeto, fornecendo requisitos e sendo o cliente inicial para os testes da aplicação. No entanto, a problemática mencionada também afeta outros Ministérios Públicos de diferentes estados do Brasil. Por isso, a expansão da ferramenta para essas entidades é uma possibilidade real. Como resultado, dados relacionados a crimes poderiam ser registrados na rede blockchain e posteriormente compartilhados entre os diversos Ministérios Públicos que adotarem a solução.

3.1.2.3 Principais funcionalidades, objetivos específicos e detalhes técnicos do GT-ChainGuard

Com o objetivo desenvolver um sistema de preservação de cadeia de custódia de vestígios digitais, o sistema pode ser dividido em três módulos: aplicação, servidor e blockchain, como mostra a Figura 6.

O módulo de aplicação é composto pelo aplicativo de coleta de vestígios e pela plataforma web. O aplicativo de coleta de vestígios, representado no item 1 da Figura 6, será utilizado pelos peritos durante as investigações. De acordo com os procedimentos operacionais padrões para a coleta de vestígios, o perito, ao utilizar o aplicativo, deverá preencher um formulário com as informações pertinentes à coleta, tirar fotos que comprovem a integridade dos vestígios e registrar os metadados. Além disso, será necessário ler as etiquetas dos lacres dos vestígios coletados e sincronizar as informações com o servidor. O aplicativo permitirá a captura das imagens por meio da câmera do dispositivo, gerando um hash criptográfico para cada imagem e registrando seus metadados.

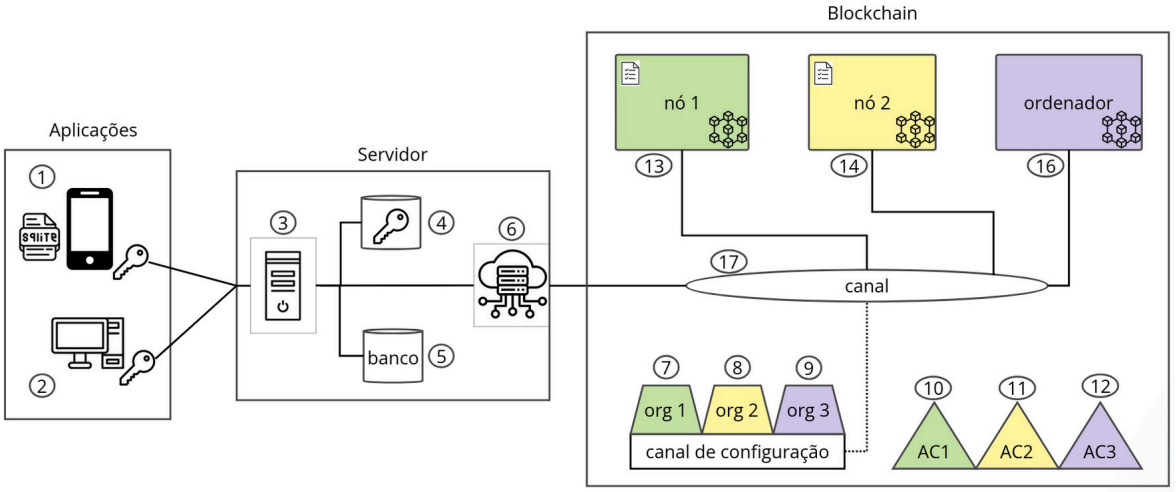

Figura 6 – Arquitetura da solução ChainGuard[6]

A leitura dos lacres será feita por meio de QR codes gerados pela solução proposta permitindo o acesso a um arquivo JSON contendo as informações relacionadas ao lacre. Como o aplicativo de coleta funcionará offline, a sincronização com o servidor será obrigatória. Esse modo offline é essencial porque, conforme apontado pelo Ministério Público do Estado do Pará, muitas coletas de vestígios ocorrem em locais com acesso limitado ou inexistente à internet. Assim, após concluir a missão, o perito deverá sincronizar os dados coletados, vinculando os vestígios a um processo específico e registrando-os na blockchain.

O aplicativo de coleta está sendo desenvolvido utilizando a linguagem Dart e o *framework* Flutter. Para possibilitar o armazenamento local dos vestígios enquanto *offline*, será adotado o banco de dados SQLite. Para garantir a integridade das imagens capturadas pelo aplicativo, será empregado o algoritmo de hash criptográfico SHA3, atualmente o padrão estabelecido pelo Instituto Nacional de Padrões e Tecnologia (NIST).

Em relação à aplicação web que corresponde ao item 2 da Figura 6, também pertencente ao módulo de aplicações, conterá funcionalidades como:

- **Cadastro de processo para cadeia de custódia** - envolve a criação da entidade que será armazenada na blockchain. O processo atuará como a unidade básica dentro da cadeia de custódia. Durante o cadastro, será necessário preencher um formulário com as informações exigidas, conforme as definições estabelecidas por um contrato inteligente;
- **Adição de informações na cadeia de custódia** - permite incluir novos dados sem a necessidade de sincronizar vestígios. Durante a análise pericial de dispositivos eletrônicos, como *smartphones*, é comum que os peritos utilizem softwares forenses para desbloquear os aparelhos e identificar evidências em seus arquivos digitais. Quando novas evidências são encontradas, é necessário registrá-las ou incorporá-las à cadeia de custódia existente. Esse registro

[6] Extraída da proposta apresentada à RNP em resposta aos Editais.

poderá ser realizado por meio da aplicação web, utilizando a funcionalidade específica para adição de informações na cadeia de custódia;

- **Consulta de processos da cadeia de custódia** - possibilita que usuários permissionários acessem as informações registradas. Essa funcionalidade será, possivelmente, a principal via de acesso para usuários externos, como advogados e servidores de outras instituições públicas. Por ser uma função restrita, a consulta exigirá que o usuário possua um cadastro no sistema e as permissões adequadas para visualizar os dados;
- **Gerenciamento de usuários** - permite o cadastro das pessoas que irão utilizar o sistema durante o qual serão solicitadas credenciais para garantir o controle de acesso, permissões e autenticidade. O controle de acesso será feito por meio de login e senha, enquanto que o controle de permissões será administrado por meio de perfis de usuário, como por exemplo, administrador, perito, promotor ou usuário externo. Cada perfil será configurado para definir quais funcionalidades estarão disponíveis para aquele usuário. Quanto à autenticação, ela será feita utilizando a infraestrutura de chaves pública e privada. No módulo de aplicação, as chaves dos itens 1 e 2 representam as chaves privadas que os usuários usarão para garantir a autenticidade. Os usuários responsáveis por criar processos da cadeia de custódia, sincronizar vestígios ou adicionar informações ao processo, deverão usar suas chaves privadas para assinar os dados que serão armazenados na blockchain;
- **Gerenciamento de etiquetas de lacres** - refere-se a um módulo destinado ao registro das informações que serão codificadas em um QR code. Essas informações serão armazenadas em um arquivo no formato JSON, simplificando o trabalho do perito durante a missão. Antes de partir para uma operação, os peritos devem usar essa funcionalidade para criar as etiquetas dos lacres que serão utilizados. Posteriormente, ao utilizar o aplicativo de coleta de vestígios, será possível escanear o QR code dos lacres para leitura das informações; e
- **Visualização de rastreabilidade da cadeia de custódia** - possibilita ao usuário realizar auditorias, verificar a integridade e autenticar todas as informações armazenadas na blockchain. A principal contribuição deste sistema será a simplificação da verificação dessas comprovações, garantindo a validade e confiabilidade da cadeia de custódia.

O segundo módulo da proposta diz respeito ao servidor, como ilustrado na Figura 6. Este módulo é composto por quatro componentes, identificados como itens 3, 4, 5 e 6. O item 3 refere-se ao servidor de aplicação, que será responsável por atender às requisições das aplicações. O back-end desse servidor será desenvolvido utilizando a linguagem de programação Python e o *framework* Django. Como mostrado na Figura 6, o servidor de aplicação irá interagir com o chaveiro de chaves públicas (item 4) para verificar assinaturas, com o banco de dados relacional (item 5) para gerenciar as credenciais dos usuários e com o gateway (item 6) para se comunicar com a blockchain.

O componente responsável pelo chaveiro de chaves públicas (item 4) também será responsável por definir a infraestrutura de chave pública a ser utilizada na solução. Nesse contexto, a assinatura digital será fornecida por meio do algoritmo pós-quântico

Module-Lattice-Based Digital Signature Standard, que é o algoritmo padrão determinado pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos.

O banco de dados descrito no item 5 do módulo do servidor será encarregado de armazenar as credenciais dos usuários que utilizarão o sistema. Para essa finalidade, será utilizado o banco de dados relacional PostgreSQL.

Por fim, o último componente do módulo servidor, identificado como item 6, refere-se ao gateway de comunicação com a blockchain. O gateway é a API responsável por gerenciar os contratos inteligentes. Neste projeto, os contratos inteligentes serão desenvolvidos utilizando a linguagem de programação Java.

O último módulo da solução se refere à blockchain. Conforme ilustrado na Figura 6, será criada uma blockchain composta por três organizações, todas conectadas por um único canal. A organização 3 será encarregada de manter o nó ordenado da rede. Por ser uma rede permissionada, construída sobre o *framework* Hyperledger Fabric, o nó ordenado terá a função de orquestrar a rede, aplicando a política de consenso e assumindo responsabilidades administrativas dentro da rede.

As demais organizações, representadas pelos nós 1 e 2, serão responsáveis por hospedar cópias do livro-razão da blockchain. No Hyperledger Fabric, o livro-razão é dividido em duas partes: a blockchain, onde os dados são persistidos de maneira encadeada, e o estado global, que contém valores atualizados, permitindo que o sistema acesse informações atuais sem a necessidade de percorrer toda a blockchain.

Outro componente essencial da blockchain é o canal, identificado como item 17 na Figura 6, que interconecta os componentes da rede. Dentro do Hyperledger Fabric, cada canal gerencia transações de dados para um livro-razão específico, significando que todos os nós de um mesmo canal compartilham a mesma cópia do livro-razão. Caso seja necessário criar novos livros-razões para nós existentes ou novos nós, um novo canal deverá ser criado para gerenciar as transações.

Ao construir a solução apresentada na Figura 6, será possível gerenciar as informações da cadeia de custódia de evidências digitais, garantindo a integridade e a autenticidade dos dados armazenados. Acredita-se que essa solução é inovadora, pois, no contexto da Segurança Pública, particularmente nos Ministérios Públicos, não há conhecimento de soluções semelhantes sendo utilizadas.

Importante destacar que será utilizado o *framework* Hyperledger Fabric, que é uma das tecnologias disponíveis no *testbed* do Projeto Ilíada e será utilizado para construir a infraestrutura de blockchain. Além de contemplar os requisitos de integridade e imutabilidade, sua adoção deve-se a que, diferentemente de outras soluções de blockchain, esse *framework* possibilita a construção de uma rede permissionada, permitindo que os participantes da rede sejam conhecidos, o que influencia diretamente na política de consenso da rede. Na rede permissionada, políticas de consenso baseada em crash fault-tolerant (CFT) podem ser mais adequadas do que as políticas baseadas em byzantine fault tolerant (BFT).

3.1.3 GT-SWARM - Self-sovereign wi-fi Authentication Roaming

O Self-sovereign wi-fi Authentication Roaming (GT-SWARM) tem como tópico de interesse a "Informação e comunicação", que inclui as telecomunicações, e como principal setor econômico de aplicação o Educacional.

O desenvolvimento desta aplicação está sendo coordenado pela Profa. Carla Merkle Westphall da Universidade Federal de Santa Catarina (UFSC). Formam a equipe de trabalho os colaboradores apresentados na Tabela 9.

Tabela 9 - Equipe de Colaboradores do GT-SWARM

Nome do colaborador	Instituição	URL do currículo Lattes
Profa. Carla Merkle Westphall	UFSC	http://lattes.cnpq.br/1235242182279350
Caciano Machado	UFRGS	http://lattes.cnpq.br/3635721534110256
Eduardo Hoffmann	UFSC	http://lattes.cnpq.br/6419834371011251
Cristian Alves dos Santos	UFSC	http://lattes.cnpq.br/0173844362249968

3.1.3.1 Visão geral do GT-SWARM e sua importância

As redes federadas de roaming possibilitam que usuários acessem a infraestrutura de múltiplos provedores de rede (Access Network Providers – ANP) utilizando uma única credencial emitida por um provedor de identidade (Identity Provider – IDP). Um exemplo notável desse modelo é o Eduroam [9], cuja arquitetura depende de uma hierarquia de servidores Radius operados pelas redes nacionais de ensino e pesquisa (NREN). Inspirado no Eduroam, o OpenRoaming também se destaca, formando um ecossistema que conecta IDPs e ANPs em uma federação com fins comerciais.

Desde a criação do Bitcoin, as tecnologias de blockchain passaram por um período intenso de testes e evolução. Diversas propostas foram desenvolvidas com o intuito de resolver problemas de maneira descentralizada, reduzindo a necessidade de confiança em entidades centralizadas. Atualmente, as potencialidades e limitações dessas tecnologias estão mais bem compreendidas. Nesse cenário, as propostas de identidades auto-soberanas vêm se destacando como uma das inovações mais promissoras.

O objetivo deste projeto é desenvolver o SWARM (Self-sovereign wi-fi Authentication Roaming), um serviço de autenticação com identidades auto-soberanas para roaming wi-fi. Busca integrar essas novas tecnologias de identidade digital descentralizada aos padrões tradicionais de autenticação utilizados em redes wi-fi, como o protocolo 802.1x. Para isso, será necessária uma investigação técnica para adaptar os métodos criptográficos da autenticação atual ao modelo de credenciais verificáveis (VC) e identificadores descentralizados (DID).
Inicialmente, o projeto foca na integração com a rede Eduroam no ambiente do Projeto Ilíada, utilizando o *testbed* da instituição para a prototipação. Posteriormente, a solução

poderá ser expandida para toda a federação Eduroam e também para outras federações, como o OpenRoaming.

O desenvolvimento do SWARM traz benefícios significativos para o ecossistema, sendo o mais evidente o de proporcionar aos usuários dos recursos do Projeto Ilíada a utilização de identidades digitais descentralizadas para acesso aos seus serviços. Deverá permitir uma forma descentralizada de autenticação dos usuários em redes *wi-fi*, independente dos servidores de *proxy* centralizados da federação do Eduroam. Adicionalmente, essa integração deve eliminar diversos pontos de falha tornando o processo de autenticação do Eduroam muito mais confiável. Melhora a privacidade dos usuários, já que, durante a autenticação, as credenciais não precisam ser transmitidas para fora do ANP.

3.1.3.2 Descrição detalhada do GT-SWARM

A criação do protocolo Wi-fi Protected Access (WPA) possibilitou o uso de arquiteturas de Autenticação, Autorização e Contabilização (AAA) em redes wi-fi, por meio do padrão de autenticação IEEE 802.1x. Com esse padrão, os pontos de acesso deixaram de depender de senhas compartilhadas (Pre-Shared Key – PSK), passando a encaminhar as autenticações dos usuários de forma segura para servidores centralizados (geralmente Radius), que acessam uma base de dados com as credenciais.

Como um desdobramento natural dessa arquitetura, surgiram as federações Radius, como o Eduroam e o OpenRoaming. Essas federações integram provedores de identidade (Identity Providers – IDPs) com provedores de acesso à rede (Access Network Providers – ANPs), por meio de uma estrutura hierárquica de servidores *proxy* Radius. Essa estrutura permite encaminhar as solicitações de autenticação dos usuários, possibilitando o acesso às redes de qualquer ANP pertencente à federação, utilizando as credenciais fornecidas pelo seu IDP de origem.

