PROJETO ILÍADA

Blockchain
em evolução.

Atividades de PD&I no Projeto ILÍADA

Descrição das Atividades

Atividade 6.3 - Gestão das bolsas de PD&I

Elaboração de chamadas e coordenação do processo de seleção

Atividade 2.2 - Pesquisa e Desenvolvimento em Escalabilidade, Segurança, Descentralização e Tecnologias Habilitadoras

Atividade 4.3 - Desenvolvimento de Aplicações Piloto

Coordenação das atividades de PD&I desenvolvidas por grupos de trabalho e Startups

- Grupos de Pesquisa: oferta de bolsas de PD&I através do programa de bolsas da RNP
- Startups: Contratação através de prestação de serviços especializados para desenvolvimento de PoCs

Grupos de Trabalho selecionados para evolução de plataformas

Grupo de Trabalho	Instituições envolvidas
Pesquisa e Desenvolvimento em soluções para viabilizar a evolução de tecnologias e implementação de novas funcionalidades para testbed	Grupos de pesquisa de Universidades/Institutos
Pesquisa e Desenvolvimento em aplicações de blockchain em áreas selecionadas	Grupos de pesquisa de Universidades/Institutos
Desenvolvimento de Provas de Conceito para avaliação de viabilidade de implantação de blockchain em diversos setores da sociedade	Startups

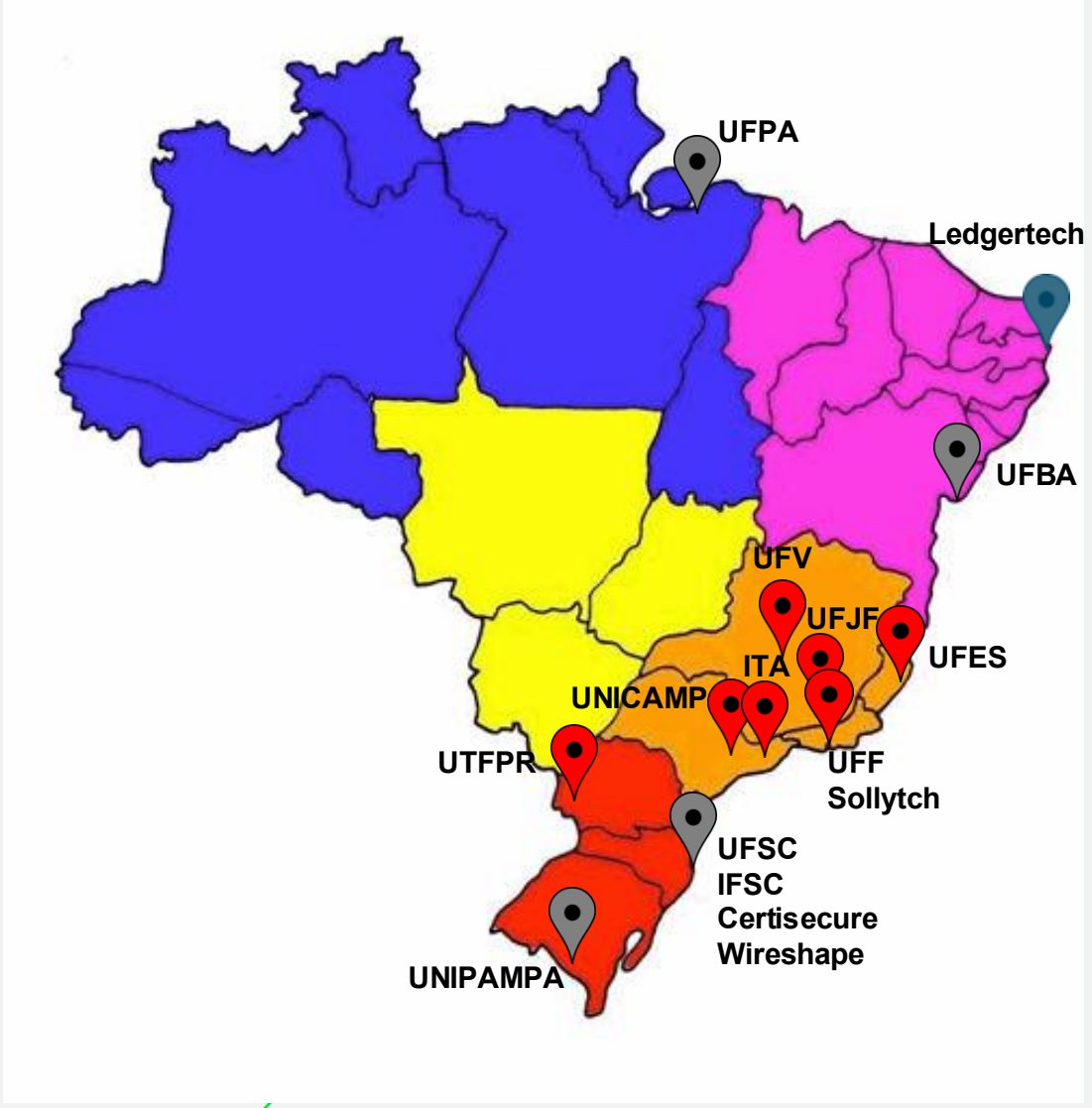
Ações de Pesquisa, Desenvolvimento e Inovação

13 Grupos de trabalho em execução

- 8 GTs selecionados em 2024 para desenvolvimento de soluções para evoluir plataformas de blockchain existentes
- 5 GTs para desenvolvimento de aplicações em setores estratégicos para demonstração do valor da adoção da tecnologia blockchain

4 Startups

- Desenvolvimento de PoCs para evoluir soluções existentes com o uso de blockchain e demonstrar valor de adoção da tecnologia de maneira aplicada ao mercado



Grupos de Trabalho selecionados para evolução de plataformas