Para ilustrar esse tipo de funcionamento, a Figura 7 apresenta um exemplo com a federação Eduroam. Nele, um usuário da UFSC (que atua como IDP) visita a UFRGS (que funciona como ANP) e tenta acessar a rede usando suas credenciais da UFSC. O ponto de acesso wi-fi na UFRGS envia a solicitação de autenticação ao seu servidor Radius local. Como o usuário não pertence à UFRGS, esse servidor repassa a solicitação ao *proxy* Radius da RNP, que por sua vez a encaminha ao servidor Radius da UFSC, onde a autenticação do usuário é finalmente validada.

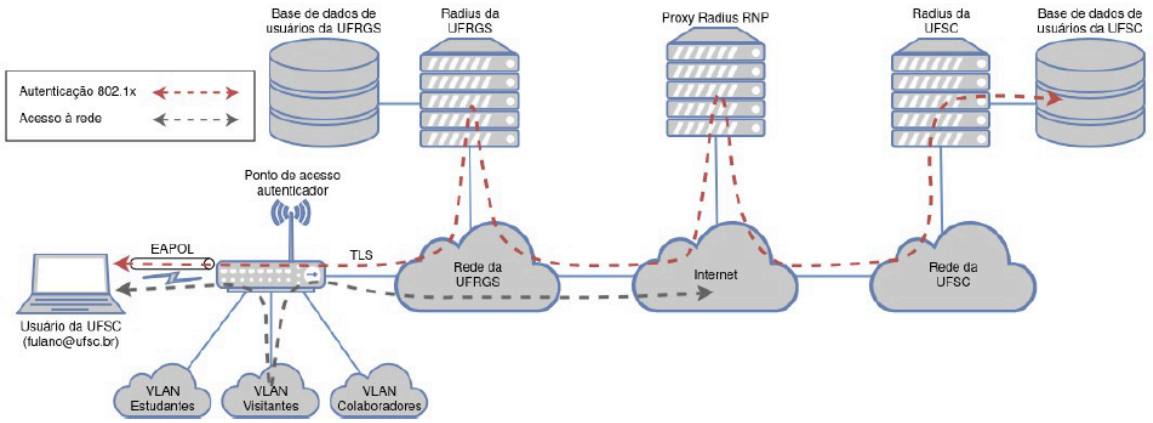

Figura 7 - Arquitetura do Eduroam na RNP[7]

As identidades auto-soberanas (SSI – Self-Sovereign Identity) têm ganhado destaque como uma abordagem promissora nas pesquisas sobre sistemas descentralizados baseados em blockchain. Essas soluções oferecem a indivíduos, organizações e dispositivos a capacidade de gerenciar integralmente suas identidades digitais, controlando o compartilhamento de informações com segurança e privacidade, sem a necessidade de intermediários ou autoridades centralizadas.

Uma identidade digital baseada no modelo SSI pode incluir declarações certificadas por emissores, como nome, idade, gênero, diploma, habilitação, entre outros dados do titular. Esse modelo é fundamentado em duas tecnologias principais: os identificadores descentralizados (DID – Decentralized Identifier) e as credenciais verificáveis (VC – Verifiable Credentials).

Os DIDs são identificadores únicos que permitem referenciar entidades de forma precisa. Diferentemente dos esquemas de identificação federada, os DIDs foram projetados para operar de maneira independente de bancos de dados centralizados, provedores de identidade ou autoridades certificadoras. Cada DID está associado a documentos DID, armazenados em um registro verificável (blockchain), contendo informações como chaves públicas. Esses dados possibilitam que a entidade comprove sua identidade e o vínculo com o DID por meio de criptografia assimétrica, utilizando suas chaves privadas.

Como ilustrado na Figura 8, uma VC contém declarações associadas a um titular (*holder*) e é emitida por uma entidade emissora (*issuer*). Tanto o proprietário quanto o emissor possuem seus próprios identificadores descentralizados (DIDs). A credencial é armazenada pelo titular em sua carteira digital (data wallet).

Essas VCs podem ser validadas por meio de assinaturas digitais, utilizando criptografia assimétrica. Um exemplo prático seria uma universidade (*issuer*) que emite um crachá digital (VC) para um estudante (*holder*), permitindo o acesso a serviços como restaurante universitário, rede wi-fi, biblioteca e setores administrativos. Quando

[7] Extraída da proposta apresentada à RNP em resposta aos Editais.

necessário, o estudante apresenta essa credencial digital a um agente verificador (*verifier*), que confere sua autenticidade.

Para realizar essa verificação, o agente recupera a chave pública do emissor diretamente de um registro de dados verificável, como uma blockchain. Além disso, o titular da credencial pode escolher quais informações serão compartilhadas com o verificador, conforme o tipo de serviço solicitado, garantindo maior controle sobre sua privacidade.

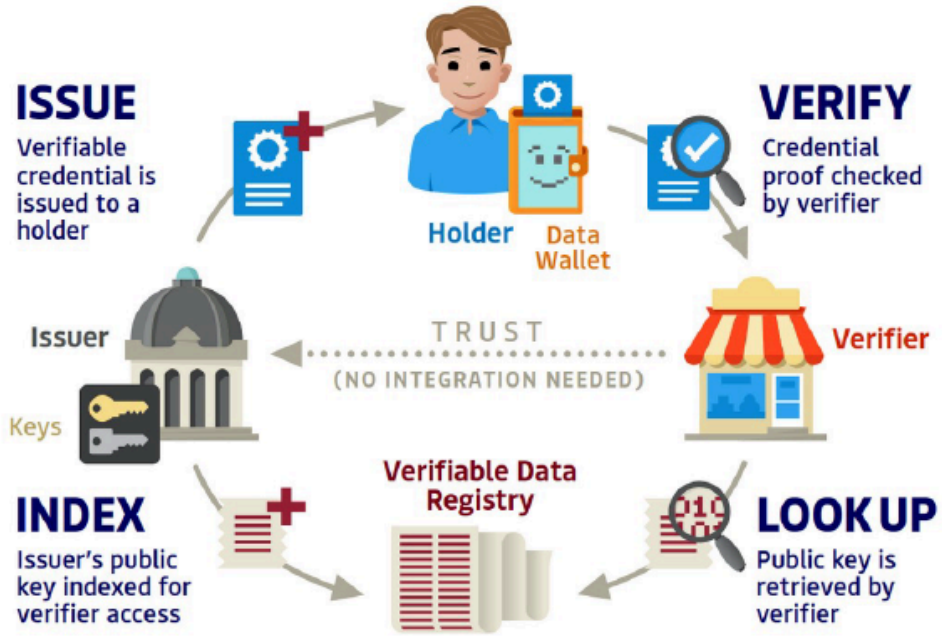

Figura 8 - Funcionamento de DID/VC[8]

Diversos estudos investigam o uso de identificadores descentralizados (DID) e credenciais verificáveis (VC) para autenticação em redes wi-fi. Propostas como Trustroam [10], Roam [11] e os trabalhos de Ahmed e Hussain [12] [13] utilizam tecnologias como smart contracts, Sovrin [14] e Hyperledger Indy [15] mas geralmente requerem access points com firmware específico e, em alguns casos, hardware com TPM. Para garantir compatibilidade com a infraestrutura wi-fi existente, é necessário considerar os padrões atuais, como o IEEE 802.1x e os métodos EAP suportados por dispositivos e servidores Radius.

O problema a ser resolvido com a concepção do SWARM é possibilitar que usuários de SSI possam se autenticar em redes wi-fi federadas nos ANPs, com base nas permissões concedidas pelas autoridades dos IDPs participantes. A proposta consiste em investigar como adaptar o modelo DID/VC aos mecanismos criptográficos utilizados na autenticação IEEE 802.1x, levando em conta também as vulnerabilidades de segurança associadas a esse padrão [16].

[8] Fonte: https://trustoverip.org/

3.1.3.3 Principais funcionalidades, objetivos específicos e detalhes técnicos do GT-SWARM

A entrega prevista para esta proposta é a integração do SWARM a um ambiente de testes (*testbed*) do Eduroam, mantido pela RNP. Futuramente, em fases posteriores do grupo de trabalho, essa integração poderá ser expandida para toda a federação Eduroam e também para o OpenRoaming. A validação dessa integração será realizada por meio da instrumentação de servidores Radius, permitindo a autenticação de usuários através de DID/VC, utilizando a blockchain Hyperledger. A Figura 9 ilustra o processo de autenticação de um usuário em uma instituição integrada ao SWARM.

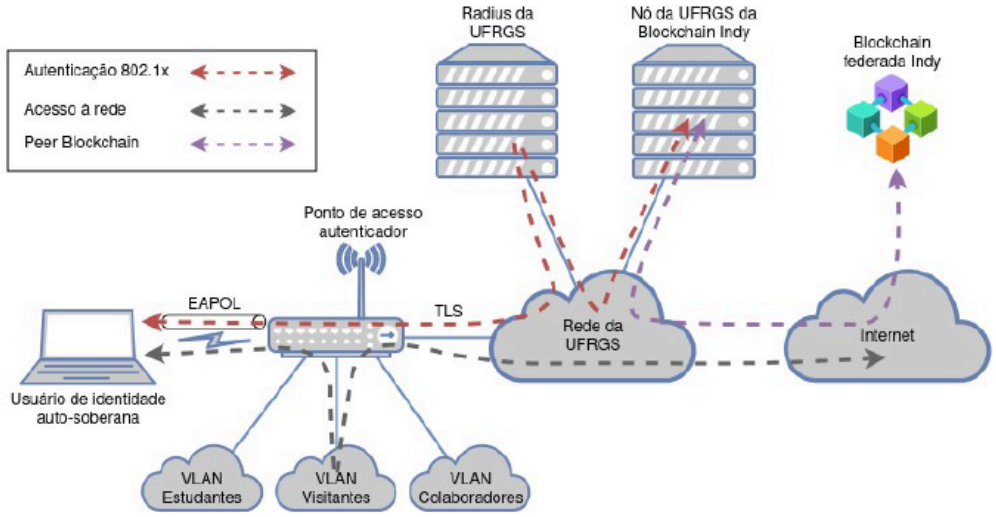

Figura 9 - Autenticação de identidades descentralizadas no Eduroam[9]

A proposta está organizada em duas frentes principais, com o objetivo de validar um mecanismo baseado em DID/VC para autenticação em redes 802.1x com WPA2/3 Enterprise, aplicável à federação Eduroam.

A primeira frente, que representa o núcleo do projeto, foca na pesquisa e desenvolvimento de um método EAP compatível com autenticação baseada em DID/VC. Essa linha já conta com estudos preliminares conduzidos pelo Laboratório de Redes e Gerência da UFSC. A segunda frente envolve a criação de uma plataforma de gerenciamento de DID/VCs, permitindo que instituições — como a RNP — concedam permissões para que identidades auto-soberanas possam autenticar-se dentro da federação Eduroam.

Na primeira frente, o trabalho prevê a instrumentação de softwares de código aberto, como o FreeRADIUS, com o uso de ferramentas como radiusclient e epol_test. A ideia é modificar métodos EAP existentes, como ilustrado na Figura 10, ou desenvolver novos, viabilizando a autenticação 802.1x com segurança usando DID/VC. Essas ferramentas permitem simular o processo de autenticação de usuários em redes wi-fi 802.1x sem a necessidade de implantar toda a infraestrutura de rede sem fio. Para isso, será necessário desenvolver novos módulos ou utilizar os módulos de script existentes (em

[9] Extraída da proposta apresentada à RNP em resposta aos Editais.

Python ou Perl) para integrar o FreeRADIUS com o sistema de autenticação baseado em DID/VC.

Figura 10 - Métodos de autenticação EAP[10]

O projeto Roam propõe duas abordagens para adaptar os métodos EAP-TTLS e EAP-TEAP para utilização de DID/VC. No EAP-TTLS, a VP é incorporada em um campo opcional do MS-CHAP-V2, o que representa uma limitação. Já no EAP-TEAP, a inclusão ocorre em um campo obrigatório (TLV Basic Password-Auth-Req), tornando a estratégia mais robusta. A viabilidade dessas soluções será analisada na primeira frente de desenvolvimento do projeto, podendo orientar a futura integração da autenticação wi-fi com DID/VC.

A segunda frente do projeto consiste na criação de um Produto Mínimo Viável (Minimum Viable Product - MVP) que permita demonstrar o funcionamento de um ecossistema de gerenciamento de permissões de acesso aos DIDs na rede Eduroam, seguindo um processo semelhante ao ilustrado na Figura 11. Essa demonstração será realizada na rede de testes do Eduroam, utilizando servidores FreeRADIUS configurados com os resultados obtidos na primeira frente. A integração deverá possibilitar que os servidores Radius verifiquem, de forma segura, as apresentações verificáveis (VPs) geradas pelos clientes wi-fi por meio da blockchain.

Serão utilizadas ferramentas de desenvolvimento e prototipação para contratos inteligentes como Truffle/Ganache e Remix, *frameworks* e linguagens de programação como Node.js e Solidity, além dos *testbeds* das redes Hyperledger Fabric, Indy e Besu disponibilizados pela RNP.

[10] Fonte: https://www.ciscozine.com/

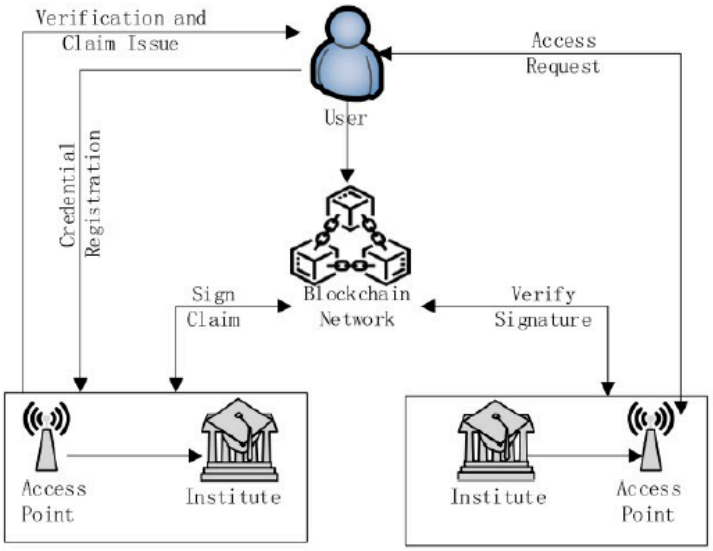

Figura 11 - Processo de autenticação WiFi com DID/VC[11]

3.1.4 GT-Smart AgroRAF - Smart Contracts para Rastreamento da Agricultura Familiar

O Smart Contracts para Rastreamento da Agricultura Familiar (GT-Smart AgroRAF) tem como tópicos de interesse a tokenização de ativos, rastreabilidade de procedência e de cadeias e como principal setor econômico de aplicação o Agropecuário.

O desenvolvimento desta aplicação está sendo coordenado pelo Prof. Rodrigo Brandão Mansilha da Universidade Federal do Pampa (UNIPAMPA). Formam a equipe de trabalho os colaboradores apresentados na Tabela 10.

Tabela 10 - Equipe de Colaboradores do GT-Smart AgroRAF

Nome do colaborador	Instituição	URL do currículo Lattes
Prof. Rodrigo Brandão Mansilha	UNIPAMPA	http://lattes.cnpq.br/3118442101667444
Prof. Diego Kreutz	UNIPAMPA	http://lattes.cnpq.br/2781747995973774
Prof. Roben Castagna Lunardi	IFRS	http://lattes.cnpq.br/1243090119249735
Prof. Ewerton Rodrigues Andrade	UNIR / SIDIA Samsung	http://lattes.cnpq.br/9038113331816861
Prof. Nykolas Fornaziero dos Santos	UNIFAE/ UNIPAMPA	http://lattes.cnpq.br/3308709051169260

Além da equipe de colaboradores, o projeto contará com o apoio de consultores *ad-hoc*.

[11] Fonte: Referência [13] deste relatório.

3.1.4.1 Visão geral do GT-Smart AgroRAF e sua importância

Atualmente, há mais de 608 milhões de propriedades rurais no mundo, das quais aproximadamente 90% são fazendas familiares, responsáveis por cerca de 80% da produção global de alimentos. Já no Brasil, a agricultura familiar representa 77% dos estabelecimentos rurais e é a base econômica de 90% dos municípios com população de até 20 mil habitantes [17].

A Instrução Normativa Conjunta nº 02/2018 [18] estabelece regras para rastrear vegetais frescos no Brasil, afetando políticas como a que destina 30% dos recursos da merenda escolar à agricultura familiar. No entanto, o alto custo ainda é um obstáculo para a adoção da rastreabilidade por pequenos produtores.

O Programa de Rastreabilidade da Agricultura Familiar (Proraf) é uma resposta inovadora aos desafios enfrentados pela agricultura familiar brasileira na implementação da rastreabilidade [19]. Atualmente o Proraf atende experimentalmente famílias, oferecendo aplicativos aos produtores e consumidores com dados armazenados de maneira centralizada.

Este projeto prevê o uso de blockchain para tornar o livro razão da rastreabilidade da produção agrícola familiar acessível a várias entidades, garantindo transparência, imutabilidade e segurança dos dados. Isso fortalece a confiança e o valor na cadeia produtiva, além de apoiar a execução de políticas públicas. Embora já existam estudos focados em culturas como cacau e cana-de-açúcar, este projeto se diferencia ao aplicar essa tecnologia à agricultura familiar, em conformidade com a INC 02/2018.

O objetivo geral é então desenvolver uma solução de rastreamento de produtos da agricultura familiar baseada em blockchains e *tokens* em acordo com a INC 02/2018 para o Proraf, em que são delineados três objetivos específicos:

1. **Projeto de contratos inteligentes para o Proraf** - Projetar os contratos inteligentes considerando as necessidades de tokenização e rastreabilidade;
2. **Implementação de contratos inteligentes no Proraf** - Acoplar o sistema de informação do Proraf à blockchain, envolvendo atividades de análise, projeto, implementação e testes de interface de usuário conectadas ao Hyperledger Besu disponibilizado na infraestrutura desenvolvida no contexto do Projeto Ilíada;
3. **Teste de blockchains para os contratos inteligentes do Proraf** - Será realizada uma avaliação sistemática das blockchains Hyperledger Besu e Ethereum, considerando custo, tempo de inserção, taxa de transações por segundo (TPS) e usabilidade. Os resultados servirão de base técnica e econômica para analisar a viabilidade e escalabilidade da solução, subsidiando um estudo para um futuro MVP.

Em resumo, este projeto propõe uma solução baseada em blockchain para garantir a rastreabilidade da cadeia produtiva da agricultura familiar no contexto do Proraf. A expectativa é que, futuramente, essa solução possa ser adaptada e aplicada a outras

iniciativas similares ou a ecossistemas diferentes, como comunidades de pescadores e ribeirinhos, por exemplo.

A crescente exigência por produtos com rastreabilidade está em consonância com a INC 02/2018, que estabelece os procedimentos para rastrear vegetais frescos destinados à alimentação humana. Além disso, a busca por certificações de qualidade se alinha ao programa Produtos Premium, do Governo do Estado do Rio Grande do Sul, instituído pelo Decreto nº 55.515, de 30 de setembro de 2020 [20], que incentiva a agregação de valor aos produtos locais.

O projeto também está em harmonia com o planejamento estratégico das regiões da Fronteira Oeste e da Campanha do RS, além de contribuir com os Objetivos de Desenvolvimento Sustentável da Agenda 2030.

Sua importância reside em sua capacidade de promover a rastreabilidade, transparência, e sustentabilidade na agricultura familiar, ao mesmo tempo em que contribui para a economia local, facilita a agregação de valor aos produtos e está alinhado com as políticas públicas e os Objetivos de Desenvolvimento Sustentável.

3.1.4.2 Descrição detalhada do GT-Smart AgroRAF

Para persistir o rastreamento da cadeia produtiva atendendo os requisitos não funcionais avançados, propôs-se a elaboração de uma solução baseada em blockchain, como mostra a Figura 12.

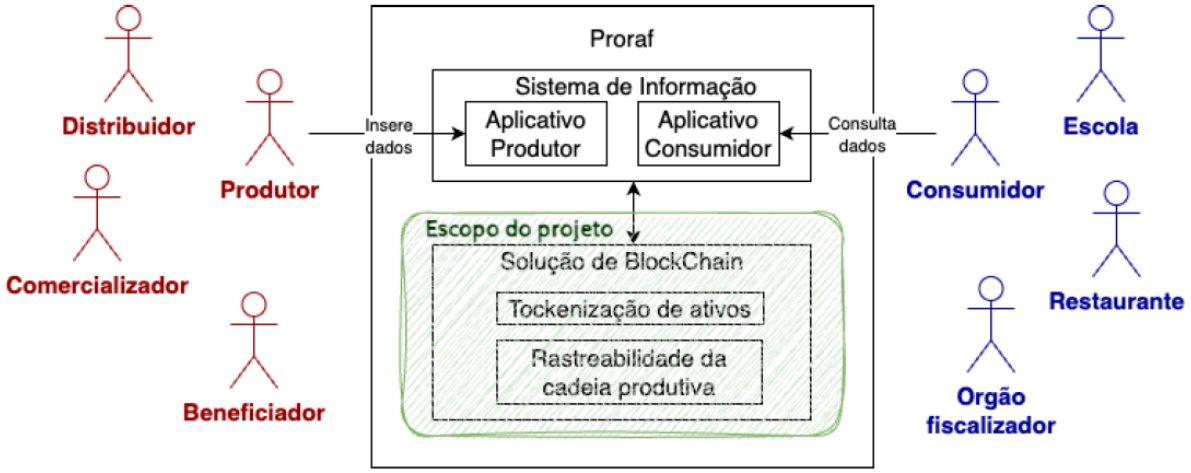

Figura 12 - Escopo da solução proposta e sua integração com o Ecossistema Proraf[12]

Quando o produtor cadastrar um novo lote de produção, o Sistema de Informação (SI) criará uma entrada de tokenização de ativos na blockchain. Quando o produtor criar uma movimentação no aplicativo, será adicionada uma entrada na cadeia produtiva rastreável. Os consumidores (e suas variantes), por sua vez, poderão consultar dados através do SI.

Além da INC 02/2018 obrigar o rastreamento da cadeia de produção de vegetais, há uma motivação econômica que é participar em programas governamentais, como

[12] Extraída da proposta apresentada à RNP em resposta aos Editais.

Programa Nacional de Alimentação Escolar (PNAE). Porém, a rastreabilidade da agricultura familiar apresenta diversos desafios relacionados a custos e conformidade legal.

O Proraf busca enfrentar os desafios impostos pela INC 02/2018 por meio da oferta de serviços tecnológicos escaláveis e acessíveis, voltados à agricultura familiar. Esses serviços visam agregar valor à produção e reduzir custos operacionais, ao mesmo tempo em que atendem às exigências da normativa.

O sistema central do Proraf é um Sistema de Informação (SI), composto por dois aplicativos principais: um voltado para os produtores (aplicativo Produtor) e outro para os consumidores (aplicativo Consumidor).

Atualmente, os dados do SI são armazenados em um Sistema Gerenciador de Banco de Dados (SGBD) tradicional, como o MySQL. No entanto, essa abordagem apresenta algumas limitações importantes: falta de transparência (as movimentações não podem ser auditadas de forma independente), centralização excessiva (o controle dos dados está concentrado nos gestores do Proraf) e baixa resiliência (caso o sistema seja desativado, o histórico de dados pode ser perdido).

Em resumo, embora a solução atual atenda aos requisitos de desempenho e usabilidade por meio de uma abordagem centralizada, a implementação de blockchain com contratos inteligentes descentralizados pode agregar funcionalidades adicionais avançadas, como: (i) transparência e auditabilidade, (ii) escalabilidade autoritativa e (iii) resiliência.

Para que o Proraf aproveite os benefícios da tecnologia blockchain, é necessário um planejamento cuidadoso que equilibre desafios como escalabilidade, consumo de recursos, latência e taxa de transações, além de privacidade, confiança e custos financeiros. Esse processo envolve decisões sobre a plataforma a ser utilizada (como Ethereum ou Hyperledger), validação de blocos (completo ou parcial), imutabilidade (blocos editáveis ou não), mecanismos de consenso (como Proof of Work ou Proof of Stake), hierarquia (cadeia única ou múltipla) e tipo de acesso (público ou privado). Além disso, será necessário avaliar o custo e o desempenho das transações, especialmente em sistemas que registram dados além da simples troca de *tokens*. Todas essas decisões devem ser tomadas com base nos requisitos funcionais do sistema.

3.1.4.3 Principais funcionalidades, objetivos específicos e detalhes técnicos do GT-Smart AgroRAF

Neste projeto, consideram-se os seguintes requisitos:

1. **Inserção de tokens dos ativos gerados pelo produtor**. Antes de um produto ser movimentado, como no caso de uma venda, ele precisa ser vinculado a um lote de produção e associado a um conjunto de informações, junto com um *token* único. A partir desse *token* original do lote, podem ser criados *tokens* derivados para identificar individualmente os itens pertencentes a esse lote.

2. **Revogação de *tokens***. Em caso de erro ou quando um produto/lote deixa de existir, deve haver uma funcionalidade para revogar o token correspondente.
3. **Transferência de *tokens***. Lotes podem ser movimentados entre entidades gerando uma cadeia de rastreabilidade. Para isso, é necessário que as informações de transação sejam registradas para rastreamento.
4. **Consulta de movimentação de *tokens***. Lotes e produtos podem ser rastreados e identificados por meio dos *tokens* associados e dos registros de suas transferências. Todas as informações relacionadas aos produtos, aos lotes e às suas movimentações devem estar disponíveis publicamente;
5. **Padronização**. Os ativos tokenizados devem estar em conformidade com os padrões exigidos pela legislação atual, incluindo os campos obrigatórios estabelecidos pela INC 02/2018, como demonstrado na Figura 13. Os *tokens* seguirão, inicialmente, o padrão ERC-20, mas também será considerada a adoção de outros padrões, como o ERC-1400, para assegurar uma implementação segura dos contratos inteligentes, especialmente devido à forte ligação desses ativos com elementos do mundo físico.

1 – Informações do Produto Vegetal	
1.1- Nome do produto vegetal	1.2- Variedade ou cultivar
1.3- Quantidade do produto expedido	1.4- Identificação do lote
1.5- Data da expedição do P.V	
2 – Informações do Comprador	
2.1- Nome ou Razão Social	2.2 – CPF, I.E ou CNPJ ou CGC/MAPA
2.3- Endereço completo, ou quando localizado em zona rural, coordenada geográfica ou CCIR	

1 – Informações do Produto Vegetal	
1.1- Nome do produto vegetal	1.2- Variedade ou cultivar
1.3- Quantidade do produto recebido	1.4- Identificação do lote
1.5- Data do recebimento do P.V	
2 – Informações do Fornecedor	
2.1- Nome ou Razão Social	2.2 – CPF, I.E ou CNPJ ou CGC/MAPA
2.3- Endereço completo, ou quando localizado em zona rural, coordenada geográfica ou CCIR	

Figura 13 - Dados que precisam ser registrados conforme INC 02/2018[13]

Para atender aos requisitos mencionados anteriormente, propõe-se a arquitetura de software ilustrada na Figura 14. Os elementos em azul representam os principais papéis e componentes do Sistema de Informação (SI), que já estão implementados como produtos funcionais, em operação pública com produtores beta selecionados e acesso livre para consumidores. Os elementos destacados em vermelho correspondem aos componentes baseados em blockchain que ainda precisam ser desenvolvidos durante a execução do projeto.

Está prevista a adaptação de componentes já existentes, especialmente os aplicativos voltados para Produtor e Consumidor, com o objetivo de permitir uma visualização simples e intuitiva do histórico e do status das transações na blockchain. Também será criada uma nova API Blockchain, responsável por validar e garantir a autenticidade e a origem dos dados trocados entre produtores e consumidores. Essa API também gerenciará a execução dos contratos inteligentes, de forma independente da interface do usuário. Além disso, a API será encarregada do processo de tokenização de ativos — como lotes e produtos —, que funcionarão como pontos de referência para o rastreamento das movimentações na cadeia produtiva entre diferentes participantes.

[13] Extraída da proposta apresentada à RNP em resposta aos Editais.

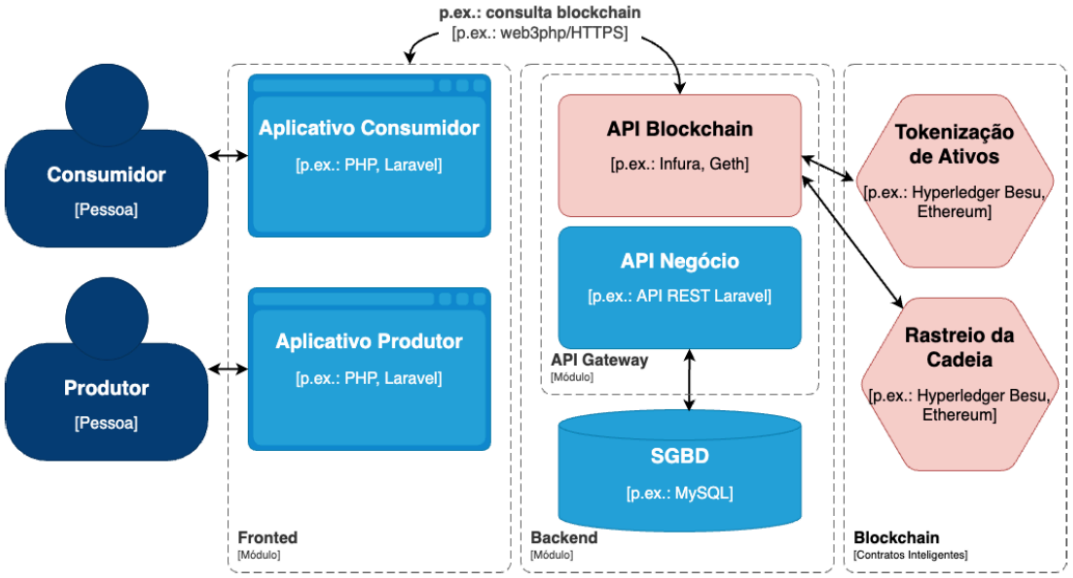

Figura 14 - Arquitetura proposta: componentes existentes (azul) e projetados (vermelho)[14]

A blockchain do Proraf será desenvolvida e testada utilizando a infraestrutura tecnológica do *testbed* disponibilizado pelo Projeto Ilíada, com foco específico na Modalidade 2: Redes de Curto Prazo. Considerando o prazo limitado de execução do projeto (9 meses), o objetivo é entregar uma solução em nível de Prova de Conceito (PoC), acompanhada de resultados de avaliação que, futuramente, poderão servir de base para a proposta e desenvolvimento de um Produto Mínimo Viável (MVP).

Do ponto de vista tecnológico, a rede Hyperledger Besu será adotada como base, em conjunto com ao menos três componentes da plataforma de experimentação do Projeto Ilíada. Primeiramente, será utilizado o Block Explorer para permitir a visualização transparente de transações e blocos, facilitando auditorias e o acompanhamento das atividades registradas na blockchain. Em segundo lugar, serão empregados recursos de monitoramento e logs centralizados para garantir o acompanhamento contínuo do desempenho, a rastreabilidade de eventos e a identificação rápida de falhas, promovendo maior segurança e confiabilidade. O terceiro componente será o repositório de containers, que permitirá o versionamento e armazenamento de imagens, facilitando a implantação e atualização de serviços em ambientes de produção.

Para aprimorar a experiência do usuário final, será adotada uma carteira digital para envio de transações da aplicação à blockchain. A ferramenta escolhida é a Metamask, devido à sua versatilidade — compatível com diferentes redes públicas e privadas — e à ampla adoção em múltiplas plataformas.

Em conformidade com as diretrizes do Projeto Ilíada, será priorizada a utilização de uma pilha tecnológica baseada em software livre e de código aberto, com apoio de comunidades ativas e consolidadas. As aplicações serão executadas em containers Docker gerenciados por Kubernetes.

[14] Extraída da proposta apresentada à RNP em resposta aos Editais.

3.2 Projetos de *startups*

Os projetos de *startups* selecionados são os seguintes:

- DAIESEB - Digitalização do Acervo Acadêmico de Instituições de Ensino Superior com base em Inteligência Artificial e Blockchain
- Levery: Plataforma de Carteira Digital e Negociação de Ativos Tokenizados
- Modelagem de Aplicações Piloto Baseadas em NFTs de Ciclo Preditivo Utilizando a Plataforma Ledger NFT
- Rastreabilidade Química Inteligente: Agricultura na Era da Blockchain

Na sequência, detalha-se cada um deles.

3.2.1 DAIESEB - Digitalização do Acervo Acadêmico de Instituições de Ensino Superior com base em Inteligência Artificial e Blockchain

O projeto Digitalização do Acervo Acadêmico de Instituições de Ensino Superior com base em Inteligência Artificial e Blockchain (DAIESEB) tem como tópico de interesse a "Automatização de processos" e como principal setor econômico de aplicação o Educacional.

O desenvolvimento desta aplicação está sendo realizado pela Certisecure Serviços Digitais Ltda., *startup* fundada por Rafael Escrich e sediada em Florianópolis/SC. Formam a equipe de trabalho os colaboradores apresentados na Tabela 11.

Tabela 11 - Equipe de Colaboradores do DAIESEB

Nome do colaborador	Instituição	URL do currículo Lattes ou LinkedIn
Prof. Jean Everson Martina	UFSC	http://lattes.cnpq.br/3531795815749652
Lucas Palma	UFSC	https://www.linkedin.com/in/lucasmpalma/
Kamila Estevam	Dati Tecnologia	https://www.linkedin.com/in/kamila-estevam-%F0%9F%8F%B3%EF%B8%8F%E2%80%8D%F0%9F%8C%88-mba-csm-cspo-a7bb1a31/
Rafael Escrich	Certisecure	https://www.linkedin.com/in/rafaelescrich/

3.2.1.1 Visão geral do DAIESEB e sua importância

O projeto Diploma Digital [21], uma iniciativa do Ministério da Educação (MEC) e do Governo Federal, foi criado com o objetivo de modernizar a documentação acadêmica e combater fraudes na emissão e no registro de diplomas de conclusão de cursos de graduação. No âmbito desse projeto, o MEC define um padrão para a emissão de documentos nativos digitais, utilizando arquivos XML assinados digitalmente. Esse formato assegura características essenciais como autenticidade e integridade dos dados.

Os XMLs que precisam ser emitidos pelas Instituições de Ensino Superior (IES) seguem um padrão definido pelo Ministério da Educação (MEC), com base em um conjunto de esquemas XSD e cuja versão vigente na elaboração da proposta era a 1.05. Além disso, os documentos emitidos pelas IES devem obrigatoriamente conter assinaturas digitais das partes envolvidas no processo, como, por exemplo, a assinatura do reitor no caso da emissão de um diploma de conclusão de curso.

Neste cenário, embora o projeto do Diploma Digital represente um avanço significativo na modernização da documentação acadêmica de nível superior e na prevenção de fraudes, ele não abrange, por padrão, todas as etapas do processo de graduação que também são fundamentais. Especificamente, o Diploma Digital, em sua concepção atual, não assegura a autenticidade e integridade das fases anteriores à emissão e registro do diploma de conclusão de curso. Em outras palavras, a partir do XML do diploma digital, não é possível verificar se a trajetória acadêmica do estudante ocorreu conforme os trâmites e prazos esperados.

Com o intuito de resolver essa e outras lacunas na gestão de dados educacionais no Brasil, o MEC, em parceria com a Universidade Federal de Santa Catarina (UFSC), propôs o projeto Jornada do Estudante (JE) [22]. No âmbito da JE, dois laboratórios da UFSC — o Laboratório de Segurança em Computação (LabSEC) e o Laboratório Bridge — estão envolvidos no desenvolvimento de soluções tecnológicas que conectam os estudantes ao registro de sua trajetória acadêmica.

No LabSEC, está sendo desenvolvida uma rede distribuída e descentralizada baseada em tecnologia blockchain, por meio da qual as IES participantes poderão compartilhar, entre si e com o MEC, informações sobre as jornadas acadêmicas de seus estudantes [3][4]. O padrão de dados adotado pela rede segue o modelo de interoperabilidade definido pelo Diploma Digital, e permite que as IES atuem como auditoras umas das outras. A expectativa é que essa rede blockchain evolua, futuramente, para um grande barramento de dados em tempo real sobre o ensino superior brasileiro.

A solução desenvolvida no âmbito do projeto JE, aliada aos padrões definidos pelo Diploma Digital, permite auditar toda a trajetória acadêmica do estudante — desde sua matrícula na IES até a emissão do diploma. No entanto, algumas lacunas ainda persistem. Este projeto, em particular, foca no Acervo Acadêmico: o conjunto de documentos físicos, em papel, mantidos pelas IES e emitidos antes da implementação dos processos de modernização aqui apresentados.

Sua importância reside no fato de que a solução oferece uma modernização robusta, reduzindo custos operacionais e melhorando a integridade e acessibilidade dos acervos acadêmicos. Combinando Inteligência Artificial (IA) e blockchain, ela fornece uma solução auditável e alinhada às diretrizes do MEC, garantindo que as IES tenham ferramentas para operar com maior eficiência e transparência.

Os clientes em potencial do projeto aqui proposto são as IES brasileiras, tanto públicas quanto privadas. Segundo o censo da educação superior de 2023 [23], realizado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira, existem,

atualmente, 2580 IES em território nacional, das quais 316 são públicas e 2264 são privadas. Além disso, o modelo apresentado pode ser estendido, no futuro, para outras camadas do setor educacional, como os ensinos médio e básico.

3.2.1.2 Descrição detalhada do DAIESEB

O acervo acadêmico em formato físico, mantido pelas IES, representa um desafio persistente no contexto das iniciativas de digitalização dos processos educacionais. Esses documentos são difíceis de armazenar e gerenciar, além de não estarem integrados aos dados mais recentes gerados pelas instituições. Contudo, devido à sua natureza de guarda a longo prazo, e em alguns casos, permanente, eles devem ser preservados pelas IES em seus depósitos de acervo. Por serem documentos físicos, estão sujeitos a intempéries e, mesmo as cópias que poderiam oferecer redundância e segurança, estão sujeitas a riscos de extravio e degradação.

Diante desse cenário, acredita-se que a digitalização desse acervo facilitará a integração de dados históricos, gerados antes das políticas de digitalização dos processos acadêmicos, com aqueles produzidos de acordo com as diretrizes mais recentes, como as propostas do Diploma Digital e da Jornada do Estudante. Essa integração permitirá uma visão mais abrangente e precisa da trajetória de cada IES, além de proporcionar ao MEC uma perspectiva mais ampla do ensino superior no país. Adicionalmente, os desafios e custos associados à manutenção de um acervo físico serão substituídos por processos mais baratos, confiáveis e alinhados com as necessidades do século XXI.

Propõe-se então o desenvolvimento de um fluxo automatizado para a digitalização do acervo acadêmico das IES. Esse fluxo utilizará tecnologias de ponta para implementar um sistema auditável, capaz de receber como entrada (*input*) o acervo físico da IES e gerar como saída (*output*) documentos digitais estruturados, prontos para integração com os projetos do Diploma Digital e da Jornada do Estudante. A solução seguirá as diretrizes estabelecidas pelo MEC, garantindo maior aderência às exigências do mercado. Considerando que as IES possuem autonomia na organização de seus acervos físicos, prevê-se como um primeiro desafio a conversão inicial dos documentos em papel para uma primeira versão digital intermediária.

Em outras palavras, serão definidos os mecanismos pelos quais os documentos físicos deverão ser convertidos para formatos digitais, como arquivos PDF. Já nessa etapa inicial, prevê-se uma série de desafios — especialmente no que diz respeito à classificação documental. Cada folha de papel poderá conter um único documento ou, em alguns casos, múltiplos documentos. Além disso, é possível que grande parte do acervo físico inclua fotocópias de documentos originais, como carteiras de identidade e certidões de nascimento.

A realização manual da classificação desses documentos digitalizados tornaria o processo moroso e dispendioso. Por essa razão, propõe-se o desenvolvimento de um mecanismo automatizado de identificação, extração de dados e classificação, com base em técnicas de visão computacional e inteligência artificial. O resultado esperado dessa etapa será um conjunto de documentos digitais intermediários, os quais serão

posteriormente enriquecidos com metadados extraídos dos documentos físicos originais.

Em uma segunda fase, os documentos digitais intermediários serão convertidos para o formato XML, seguindo o modelo de interoperabilidade definido pelo Diploma Digital. Os XMLs gerados serão, então, preparados para inserção em uma blockchain privada e permissionada seguindo os padrões do projeto Jornada do Estudante.

Como já mencionado, a aplicação proposta utiliza tecnologias blockchain como um elemento central para garantir autenticidade, integridade e auditabilidade dos dados acadêmicos ao longo de toda a jornada do estudante, criando um diferencial competitivo no mercado de digitalização e gestão de acervos acadêmicos.

A blockchain permissionada baseada no *framework* Hyperledger Fabric será utilizada para criar um registro imutável de todos os documentos acadêmicos digitalizados, conferindo ao sistema um nível de transparência e confiança inatingível por soluções tradicionais de banco de dados centralizados. A interoperabilidade será assegurada com o padrão XML do Diploma Digital, permitindo compartilhamento de dados entre IES e MEC de forma descentralizada, reduzindo custos e aumentando a eficiência. Além disso, os contratos inteligentes gerenciarão o ciclo de vida dos documentos, verificando conformidade com padrões do MEC, associando metadados e automatizando auditorias. Assim, a solução oferece auditoria e rastreamento em tempo real de todas as operações realizadas nos documentos, atendendo a requisitos regulatórios. Com relação à segurança criptográfica será garantida por algoritmos robustos, com cada documento associado a uma *hash* única armazenada na blockchain para verificação de integridade. Finalmente, a arquitetura será projetada para escalabilidade e resiliência, lidando com grandes volumes de dados e evitando falhas únicas, enquanto mantém alta segurança.

Em relação ao modelo de comercialização proposto, baseia-se em assinaturas anuais que concedem acesso à API REST, interface gráfica e suporte técnico, com valores escalonados de acordo com o volume de documentos processados e o nível de serviço contratado. Serviços adicionais, como treinamentos especializados e consultorias, poderão ser contratados mediante cobrança adicional. Haverá também um pacote de implantação inicial, que incluirá a configuração do sistema, treinamento básico e migração de dados. O uso da blockchain será licenciado com base no número de registros efetuados, possibilitando uma estrutura de custos proporcional à utilização e promovendo acessibilidade e escalabilidade financeira.

3.2.1.3 Funcionalidades, objetivos e detalhes técnicos do DAIESEB

As principais funcionalidades da solução são:

1. **Formalização do processo de digitalização dos documentos físicos** por meio da definição das melhores práticas no trato dos documentos, no uso dos equipamentos de escaneamento e na geração dos documentos digitais intermediários;
2. **Extração de dados e classificação de documentos digitais intermediários** por meio de técnicas de visão computacional e IA;

3. **Enriquecimento dos documentos digitais intermediários com metadados**;
4. **Conversão dos documentos enriquecidos para XMLs** no modelo do Diploma Digital;
5. **Desenvolvimento de uma API para envios dos XMLs** de Acervo Acadêmico digital para uma Blockchain permissionada;
6. **Desenvolvimento de um contrato inteligente** para gerenciamento do ciclo de vida dos XMLs, permitindo leituras e escritas

Em relação aos **requisitos funcionais**, a solução proposta busca assegurar eficiência, segurança e conformidade com as diretrizes estabelecidas pelo MEC. Para isso, será implementada uma API REST, documentada com Swagger, que permitirá o envio e o processamento de documentos digitalizados por meio de *endpoints* padronizados. Cada instituição contará com uma chave de API exclusiva, garantindo autenticação segura e acesso individualizado.

O sistema utilizará IA treinada para reconhecer e processar diferentes tipos de documentos físicos, como carteiras de identidade e certidões de nascimento. Esses documentos serão integrados a um *pipeline* automatizado que os converterá inicialmente para formatos intermediários, como PDF, e, em seguida, para XML conforme o padrão exigido pelo Diploma Digital.

A integração ocorrerá em uma blockchain permissionada baseada no *framework* Hyperledger Fabric, assegurando auditabilidade e integridade durante todo o ciclo de vida dos documentos. Além disso, a solução será compatível com os padrões tanto do Diploma Digital quanto da Jornada do Estudante, promovendo o compartilhamento seguro de dados entre as instituições de ensino e o MEC.

No que diz respeito aos requisitos não-funcionais, a solução deve ser escalável, capaz de processar grandes volumes de documentos de forma simultânea, com uma arquitetura baseada em microsserviços distribuídos em ambiente de nuvem, permitindo a alocação dinâmica de recursos conforme a demanda. Para garantir alta disponibilidade, serão adotadas estratégias de redundância em servidores, armazenamento e serviços de API, assegurando um tempo de atividade superior a 99,9%. A segurança da solução será reforçada com criptografia de ponta a ponta e autenticação baseada em *tokens* JWT, em conformidade com a Lei Geral de Proteção de Dados (LGPD). A interface gráfica será responsiva, acessível e centrada na experiência do usuário, com design otimizado para diferentes dispositivos.

A aplicação poderá ser utilizada por meio de dois mecanismos. O primeiro e principal, será por meio da interação da IES com uma API Rest, que possibilitará que a IES submeta os documentos digitais intermediários. O segundo mecanismo proposto é uma interface gráfica conectada à API, para que o cliente possa operar com maior usabilidade.

A solução requer uma infraestrutura em nuvem escalável, como AWS ou GCP, para suportar a API REST e a interface gráfica. Isso inclui servidores dedicados para o processamento de documentos, armazenamento seguro e gerenciamento de chaves de

API. Modelos de inteligência artificial, preferencialmente de código aberto, serão executados em máquinas virtuais com suporte a GPUs, a fim de otimizar a extração e classificação automatizada de dados. A blockchain Hyperledger Fabric será adotada para gerenciar o ciclo de vida dos documentos, com nós validadores distribuídos e suporte a contratos inteligentes.

Os documentos digitalizados serão armazenados em um sistema híbrido, utilizando PostgreSQL para metadados e AWS S3 para os arquivos. A API será documentada através do Swagger, e ferramentas como Postman serão integradas para facilitar a interação. O sistema de monitoramento será realizado por Prometheus e Grafana, assegurando alta disponibilidade e visibilidade em tempo real.

A segurança será robustecida com criptografia de ponta a ponta e autenticação via *tokens* JWT, em conformidade com a LGPD. A interface gráfica, construída com *frameworks* modernos como React ou Angular, será responsiva e projetada para garantir uma experiência de usuário de alta usabilidade.

Com relação ao ambiente de desenvolvimento, nas etapas iniciais do projeto, especialmente no que se refere à digitalização do acervo físico das instituições, será essencial estabelecer uma parceria com uma IES. A UFSC é uma parceira em potencial, uma vez que permitirá o acesso a um conjunto real de documentos acadêmicos, essencial para o treinamento dos modelos de IA necessários para a extração e classificação dos dados.

Para o treinamento e a execução dos modelos de IA, será necessário o uso de uma máquina virtual em nuvem, com acesso à memória RAM e GPU. Na segunda fase do projeto, a implementação de uma rede privada e permissionada baseada em blockchain será imprescindível, utilizando o *framework* Hyperledger Fabric, desenvolvido pela Hyperledger Foundation.

O *testbed* fornecido pelo Projeto Ilíada poderá ser utilizado nesta fase para garantir a avaliação e validação da rede blockchain. As etapas subsequentes, sejam intermediárias ou finais, poderão ser realizadas e testadas com recursos próprios ou de parceiros. Por exemplo, para a etapa de conversão de arquivos digitalizados intermediários para XML no padrão do Diploma Digital, será necessária a implementação de uma API de conversão, a qual poderá ser hospedada em servidores próprios. Além disso, a colaboração com as equipes de desenvolvimento dos projetos Diploma Digital e Jornada do Estudante permitirá uma integração mais eficaz da solução com os padrões e aplicações já em desenvolvimento.

3.2.2 Levery: Plataforma de Carteira Digital e Negociação de Ativos Tokenizados

A Plataforma de Carteira Digital e Negociação de Ativos Tokenizados (Levery) tem como tópicos de interesse a "Carteira digital", "Transferências monetárias" e "Interoperabilidade" e como principal setor econômico de aplicação o Financeiro.

O desenvolvimento desta aplicação está sendo realizado pela Wire Labs, *startup* sediada em Florianópolis/SC, sob a coordenação de Cristiano Policarpo. Formam a equipe de trabalho os colaboradores apresentados na Tabela 12.

Tabela 12 - Equipe de Colaboradores da Levery

Nome do colaborador	Instituição	URL do LinkedIn
Cristiano Policarpo	Wire Labs	https://www.linkedin.com/in/cristiano-policarpo
Ingrid Gomes	Wire Labs	https://www.linkedin.com/in/ingrid-m-gomes

3.2.2.1 Visão geral da Levery e sua importância

A ideia da Plataforma Levery surgiu em 2023, quando a Wire Labs passou a atender instituições que enfrentavam uma crescente demanda por soluções capazes de integrar ativos digitais de forma segura aos seus serviços. No entanto, essas instituições encontravam obstáculos relacionados a desafios tecnológicos e aos rigorosos requisitos de conformidade e segurança exigidos pelo setor financeiro.

Em 2024, a Wire Labs deu início ao desenvolvimento da plataforma no âmbito da incubação promovida pela Uniswap, empresa americana referência em tecnologia DeFi. Essa parceria estratégica permitiu acelerar a criação de uma plataforma inovadora baseada em tecnologia AMM, com foco em conformidade regulatória, ao aproveitar a ampla expertise da Uniswap no setor de finanças descentralizadas.

Mais recentemente, a Levery foi selecionada para o programa de aceleração do Santander X, sendo reconhecida como uma das 10 fintechs mais promissoras do país entre mais de 800 candidaturas. Essa conquista reforça o potencial de impacto da solução e abre novas oportunidades de colaboração e expansão no mercado financeiro.

Como proposta de valor, a Levery oferece às instituições financeiras uma porta de entrada segura, regulada e eficiente para o universo dos ativos digitais. Ao permitir a expansão de serviços, a atração de novos públicos e a geração de novas fontes de receita, a solução posiciona essas instituições na vanguarda da inovação financeira. Com foco na adoção de tecnologias DeFi, na liquidez de ativos tokenizados e na integração com o Drex, o Levery viabiliza um avanço estratégico rumo à digitalização do sistema financeiro.

Apesar da presença de empresas especializadas em tokenização no Brasil, ainda há uma lacuna significativa: a ausência de plataformas em blockchain que ofereçam um ambiente padronizado, seguro e regulado para negociação desses ativos. A Levery foi desenvolvida exatamente para preencher essa lacuna, com uma infraestrutura robusta que alia segurança avançada à conformidade regulatória.

Baseado na tecnologia Automated Market Maker (AMM), a Levery elimina o risco de contraparte ao permitir negociações diretas, automatizadas e transparentes por meio de smart contracts. Esses contratos inteligentes garantem a execução segura das

transações e aumentam significativamente a confiança nas operações, estabelecendo um novo padrão de eficiência e segurança no mercado de ativos tokenizados. Com essa abordagem inovadora, o Levery não apenas responde a uma demanda emergente, mas redefine os caminhos possíveis para a transformação digital do setor financeiro.

São clientes potenciais da solução, bancos tradicionais e digitais, corretoras e outras instituições financeiras, empresas interessadas na negociação de ativos do mundo real tokenizados e instituições que buscam integrar serviços financeiros inovadores.

3.2.2.2 Descrição detalhada da Levery

Para ingressar no mercado de finanças descentralizadas (DeFi), as instituições financeiras enfrentam obstáculos significativos, especialmente devido à natureza anônima das transações, que conflita com exigências regulatórias e limita a adoção da tecnologia blockchain por esses agentes. Além disso, há uma notável ausência de infraestruturas robustas que viabilizem a operação e a liquidez de ativos reais tokenizados em ambientes sob supervisão regulatória.

Essas instituições demandam soluções que assegurem conformidade com normas como Know Your Customer (KYC) e Anti-Money Laundering (AML), ao mesmo tempo em que proporcionem altos níveis de segurança na custódia de ativos digitais. A integração de ativos digitais a sistemas legados também representa um desafio, agravado pela complexidade de gerenciar os riscos inerentes às transações descentralizadas — fatores que, em conjunto, dificultam sua atuação no ecossistema DeFi.

Ainda assim, o potencial desse mercado é expressivo. Embora o valor atual dos criptoativos esteja estimado em 3,3 trilhões de dólares, segundo o CoinMarketCap, o Fórum Econômico Mundial aponta que a tecnologia blockchain poderia movimentar até 867 trilhões de dólares em ativos reais tokenizados — como derivativos e títulos de dívida — desde que sejam desenvolvidas infraestruturas adequadas para sua operação e liquidez em ambientes regulados.

A Levery é uma plataforma *white label* que permite a instituições financeiras criarem suas próprias carteiras digitais e plataformas de negociação de ativos tokenizados.

Sua infraestrutura de carteira digital é totalmente compatível com a Ethereum Virtual Machine (EVM), possibilitando a integração com diversas blockchains públicas ou privadas baseadas em EVM, como Ethereum, Hyperledger Besu, Binance Smart Chain, Polygon, entre outras. Essa compatibilidade assegura a interoperabilidade com contratos inteligentes, DApps (aplicações descentralizadas) e *tokens* nos padrões ERC-20 e ERC-721 em múltiplas redes.

A plataforma combina custódia segura — com o uso de Hardware Security Modules (HSM) para a gestão de chaves privadas — com um robusto sistema de conformidade regulatória, integrando ferramentas de KYC e AML. Essa abordagem garante segurança operacional e aderência às normas legais vigentes.

Além disso, a Levery incorpora tecnologia de AMM para viabilizar a negociação de ativos digitais via contratos inteligentes, eliminando intermediários e mitigando os riscos de contraparte comuns em corretoras centralizadas.

A plataforma também integra oráculos de preço em tempo real, permitindo que o sistema AMM ajuste dinamicamente as taxas de transação com base nos valores atuais dos ativos. Isso assegura que os provedores de liquidez não negociem ativos abaixo do valor de mercado, protegendo seus interesses e preservando a integridade e a eficiência das operações.

Com a Levery, instituições financeiras podem ampliar seu portfólio de serviços oferecendo aos clientes opções inovadoras e seguras de investimento em ativos digitais.

Atualmente, a solução encontra-se em fase de validação, com um MVP funcional testado em ambiente simulado e um modelo de negócio já estruturado.

A aplicação utiliza tecnologias blockchain para viabilizar transações transparentes, seguras e imutáveis, eliminando a necessidade de intermediários e reduzindo significativamente os custos operacionais. Por meio da integração com contratos inteligentes e com a tecnologia de AMM, é possível implementar novos modelos de negócio, como a negociação direta de ativos e a formação de pools de liquidez.

Um dos grandes diferenciais da solução é sua compatibilidade com o Drex, a moeda digital brasileira em desenvolvimento. Isso posiciona a plataforma como pioneira na integração com a Central Bank Digital Currency (CBDC) nacional, ampliando as oportunidades no mercado financeiro e oferecendo uma vantagem competitiva relevante em um cenário de rápida tokenização de ativos.

Essa visão está alinhada com as diretrizes discutidas pelo coordenador do Piloto Drex do Banco Central do Brasil, Fábio Araújo, durante a 5ª reunião do Fórum Drex, realizada no G20 TechSprint 2024, em 27 de novembro de 2024. Na ocasião, Araújo destacou a importância da integração entre ativos digitais e o mercado tradicional de ativos do mundo real — como debêntures, créditos do agronegócio, automóveis e créditos de descarbonização — para promover maior eficiência e acessibilidade ao sistema financeiro.

Ao se alinhar a essas tendências, a Levery permite que instituições financeiras atuem no emergente mercado de ativos tokenizados, utilizando a tecnologia blockchain como um diferencial estratégico para agregar valor a seus produtos e serviços.

Com relação ao modelo de comercialização da solução, pode-se destacar:

- **Taxa de Setup**: Instituições financeiras pagam uma taxa de configuração da plataforma, incluindo backend, frontend, gestão de chaves privadas e assinaturas usando HSM, integração com oráculos de cotação preço, smart contracts e APIs.

- **Serviços de Customização**: Desenvolvimento de funcionalidades específicas para clientes.
- **Taxas de Transação**: Recebimento de uma porcentagem sobre as transações realizadas na plataforma.
- **Consultoria Especializada**: Serviços de consultoria em tecnologia blockchain com compliance regulatório.

3.2.2.3 Funcionalidades, objetivos e detalhes técnicos do Levery

As principais funcionalidades da plataforma são:

1. **Custódia Segura de Ativos Digitais**: utilização de HSMs para gestão de chaves privadas;
2. **Conformidade *(Compliance)* Regulatória**: integração com ferramentas de KYC e AML para verificação de identidade e monitoramento de transações;
3. **Gestão de Carteira**: interface intuitiva para gerenciamento, visualização, envio e recebimento de ativos digitais, com suporte a múltiplas redes blockchain;
4. **Plataforma AMM**: Permite a negociação de ativos digitais via contratos inteligentes, eliminando intermediários e reduzindo riscos;
5. **Integração *On-Ramp* Opcional**: facilita a compra de criptoativos com cartão de crédito, ampliando o acesso dos usuários e gerando comissões para a instituição;
6. ***Pools* de Liquidez**: Instituições podem criar pools de liquidez, atraindo provedores de liquidez e negociadores, gerando novas fontes de receita.

Para atendimento ao problema descrito, são requisitos da solução:

1. Implementação de protocolos robustos de segurança cibernética e uso de HSMs para gestão segura de chaves privadas;
2. Adequação às regulamentações financeiras nacionais e internacionais, incluindo KYC e AML, garantindo conformidade legal e prevenção a fraudes;
3. Integração entre múltiplas redes blockchain e compatibilidade com sistemas legados das instituições financeiras, facilitando a integração e expansão dos serviços;
4. Integração de oráculos de cotação de preço para obter dados de mercado em tempo real, assegurando precisão nas transações e ajustes automáticos das taxas no sistema AMM;
5. Escalabilidade para atender a um grande volume de transações e usuários simultaneamente, mantendo desempenho e estabilidade;
6. Interface amigável, projetada para facilitar a adoção por usuários com diferentes níveis de familiaridade com tecnologias digitais, garantindo uma experiência agradável e de fácil compreensão.

Em relação à forma de utilização, no processo de *onboarding*, a criação de uma carteira é simples e segura, utilizando abstração de contas blockchain. O cliente pode acessar a plataforma pelo celular ou computador, vinculando sua conta de e-mail diretamente à nova carteira. Integrado ao sistema KYC, o processo inclui a verificação de documentos

e biometria facial para garantir a autenticidade. As chaves privadas são armazenadas com máxima segurança no backend, utilizando módulos HSM para sua gestão.

A plataforma oferece uma visão abrangente dos ativos digitais, com saldo consolidado em reais, histórico de desempenho em tempo real e histórico de atividades detalhado e transparente, semelhante a um extrato bancário. Cada transação exibe informações como *hash*, *timestamp*, carteiras envolvidas e valor transferido, garantindo total transparência.

A interface permite a gestão de ativos, negociação em *pools* de liquidez, investimentos, envio e recebimento de ativos digitais, além de interação com serviços financeiros descentralizados — tudo com um elevado nível de segurança e em conformidade com as normas regulatórias.

O sistema AML monitora continuamente as interações para identificar riscos, bloquear transações suspeitas em tempo real e notificar a equipe de risco da instituição provedora do serviço, assegurando a conformidade com as regulamentações.

Estão sendo utilizados os seguintes recursos tecnológicos:

- Infraestrutura de servidores seguros para hospedagem da plataforma.
- HSMs para gerenciamento de chaves privadas.
- Integração com APIs de parceiros de KYC/AML.
- Integração com oráculos de cotação preço.
- Ambiente de desenvolvimento compatível com EVM.

Finalmente, com relação ao ambiente de desenvolvimento e testes, está sendo utilizada a infraestrutura própria Wireshape Floripa Testnet. Além disso, o *testbed* provido pelo Projeto Ilíada será também adotado para experimentação, testes adicionais e validação da solução. A infraestrutura oferecida pelo projeto permite a implantação dos nós blockchain necessários e a integração com redes EVM.

3.2.3 Modelagem de Aplicações Piloto Baseadas em NFTs de Ciclo Preditivo Utilizando a Plataforma Ledger NFT

A Modelagem de Aplicações Piloto Baseadas em NFTs de Ciclo Preditivo Utilizando a Plataforma Ledger NFT tem como tópicos de interesse a "Automatização de processos", "Gestão de ativos", "Interoperabilidade" e "rastreabilidade de procedência e de cadeias" e como principal setor econômico de aplicação o Informação e Comunicação.

O desenvolvimento desta aplicação está sendo realizado pela Ledgertec, *startup* sediada em João Pessoa/PB. Formam a equipe de trabalho os colaboradores apresentados na Tabela 13.

Tabela 13 - Equipe de Colaboradores de Modelagem de Aplicações Piloto

Nome do colaborador	Instituição	URL do currículo Lattes
Caio Souza Florentino	Ledgertec	Não disponível
Daniel Faustino Lacerda de Souza	Ledgertec	http://lattes.cnpq.br/7175882793842898
Guido Lemos de Souza Filho	Ledgertec	Não disponível
Marcelo Hercules Cunha Soares	Ledgertec	http://lattes.cnpq.br/4298506592950477
Rostand Edson Oliveira Costa	Ledgertec	http://lattes.cnpq.br/3145331081780004

3.2.3.1 Visão geral da Modelagem de Aplicações Piloto e sua importância

Embora os NFTs tenham ganhado popularidade principalmente como colecionáveis digitais, sua tecnologia tem potencial para aplicações mais amplas, inclusive em cadeias de valor com ativos reais. Baseados no padrão ERC-721, os NFTs garantem exclusividade por meio de metadados. No entanto, tais operações não permitem suportar alguns requisitos específicos de algumas aplicações que podem se beneficiar de parte das características de um NFT tradicional mas demandam tratamentos especiais. Dentre as singularidades de interesse, está a possibilidade de limitar a troca de propriedade de um NFT.

A partir dessa observação, a Ledger desenvolveu um conceito complementar de NFT voltado à gestão de ativos digitais com circulação restrita. Esses *tokens* especiais, denominados NFTs de Ciclo Preditivo (NFT-CP), têm como principal característica a definição de um ciclo específico e/ou finito para operações de troca de estado e/ou transferência de propriedade.

Quando o ciclo de um NFT-CP prevê a existência de um destinatário final — ou seja, um detentor definitivo do ativo, com perfil previamente definido — esses *tokens* podem ser agrupados em uma categoria específica chamada NFTs Não Vendáveis (NFT-NV). Nessa modalidade, os ativos não podem ser transferidos livremente, respeitando o propósito de destinação final.

Além disso, ao incorporar a possibilidade de que o ativo digital representado — ou ao menos alguns de seus atributos ou estados — possa ser alterado por fatores externos específicos, surge uma nova classe de NFT-CP, denominada NFTs Dinâmicos (NFT-D). Essa categoria permite a vinculação a oráculos dedicados, que viabilizam a verificação de informações externas sujeitas a variações.

Paralelamente, surgiu também a ideia de desenvolver uma plataforma *no-code/low-code* capaz de adaptar a tecnologia de *tokens* não fungíveis para, de forma simplificada e interativa, viabilizar os conceitos de NFTs de Ciclo Preditivo, NFTs Não Vendáveis , NFTs Dinâmicos e NFTs Não Vendáveis Dinâmicos (NFT-NVD) (combinação das duas anteriores). A plataforma tem como objetivo oferecer suporte a aplicações

que exigem a representação e a gestão digital de ativos com essas características específicas.

Em 2021, a Ledger teve uma proposta aprovada no âmbito da Chamada CNPq/MCTI/SEMPI Nº 021/2021, voltada à colocação de pesquisadores em empresas. Com isso, contou com a colaboração de um doutor, um mestre e um graduado, além de sua equipe interna, para consolidar o conceito de NFT-CP e desenvolver a Plataforma LedgerNFT. Atualmente em início de operação, a plataforma está alinhada com a 3ª Chamada do Projeto Ilíada, e o objetivo da proposta é desenvolver três protótipos funcionais baseados em NFTs de Ciclo Preditivo.

A proposta de valor da plataforma LedgerNFT está baseada na capacidade de resolver um problema atual e significativo: garantir segurança e padronização nos processos de criação e transferência de ativos digitais, além de combater fraudes na verificação de estado e condições de propriedade. Com a introdução de um processo integrado e padronizado, a plataforma facilita e torna mais segura a realização de provas de integridade, autenticidade, autoria e propriedade, bem como outras cerimônias de verificação e alteração de ativos digitais. Espera-se que a plataforma permita a emissão mais ágil e econômica de certificados acadêmicos, o controle de carteiras de conselhos de classe e a confirmação e renovação de cadastros, proporcionando maior frequência, conveniência e redução de riscos para os clientes, ao mesmo tempo em que aumenta o conforto para os usuários.

Do ponto de vista de negócios, a tokenização de documentos digitais é apenas uma das várias aplicações previstas. O público-alvo da plataforma proposta é diversificado e pode ser segmentado em três grupos principais:

- clientes - agências reguladoras, conselhos de classe, ministérios, universidades, bancos, fintechs, operadoras de cartões de crédito, seguradoras, órgãos públicos, entre outros;
- usuários - alunos, médicos, engenheiros, arquitetos, vendedores, compradores, entre outros; e
- operadores - instituições ou servidores responsáveis por realizar cadastramento, confirmação e autenticação de integridade, autenticidade, autoria e propriedade de ativos reais e digitais.

No que se refere ao relacionamento com clientes, a plataforma adota dois modelos clássicos. O primeiro é um relacionamento personalizado, voltado a clientes e operadores nas fases de integração, configuração, implantação e operação da plataforma, bem como no desenvolvimento de projetos sob medida. O segundo é um relacionamento automatizado, direcionado aos usuários e operadores que utilizam a plataforma para emissão, controle e geração de provas de integridade, autenticidade, autoria e propriedade.

3.2.3.2 Descrição detalhada da Modelagem de Aplicações Piloto

A Ledger já atua no segmento de registro em blockchain, oferecendo soluções baseadas em estratégias tradicionais, como o uso de âncoras criptográficas para

garantir provas de integridade, existência e autoria de documentos digitais relevantes. No entanto, essa abordagem funciona apenas como um complemento aos fluxos naturais das aplicações onde esses recursos são empregados.

Nesse contexto, os NFTs surgem como aliados estratégicos para o gerenciamento do ciclo de vida de Documentos Digitais Relevantes (DDRs), possibilitando a definição de semânticas específicas adaptadas a cada tipo de documento. Mais do que fornecer as funcionalidades fundamentais de uma DLT com criptografia robusta, os NFTs permitem a implementação de salvaguardas adicionais contra falsificação de dados e alterações não autorizadas de estado ou propriedade.

Com isso, abre-se um leque de novas possibilidades e aplicações para o setor de gestão de documentos digitais relevantes.

O conceito de NFT de Ciclo Preditivo (NFT-CP) pode ser aplicado à representação de documentos digitais relevantes como diplomas, certidões, autorizações, contratos e documentos de identificação pessoal. Cada tipo de documento segue fluxos específicos de emissão e validação, envolvendo diferentes atores. Por exemplo, a emissão de diplomas graduação envolve o MEC, universidades e alunos; já o CPF é emitido diretamente pela Receita Federal ao contribuinte. Em todos os casos, os documentos são intransferíveis, pertencem exclusivamente ao titular e contêm informações imutáveis, o que torna os NFT-CPs uma solução ideal para sua representação e controle.

Assim, o objetivo deste projeto é modelar aplicações baseadas em contratos inteligentes piloto para controlar *tokens* baseados em NFTs-CP e suas variações, servindo como prova de conceito da aplicabilidade e da flexibilidade da Plataforma LedgerNFT. Neste sentido, serão especificados, modelados, implementados e validados três protótipos de aplicações piloto utilizando a Plataforma LedgerNFT, a saber:

- **NFT-Badge**: especificar, modelar e implementar um *token* baseado no template de NFT de ciclo preditivo do tipo Não Vendável para representar medalhas e certificações associadas com habilidades e competências adquiridas ou oriundas de educação continuada, considerando uma cadeia de custódia e controle que envolva entidades certificadoras, empresas licenciadas e detentores;
- **NFT-License**: especificar, modelar e implementar um *token* para representar registros de qualificação de especialista e área de atuação de um médico, considerando uma cadeia de custódia e controle que envolva CFM, CRMs e médicos;
- **NFT-Certificate**: especificar, modelar e implementar um *token* para representar certificados de conclusão do ensino médio, considerando uma cadeia de custódia e controle que envolva MEC, Secretarias Estaduais e Municipais de Educação, escolas e alunos.

A proposta de modelagem de aplicações baseadas em NFTs de Ciclo Preditivo alia alto grau de inovação tecnológica a um forte apelo social e econômico, ao explorar a

aplicação de avanços recentes em tokenização e propriedade digital para aprimorar a gestão do ciclo de vida de documentos digitais relevantes — especialmente aqueles que representam ativos ou entidades do mundo real. A Plataforma LedgerNFT tem potencial para se consolidar como um serviço estratégico da Ledger voltado a instituições públicas e privadas de diversos setores.

A oferta de uma solução confiável e eficiente para a gestão de ativos digitais é particularmente oportuna diante do avanço da digitalização nas relações humanas. O projeto busca investigar usos inovadores dos NFTs em contextos ainda inexplorados, o que confere elevado grau de originalidade aos resultados esperados. A expertise tecnológica e científica desenvolvida pela Ledger representa uma vantagem competitiva significativa, servindo como base para o amadurecimento da plataforma LedgerNFT e para a consolidação do conceito de NFT de Ciclo Preditivo no mercado.

Além disso, a Plataforma LedgerNFT é compatível com os canais e formas de entrega já utilizados pela Ledger, incluindo ministérios, organizações sociais, órgãos públicos, empresas privadas, fundações e instituições de ensino superior (IES). Essa compatibilidade amplia o potencial de adoção da solução, facilitando a geração e o desenvolvimento de demanda nesses e em novos segmentos. Além disso, a plataforma apresenta forte sinergia com outros produtos da Ledger, como o LedgerSign e o LedgerDoc (que utilizam recursos de NFTs Dinâmicos), o LedgerChain e o LedgerGuard (voltados ao registro e guarda de objetos digitais com base em NFTs-CP), e o LedgerMedDoc (que aplica NFTs Não Vendáveis em prescrições, atestados e documentos médicos).

3.2.3.3 Funcionalidades, objetivos e detalhes técnicos da Modelagem de Aplicações Piloto

Os NFTs considerados neste projeto, denominados NFTs de Ciclo Preditivo ou de ciclo pré-determinado, têm seu ciclo de vida completamente definido desde a concepção. No desenvolvimento do contrato inteligente, é possível estabelecer quantas — e quais — entidades participarão do processo, quantos e quais atributos serão representados no *token*, quem poderá modificá-los e em que momento isso ocorrerá. Dessa forma, tanto o ativo representado quanto as regras para a entrega dos *tokens* podem ser configurados de forma personalizada, conforme os requisitos específicos de cada contexto ou aplicação.

Neste sentido, o conceito de NFT-CP desenvolvido pela Ledger baseia-se em uma sequência finita de estados, onde cada fase é responsável por atualizar os atributos do *token* até que ele esteja pronto para ser entregue ao proprietário definitivo, como mostra a Figura 15. São definidos, pelo menos, três tipos distintos de entidades, cada uma representada por uma ou mais carteiras na blockchain, desempenhando papéis específicos na interação com a instância do NFT-CP:

- **Entidade Emissora** (EE): Responsável pelo processo inicial de criação dos *tokens*. A carteira dessa entidade terá permissões de administração dentro dos contratos;

- **Entidades Controladoras** (EC): Responsáveis por modificar ou adicionar novos atributos ao *token* antes de chegar ao destinatário final. Entidades Controladoras podem também transferir o *token* para outras entidades, além da Entidade Final;
- **Entidade Destinatária** (ED): O/a proprietário(a) final do NFT-CP. Ele não poderá transferir ou modificar características de seu *token*.

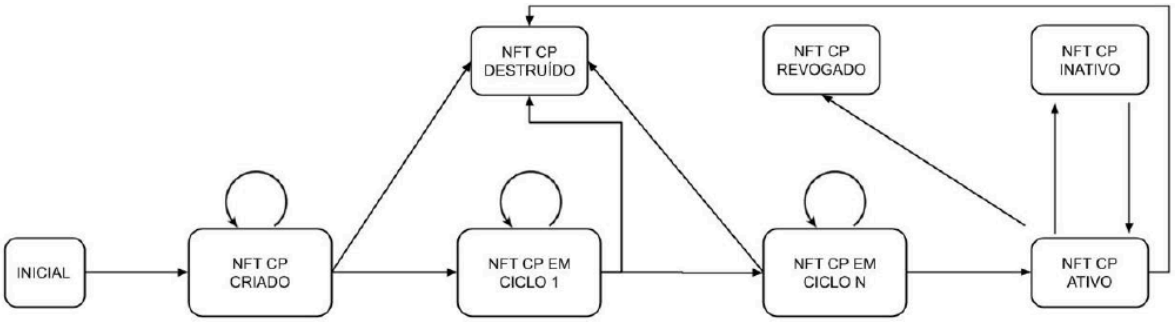

Figura 15 - Estados do ciclo de vida de um NFT-CP[15]

Ao longo de seu ciclo de vida, um NFT de Ciclo Preditivo (NFT-CP) pode transitar por cinco estados distintos, que definem quais entidades têm permissão para interagir com o *token* e quais ações podem ser realizadas. Os estados são:

- Editável pela Entidade Emissora;
- Editável pela Entidade Emissora ou por uma das Entidades Controladoras;
- Editável exclusivamente por uma das Entidades Controladoras;
- Entregue ao Destinatário Final (ou Ativo vinculado);
- Inativo ou Revogado.

Além desses estados, o NFT-CP também pode ser destruído pela Entidade Emissora ou por uma das Entidades Controladoras, em situações especiais previamente definidas.

No que tange os requisitos necessários da solução, destacam-se os seguintes:

1. **Uso de templates de Contratos Inteligentes** - Permite padronizar e reutilizar componentes para diferentes aplicações;
2. **Abordagem baseada em Linha de Produto de Software** (LPS) – Viabiliza a criação de variações do produto a partir de uma base comum;
3. **Personalização de contratos NFTs-NV, NFTs-D e NFTs-NVD** – Adaptabilidade da solução conforme as necessidades específicas de cada cliente;
4. **Plataforma funcional no code/low code** – Usuários podem configurar e criar soluções sem necessidade de programação avançada;
5. **Parametrização como principal forma de customização** – Reduz a complexidade técnica para adaptar o produto a diferentes contextos;
6. **Agilidade na implantação** – Permite entrega rápida de soluções ao cliente;
7. **Redução de custos e prazos de desenvolvimento** – Otimização de recursos ao evitar reescrita de código para cada projeto.

[15] Extraída da proposta apresentada à RNP em resposta aos Editais.

Com relação à sua utilização, a Plataforma LedgerNFT conta com os seguintes cinco módulos principais que compõem o fluxo de uso, abrangendo todo o ciclo de interação dos usuários com a aplicação, como pode ser observado na Figura 14:

- **Módulo Composer** - onde o usuário irá definir e personalizar o contrato de acordo com sua necessidade;
- **Módulo Builder** - o usuário usará as configurações criadas no Composer para gerar o código-fonte de seus contratos inteligentes personalizados;
- **Módulo Deployer** - responsável pela implantação do código de seu contrato criado pelo Builder em alguma blockchain de preferência.
- **Módulos de Contratos Inteligentes e de *Tokens*** - possibilitam ao usuário uma interação facilitada com as funções tanto de um contrato inteligente quanto de uma instância de um *token* NFT-CP. Essas operações incluem leitura dos dados, cunhagem de novos *tokens* e alteração do estado dos *tokens* existentes.

Ainda, existem quatro principais perfis de usuários que podem interagir com a Plataforma LedgerNFT, com permissões e responsabilidades específicas dentro de cada módulo do sistema, quais sejam:

- Desenvolvedor de Aplicações;
- Implantador/Operador de Contratos Inteligentes;
- Emissor de *tokens* e Detentor de *tokens*.

Além disso, os contratos inteligentes criados na plataforma também podem definir o seu próprio controle de acesso e autorização para as entidades envolvidas, a partir das configurações realizadas no módulo Composer.

A Plataforma LedgerNFT é ofertada como SaaS pela Ledger e será utilizada no desenvolvimento dos protótipos das três aplicações baseadas em *tokens* NFT-CP previstas no projeto.

Serão usados para desenvolvimento e testes os ambientes Ethereum Sepolia Testnet e Ethereum Holesky Testnet . Caso haja compatibilidade, também gostaríamos, em atividade complementar, de integrar a Plataforma LedgerNFT com o *testbed* provido pelo Projeto Ilíada.

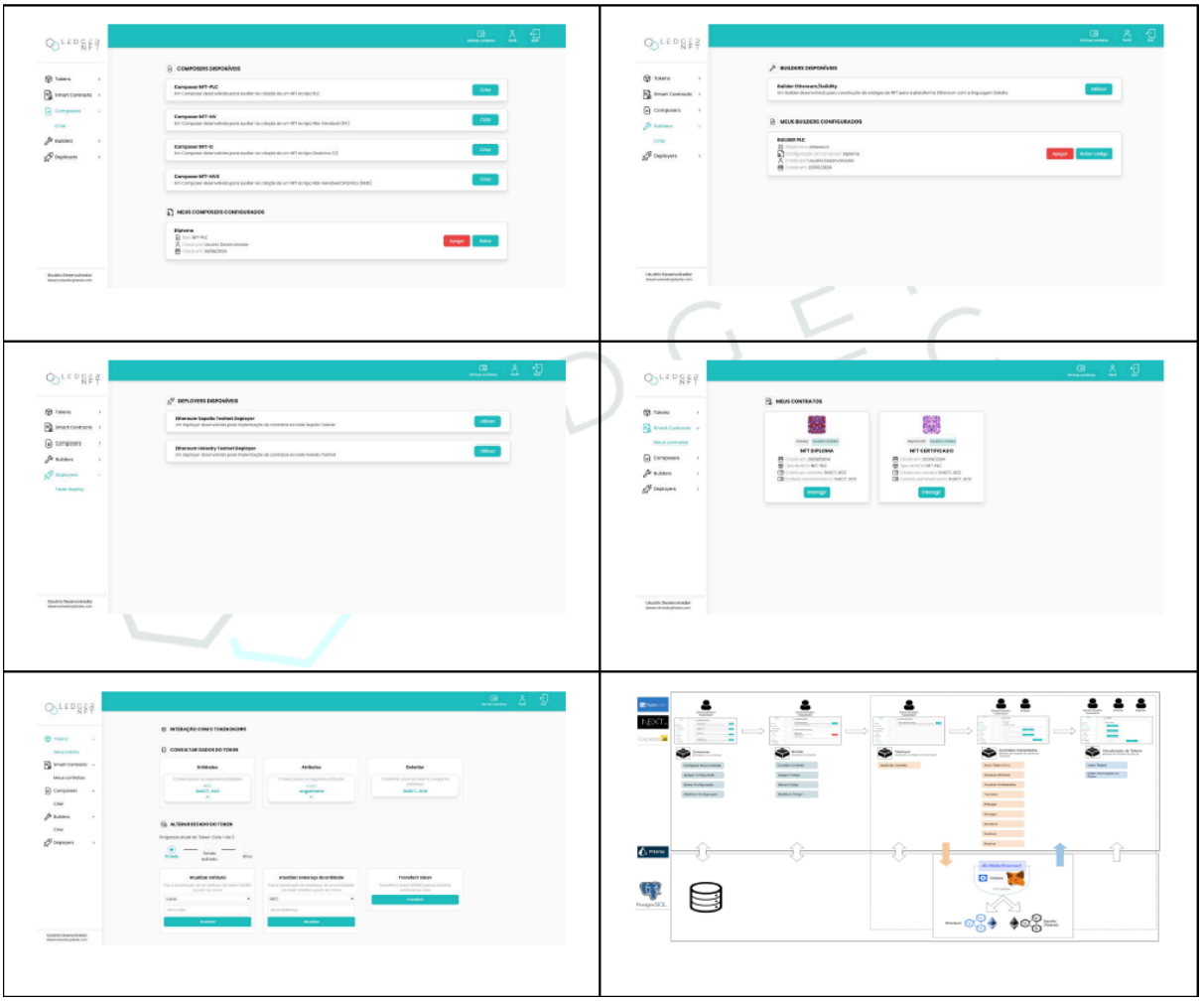

Figura 14 - Visão geral dos módulos e da arquitetura da Plataforma LedgerNFT[16]

3.2.4 Rastreabilidade Química Inteligente: Agricultura na Era da Blockchain

A Rastreabilidade Química Inteligente: Agricultura na Era da Blockchain tem como tópicos de interesse a "Rastreabilidade de procedência e de cadeias" e como principal setor econômico de aplicação o Agropecuário.

O desenvolvimento desta aplicação está sendo realizado pela SOLLYTCH, *startup* sediada no Rio de Janeiro/RJ, sob a coordenação de Mônica Santana Vianna. Formam a equipe de trabalho os colaboradores apresentados na Tabela 14.

[16] Extraída da proposta apresentada à RNP em resposta aos Editais.

Tabela 14 - Equipe de Colaboradores do Rastreabilidade Química Inteligente

Nome do colaborador	Instituição	URL do currículo Lattes ou LinkedIn
Mônica Santana Vianna	SOLLYTCH	http://lattes.cnpq.br/6640474781040632
Prof. João Paulo Machado Torres	SOLLYTCH e UFRJ	http://lattes.cnpq.br/3779152785564988
Sérgio de Gouvêa Vianna	SOLLYTCH	Não disponível
Carina Camões Silva da Rosa	SOLLYTCH	http://lattes.cnpq.br/4221413012372895
Walter Spolidoro	Zichat	https://www.linkedin.com/in/walter-spolidoro/
Prof. Wilson Melo	Lainf e PPG/INMETRO	Não disponível

3.2.4.1 Visão geral do Rastreabilidade Química Inteligente e sua importância

Uma das principais expertises dos sócios da SOLLYTCH é a Química Analítica, especialmente sua aplicação nas áreas de agricultura e sustentabilidade. A rastreabilidade química sempre foi um diferencial desta *startup*, com foco na importância de informações precisas e essenciais para a indústria. Com base nessa experiência, a empresa desenvolveu e fabrica seus próprios *kits* rápidos de análise química, que alimentam a plataforma de rastreabilidade.

Desde o início, ficou claro que esses *kits* de análise teriam limitações, especialmente em relação à certificação e conformidade para comercialização, visto que muitos órgãos reguladores e de fiscalização enfrentam dificuldades para aceitar os resultados desses *kits*. Com isso em mente, surgiu a questão central deste projeto: como validar rapidamente os resultados obtidos pelos *kits* de análise, garantindo total aceitação por parte do mercado e das áreas técnicas de regulamentação?

A resposta a essa questão envolveu a criação de um procedimento que permitisse comparar rapidamente o desempenho dos *kits* com metodologias reconhecidas como padrão-ouro, que são as únicas aceitas para validar análises químicas complexas. Embora a comparação já seja feita internamente no sistema da empresa, os dados técnicos dessa validação não estão acessíveis aos usuários ou outros envolvidos no processo. Para garantir a aceitação rápida pelos órgãos competentes, é fundamental que os dados sejam transparentes, seguros, imutáveis e compartilhados de forma eficaz.

A proposta de valor e importância desta solução reside em:

- Oferecer um serviço de rastreabilidade ágil, completo de menor custo incluindo informações sobre a qualidade dos processos de produção e produto final que farão o diferencial na comercialização e no atendimento à fiscalizações;

- Otimizar o processo de produção (economia) e maior valor agregado dos produtos;
- Agilizar os processos de comercialização de produtos perecíveis;
- Evitar ações protecionistas e ampliação do mercado internacional dos produtos rastreados.

Os potenciais clientes para esta solução de rastreabilidade química incluem produtores rurais, agroindústrias e empresas do setor de controle de qualidade de matéria-prima, bem como o varejo de produtos in natura, como supermercados e centrais de abastecimento de alimentos. Além disso, empresas de exportação (como comercializadoras e *Trading Companies*) e certificadoras de qualidade de alimentos e bens agropecuários também são partes interessadas. Devido à sua inovação no setor, o mercado internacional representa uma oportunidade adicional. Outro segmento relevante são os órgãos responsáveis pela fiscalização de alimentos, produtos agropecuários e controles fitossanitário e sanitário animal, abrangendo as esferas municipal, estadual e federal. A empresa já atende à demanda do setor de pesquisa e desenvolvimento, com universidades e centros de pesquisa adquirindo os kits para seus estudos agroambientais e de qualidade na indústria.

3.2.4.2 Descrição detalhada do Rastreabilidade Química Inteligente

Um exemplo concreto que aconteceu ao longo da trajetória da empresa, mas já previsto pela sua análise SWOT (Strengths, Weaknesses, Opportunities e Threats) foi a não aceitação dos resultados dos *kits* para exportação de produtos agrícolas. Esse problema não se limita à exportação, mas também afeta o mercado interno, especialmente no varejo, que enfrenta a mesma restrição. Embora a produção e os produtos sejam detalhados de maneira mais precisa, a metodologia aplicada nos *kits* de análise ainda não é reconhecida dentro dos protocolos e processos burocráticos da fiscalização, mesmo estando validada por documentação técnica pertinente.

Em situações como essa, não apenas para exportação, mas também para certificações e processos de fiscalização e qualificação de produtos, a metodologia aceita de análise química é exclusivamente o padrão-ouro. Esses métodos, considerados o padrão de excelência, são complexos, custosos, exigem equipamentos sofisticados, difíceis de operar, manter e calibrar, além de apresentarem prazos de resposta incompatíveis com os ciclos rápidos de comercialização.

Embora os *kits* sejam amplamente reconhecidos na fase inicial de triagem e varredura da produção, eles não são aceitos na etapa final de validação da qualidade e conformidade. No entanto, devido ao alto desempenho dos *kits*, eles poderiam ser utilizados em todas as etapas da cadeia produtiva, pois oferecem precisão, menor custo e agilidade nos resultados. O grande desafio, porém, tem sido a dificuldade em integrar essa validação de métodos mais simples ao fluxo dinâmico de uma cadeia produtiva tão complexa.

Nesse sentido, este projeto propõe o uso da tecnologia blockchain no processo de validação ágil dos métodos de análise por *kits* rápidos para uso em toda a cadeia de produção e logística do setor agropecuário.

A maior dificuldade para esta validação reside na comparação de desempenho de ambos os métodos: os inovadores (como os *kits*, por exemplo) e os métodos classificados como padrão-ouro. Mesmo que sejam desenvolvidos modelos e algoritmos para que esta operação aconteça rapidamente, outros requisitos precisam ser atendidos: transparência, integridade dos dados, seu compartilhamento seguro com auditabilidade e a visão geral da cadeia de custódia.

O processo de validação de métodos de análise pode ser acelerado por meio da confiabilidade nos procedimentos de aquisição e tratamento de dados. Nesse contexto, o objetivo é viabilizar uma validação mais ágil dos métodos analíticos utilizados nos *kits* de detecção de substâncias químicas, por meio da comparação do seu desempenho com os métodos considerados padrão-ouro, utilizando tecnologia blockchain.

Os parâmetros de desempenho utilizados nessa validação seguem os protocolos internacionais e as diretrizes estabelecidas pelo INMETRO — órgão responsável por garantir a rastreabilidade, confiabilidade e precisão das medições em território nacional. Para isso, o tratamento dos dados será realizado com o uso de modelos de inteligência artificial baseados em regressão, implementados diretamente em contratos inteligentes na blockchain ("*on-chain*"), assegurando transparência, imutabilidade e auditabilidade em todo o processo.

Atualmente o uso do *kit* consiste nas seguintes etapas:

1. Adição da amostra ao suporte (do *kit*);
2. Revelação da cor no suporte após a adição da amostra;
3. Envio deste resultado pelo usuário através de uma imagem com as cores reveladas;
4. Tradução da imagem em valor numérico de concentração da amostra analisada pelo sistema da empresa;
5. Envio dos resultados validados para a plataforma de rastreabilidade.

A tecnologia blockchain será utilizada tanto para armazenar dados e informações associadas aos métodos padrão-ouro quanto para registrar as imagens da revelação de cor dos *kits* de análise. As imagens obtidas pelos *kits* ("off-chain") geram resumos criptográficos ("on-chain"), garantindo integridade e possibilitando auditorias futuras. Todo o processo de comparação poderá ser executado automaticamente por meio de um contrato inteligente, que centraliza as operações de validação.

Esse fluxo, embora relativamente simples, representa uma solução elegante e tecnicamente sofisticada. Ressalta-se ainda o desafio científico-tecnológico envolvido, especialmente pela integração de modelos de inteligência artificial diretamente no smart contract, o que amplia as capacidades do sistema.

Ao incorporar blockchain, o serviço de análise química torna-se mais eficiente, transparente e escalável, sendo capaz de atender a um número crescente de usuários e volumes maiores de dados sem comprometer a confiabilidade dos resultados. Isso amplia o acesso ao serviço e facilita a colaboração entre diferentes agentes, estimulando a inovação e o avanço na área de análises químicas.

1. Fase de configuração:

    a. Cada *kit* é associado ao seu padrão ouro de verificação

    b. O arquivo de dados numéricos é inserido na rede blockchain, de forma imutável

2. Fase de auditoria/verificação
    a. Cada *kit* é associado ao seu padrão ouro de verificação
    b. O arquivo de dados numéricos é inserido na rede blockchain, de forma imutável
    c. Uma aplicação cliente (pode ser um app de celular) captura a imagem do *kits* em campo
    d. A imagem é inicialmente armazenada em um serviço off-chain (tipo IPFS)
    e. A imagem é enviada como parâmetro para um contrato inteligente no blockchain
    f. O contrato inteligente aplica modelos de IA que extraem o padrão de comparação
    g. O contrato inteligente compara os padrões, gravando o resultado, juntamente com um resumo criptográfico da imagem, para fins de auditoria.

A obtenção de dados químicos sobre diversas substâncias presentes na produção agrícola tornou-se cada vez mais estratégica, sendo essencial para aprimorar a precisão dos serviços de rastreabilidade, a previsibilidade da produção e a qualidade dos processos e do produto final. No entanto, esses dados são tradicionalmente difíceis de coletar, devido à complexidade das medições e ao tempo necessário para obtê-los.

Nesse contexto, o uso da tecnologia blockchain surge como uma solução para superar essas limitações. Ao garantir a integridade, rastreabilidade e segurança das informações, a blockchain oferece um diferencial competitivo — criando uma barreira de entrada para novos concorrentes e abrindo caminho para uma transformação na área de análises químicas.

É importante destacar que, na área de validação de dados analíticos — sejam químicos, biológicos ou físico-químicos —, a confiabilidade depende diretamente da presença simultânea de rastreabilidade, segurança e integridade dos dados. Essas características são inseparáveis e indispensáveis para garantir a credibilidade dos resultados. Além disso, sua integração permite a agilidade necessária para agregar valor aos clientes e demais atores da cadeia produtiva.

A tecnologia blockchain oferece um ambiente confiável, transparente e seguro para o registro e gerenciamento de dados em análises químicas, com potencial transformador na forma como esses dados são gerados, armazenados e compartilhados. Imagine um sistema em que cada etapa da análise — da coleta da amostra à obtenção do resultado final — é registrada de maneira imutável e auditável. Esse nível de rastreabilidade cria as bases para validações seguras, rápidas e até mesmo remotas.

A aplicação da blockchain na rastreabilidade é uma estratégia crucial, especialmente por impactar diretamente dois elementos-chave na cadeia de escoamento e comercialização de produtos agropecuários: custo e tempo. A capacidade de validar rapidamente métodos analíticos mais acessíveis, mas com desempenho comprovado, torna essa tecnologia um catalisador de escala para outras soluções no setor.

A utilização da tecnologia blockchain resolve um dilema até então insuperável: a dicotomia entre confiabilidade e agilidade. Tradicionalmente, garantir a confiabilidade dos elos da cadeia exige alto custo e tempo, devido ao uso exclusivo de metodologias padrão-ouro, sem espaço para alternativas de validação. Os processos de validação não existem para fins comerciais, uma vez que não há tecnologia capaz de integrar essa validação de forma eficiente nos fluxos logísticos e de comercialização de cadeias complexas, como a do setor agropecuário. Como resultado, a busca por confiabilidade acaba dificultando a implementação de soluções inovadoras e o uso de novas tecnologias.

A transformação está em permitir que confiabilidade e agilidade coexistam. Não basta ter inteligência em dados que forneçam respostas rápidas se o nível de confiabilidade não atender às exigências operacionais do mercado. Da mesma forma, o uso de IA nas análises não é suficiente para atender às necessidades de um mercado que exige conformidade com rigorosas normas técnicas, como certificações e outros requisitos.

A adoção do blockchain pode auxiliar na padronização de procedimentos e na garantia da qualidade das análises, especialmente em um contexto globalizado. Para criar uma solução inovadora com impacto significativo no mercado, a transparência dos processos precisa ser total. No setor agrícola, o fator tempo é fundamental, pois a cadeia de produção e logística é frequentemente complexa, envolvendo múltiplos países ou estados. Os produtos precisam ser produzidos, colhidos e comercializados em um curto espaço de tempo, enquanto enfrentam crescentes exigências de qualidade e sustentabilidade, além de barreiras protecionistas.

Nesse cenário, a qualidade dos dados fornecidos, seu custo, tempo de aquisição e confiabilidade são determinantes para o sucesso. A agilidade no reconhecimento da equivalência entre métodos analíticos é essencial para garantir que a transparência dos dados se traduza em um verdadeiro diferencial competitivo.

O uso de blockchain para validação analítica amplia a aplicação de métodos rápidos de análise, gerando impactos diretos na Agricultura de Precisão, que já utiliza sensores, *kits* portáteis e outros métodos rápidos de detecção no campo, incluindo detecções remotas via drones ou satélites. O que distingue essa abordagem é que, ao contrário

das soluções atuais, ela traz a devida validação, transparência e confiabilidade ao uso desses dispositivos remotos de mensuração.

Com relação à comercialização da solução, a proposta é manter o modelo de negócio atual, que consiste de uma assinatura mensal da plataforma digital de rastreabilidade, com a venda dos *kits* já embutida no valor da assinatura.

3.2.4.3 Principais funcionalidades, objetivos específicos e detalhes técnicos do Rastreabilidade Química Inteligente

As principais funcionalidades da aplicação são:

1. **Armazenamento de dados em blocos** - blockchain armazena dados em "blocos" interligados, formando uma cadeia cronológica e imutável;
2. **Variedade de dados** - pode armazenar diferentes tipos de dados, como transações financeiras, registros médicos, informações de propriedade intelectual e resultados de análises;
3. **Registro imutável** - uma vez que um bloco é adicionado à blockchain, as informações nele contidas não podem ser alteradas ou excluídas, garantindo a integridade dos dados;
4. **Rastreamento de transações** - possível rastrear a origem e o histórico de qualquer dado ou transação registrada na blockchain, facilitando auditorias e investigações;
5. **Criptografia** - para proteger os dados armazenados, garantindo a confidencialidade e a integridade das informações;
6. **Assinatura digital** - cada usuário possui uma chave privada que garante a autenticidade das transações e impede fraudes;
7. **Consenso distribuído** - a validação das transações é realizada por múltiplos nós na rede, tornando a blockchain resistente a ataques e falhas;
8. **Sem autoridade central** - a blockchain não depende de uma autoridade central para gerenciar as transações, o que aumenta a resiliência e a resistência à censura;
9. **Rede distribuída** - os dados são armazenados em múltiplos nós na rede, evitando um ponto único de falha;
10. **Contratos inteligentes** - permitem a automatização de processos e a execução de acordos de forma autônoma e segura, sem a necessidade de intermediários;
11. **Gerenciamento de identidade** - facilita a gestão de identidades digitais de forma segura e descentralizada.

Em relação aos requistos, a solução deve permitir que:

- sejam registrados os dados dos equipamentos (método padrão-ouro) e dos *kits* de análise ou outros dispositivos de análise a serem validados;
- seja garantida a imutabilidade dos dados armazenados na blockchain, impedindo qualquer modificação ou exclusão não autorizada;
- cada dado gerado na análise (data, hora, identificação da amostra, método utilizado, resultados e analista responsável) fique registrado em um bloco da cadeia;

- seja feita a implementação do mecanismos de criptografia para proteger os dados confidenciais;
- sejam gerados relatórios e laudos e que seja viabilizada auditorias eficientes;
- seja possível a rastreabilidade da cadeia de custódia (coleta da amostra, todos os procedimentos analíticos até o resultado final);
- seja possível a identificar casos de resultados duvidosos, facilitando a identificação da origem do problema;
- o sistema seja descentralizado: credibilidade, troca ágil de informações e evitar ataques e perda de dados
- seja possível o compartilhamento seguro entre laboratórios e instituições envolvidas (nacionais e internacionais) mantendo o sigilo de informações sensíveis;
- seja possível identificar falhas no processo de coleta de amostras e de análise.

A utilização da plataforma de rastreabilidade e dos *kits* de análise permanecerá inalterada em relação ao uso atual, como descrito anteriormente. Destaca-se que os *kits* são de operação simples e acessível a qualquer usuário, desde que siga as instruções fornecidas na embalagem. A revelação da cor ocorre em poucos minutos, e os resultados finais — os teores das substâncias identificadas nas amostras — são obtidos mediante o envio das imagens via WhatsApp ao suporte técnico da empresa.

A introdução da nova solução não modifica essa rotina operacional. A principal inovação está no registro dos dados em blockchain, garantindo integridade, rastreabilidade e certificação dos resultados. Para o usuário final, a experiência permanece a mesma, mas agora os resultados da análise química estarão devidamente certificados, validados pelos elos da cadeia produtiva e disponíveis para compartilhamento com os órgãos competentes e responsáveis pela aceitação das informações.

Além de aumentar a confiança nos dados, a implementação da blockchain possibilitará à empresa expandir sua oferta de serviços e alcançar novos segmentos de clientes, sem impactar significativamente a experiência do usuário atual.

Como ambiente de desenvolvimento da aplicação estão sendo utilizados os laboratórios da própria empresa e de parceiros (INMETRO) com o *testbed* provido pelo Projeto Ilíada.

4. Documentação e Códigos fonte das aplicações

4.1 Códigos fonte das aplicações

Nesta seção, serão incluídos os códigos fontes das aplicações descritas neste relatório. Seu conteúdo será incluído na versão final deste relatório, em função das aplicações ainda estarem em desenvolvimento.

4.2 Documentação associada às aplicações

Esta seção conterá os *links* ou referências para documentação associada, como manuais de usuário, guias técnicos, e outros documentos relevantes de cada uma das aplicações descritas neste relatório. Seu conteúdo será incluído na versão final deste relatório, em função de as aplicações ainda estarem em desenvolvimento.

5. Análise do desempenho das aplicações

5.1 KPIs relacionados ao funcionamento das aplicações

Nesta seção, serão descritos os Indicadores de desempenho (Key Performance Indicator - KPIs) adotados para avaliar o funcionamento das aplicações apresentadas neste relatório. Seu conteúdo será incluído na versão final deste relatório, em função das aplicações ainda estarem em desenvolvimento.

5.2 Método de coleta e análise de métricas de desempenho

Nesta seção, será explicado o método de coleta das métricas de desempenho e uma análise sobre os resultados. Seu conteúdo será incluído na versão final deste relatório, em função das aplicações ainda estarem em desenvolvimento.

6. Testes de conformidade com os requisitos definidos

Os testes de conformidade são necessários para se avaliar o desempenho e a aderência aos requisitos definidos, assegurando sua qualidade e confiabilidade, ou seja, certificar que a aplicação funciona conforme o esperado. Seu conteúdo será incluído na versão final deste relatório, uma vez que as aplicações ainda estão em desenvolvimento.

6.1 Descrição dos testes realizados nas aplicações

Esta seção será elaborada após a conclusão do desenvolvimento das aplicações, atualmente em andamento, e seu conteúdo será incluído na versão final deste relatório, em função das aplicações ainda estarem em desenvolvimento.

6.2 Resultados dos testes e problemas identificados

Esta seção conterá os **resultados dos testes** realizados para a validação da plataforma e será elaborada após a conclusão do desenvolvimento das aplicações, atualmente em andamento, **incluindo possíveis problemas identificados e soluções adotadas**. Seu conteúdo será incluído na versão final deste relatório, em função das aplicações ainda estarem em desenvolvimento.

7. Aspectos relativos à segurança das aplicações

Nesta seção, serão relatados os aspectos relativos à segurança das aplicações, incluindo as medidas que foram implementadas com esse objetivo, as vulnerabilidades identificadas e as ações adotadas para mitigá-las. O seu conteúdo será incluído na versão final deste relatório, assim que for finalizado o desenvolvimento das aplicações.

7.1 Medidas de segurança implementadas nas aplicações

Esta seção será elaborada após a conclusão do desenvolvimento das aplicações, atualmente em andamento, e seu conteúdo será incluído na versão final deste relatório, em função das aplicações ainda estarem em desenvolvimento.

7.2 Vulnerabilidades identificadas e medidas para mitigá-las

Esta seção será elaborada após a conclusão do desenvolvimento das aplicações, atualmente em andamento, e seu conteúdo será incluído na versão final deste relatório, em função das aplicações ainda estarem em desenvolvimento.

8. Desafios e obstáculos no desenvolvimento

Nesta seção, são detalhadas as dificuldades técnicas ou barreiras encontradas ao longo do processo de desenvolvimento das aplicações, bem como as estratégias para superá-las.

Como seu conteúdo depende da conclusão do desenvolvimento das aplicações, ainda em curso, seu conteúdo será incluído na versão final deste relatório.

8.1 Identificação e descrição dos desafios técnicos ou obstáculos enfrentados

Esta seção será elaborada após a conclusão do desenvolvimento das aplicações, atualmente em andamento, e seu conteúdo será incluído na versão final deste relatório.

8.2 Estratégias adotadas para superar os desafios

Esta seção será elaborada após a conclusão do desenvolvimento das aplicações, atualmente em andamento, e seu conteúdo será incluído na versão final deste relatório.

9. Inovação tecnológica, impacto e benefícios das aplicações

Nesta seção, serão avaliadas e discutidas as inovações tecnológicas incorporadas nas aplicações desenvolvidas e destacadas as tecnologias emergentes ou abordagens pioneiras adotadas. Além disso, avalia-se o impacto das aplicações no contexto para o

qual foram desenvolvidas e os benefícios alcançados. Por fim, destacam-se potenciais melhorias futuras nas aplicações.

Como seu conteúdo depende da conclusão do desenvolvimento das aplicações, ainda em curso, seu conteúdo será incluído na versão final deste relatório.

9.1 Discussão sobre inovações tecnológicas incorporadas

Esta seção será elaborada após a conclusão do desenvolvimento das aplicações, atualmente em andamento, e seu conteúdo será incluído na versão final deste relatório.

9.2 Tecnologias emergentes ou abordagens pioneiras utilizadas

Esta seção será elaborada após a conclusão do desenvolvimento das aplicações, atualmente em andamento, e seu conteúdo será incluído na versão final deste relatório.

9.3 Avaliação do impacto das aplicações no contexto de uso

Esta seção será elaborada após a conclusão do desenvolvimento das aplicações, atualmente em andamento, e seu conteúdo será incluído na versão final deste relatório.

9.4 Benefícios alcançados e potenciais melhorias futuras

Esta seção será elaborada após a conclusão do desenvolvimento das aplicações, atualmente em andamento, e seu conteúdo será incluído na versão final deste relatório.

10. Conclusões e recomendações

Nesta seção, serão apresentadas as conclusões decorrentes do desenvolvimento das aplicações e as recomendações para otimizações futuras ou expansões. Seu conteúdo será incluído na versão final deste relatório, uma vez que as aplicações ainda estão sendo desenvolvidas.

11. Referências bibliográficas

[1] ERC-721 **Padrão de token não-fungível**. Disponível em: <https://ethereum.org/pt-br/developers/docs/standards/tokens/erc-721/>. Acesso em: 30 abr. 2025.

[2] GS1 Global Traceability Standard. Disponível em: <https://www.gs1.org/standards/traceability>. Acesso em: 30 abr. 2025.

[3] ISO 22005:2007. **Traceability in the feed and food chain**. Disponível em: <https://www.iso.org/standard/36297.html>. Acesso em: 30 abr. 2025.

[4] SO 14064:2006. **Greenhouse gases**. Disponível em: <https://www.iso.org/standard/38381.html>. Acesso em: 30 abr. 2025.

[5] BRASIL. Lei nº 13.964 de 24 de dezembro de 2019. **Aperfeiçoa a legislação penal e processual penal**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm>. Acesso em: 30 abr. 2025.

[6] GIOVA, G. **Improving chain of custody in forensic investigation of electronic digital systems**. IJCSNS International Journal of Computer Science and Network Security, v. 11, nº.1, p.1, jan.2011. Disponível em: <http://paper.ijcsns.org/07_book/201101/20110101.pdf>. Acesso em: 30 abr. 2025.

[7] ABNT NBR ISO/IEC 27037. **Diretrizes para identificação, coleta, aquisição e preservação de evidência digital**. Disponível em: <https://www.jusbrasil.com.br/artigos/norma-iso-27037-2013/2233729951>. Acesso em: 30 abr. 2025.

[8] BRASIL. Lei nº 13.675 de 11 de junho de 2018. **Institui o Sistema Único de Segurança Pública e cria a Política Nacional de Segurança Pública e Defesa Social**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm>. Acesso em: 30 abr. 2025.

[9] WIERENGA, K.; WINTER, S.; WOLNIEWICZ, T.. **The eduroam Architecture for Network Roaming (RFC 7593)**. 2015. Disponível em: <https://www.rfc-editor.org/rfc/rfc7593.html>. Acesso em: 30 abr. 2025.

[10] LI, Chunlei et al. **Trustroam: A novel blockchain-based cross-domain authentication scheme for wi-fi access**. Wireless Algorithms, Systems, and Applications: 14th International Conference, WASA 2019. 2019. p. 149-161.

[11] MetaBlox Labs. **Roam: Decentralized OpenRoaming WiFi Networks**. 2023. Disponível em: <https://weroam.xyz/whitepaper>. Acesso em: 30 abr. 2025.

[12] Ahmed, Farooq et al. **UniRoam: An Anonymous and Accountable Authentication Scheme for Cross-Domain Access**. IEEE 2020 International Conference on Networking and Network Applications (NaNA), Haikou City, China,2020, pp. 198-205.

[13] Ahmed, Farooq; Hussain, Syeda. **A Privacy-Preserving Cross-domain Network Access Services Using Sovrin Identifier**. IEEE 2021 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 2021, pp. 30-37.

[14] WINDLEY, P. **How Sovrin Works – A Technical Guide from the Sovrin Foundation**. 2016. Disponível em <https://sovrin.org/wp-content/uploads/2018/03/How-Sovrin-Works.pdf>. Acesso em: 30 abr. 2025.

[15] Aggarwal, Shubhani, and Neeraj Kumar. **Hyperledger. Advances in computers**. Vol. 121. Elsevier, 2021. pp. 323-343.

[16] Palamà, Ivan et al. . **Computer Communications 212** (2023): pp. 129-140.

[17] IBGE. **Censo agropecuário 2017**. Disponível em: <https://www.ibge.gov.br/estatisticas/economicas/agricultura-e-pecuaria/21814-2017-censo-agropecuario.html>. Acesso em: 30 abr. 2025.

[18] BRASIL. Instrução Normativa Conjunta - INC nº 2, de 7 de Fevereiro de 2018. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/29152630/do1-2018-02-08-instrucao-normativa-conjunta-inc-n-2-de-7-de-fevereiro-de-2018-2915259.>. Acesso em: 30 abr. 2025.

[19] PRORAF. **Programa de Rastreabilidade dos Produtos da Agricultura Familiar**. Disponível em: <https://proraf.com.br>. Acesso em: 30 abr. 2025.

[20] Rio Grande do Sul (RS). Decreto nº 55.515, de 30 de setembro 2020. **Institui Programa Produtos PREMIUM/RS, no âmbito das ações voltadas à inovação e à pesquisa científica e tecnológica**. Disponível em: <https://leisestaduais.com.br/rs/decreto-n-55515-2020-rio-grande-do-sul-institui-programa-produtos-premium-rs-no-ambito-das-acoes-voltadas-a-inovacao-e-a-pesquisa-cientifica-e-tecnologica>. Acesso em: 30 abr. 2025.

[21] Diploma Digital. **Ministério da Educação**. Disponível em: <http://portal.mec.gov.br/diplomadigital/>. Acesso em: 30 abr. 2025.

[22] Jornada do Estudante. **Ministério da Educação**. Disponível em: <https://www.gov.br/mec/pt-br/jornadadoestudante>. Acesso em: 30 abr. 2025.

[23] Censo da Educação Superior. **Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira**, 2023. Disponível em: <https://www.gov.br/inep/pt-br/areas-de-atuacao/pesquisas-estatisticas-e-indicadores/censo-da-educacao-superior/resultados>. Acesso em: 30 abr. 2025.

[24] BRASIL. Lei nº 12.305, de 2 de agosto de 2010. **Institui a Política Nacional de Resíduos Sólidos; altera a Lei nº 9.605, de 12 de fevereiro de 1998; e dá outras providências**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12305.htm>. Acesso em: 30 abr. 2025.

12. Histórico de alterações do documento consolidado

Data de elaboração	Versão	Descrições das alterações realizadas
30/Abr/25	AA	Versão inicial com a apresentação dos projetos selecionados para serem desenvolvidos.

13. Execução e aprovação

Executado por:
Maria Silvina Medrano Ismael Mattos Andrade Ávila
Aprovado por: Andreza Ferraresso Lona Faro Gerente de Solução Gerência de Soluções Blockchain

Data da emissão: 30/abr/25

Este é um documento preliminar, portanto contém informações e dados que poderão sofrer alterações até a entrega do documento final.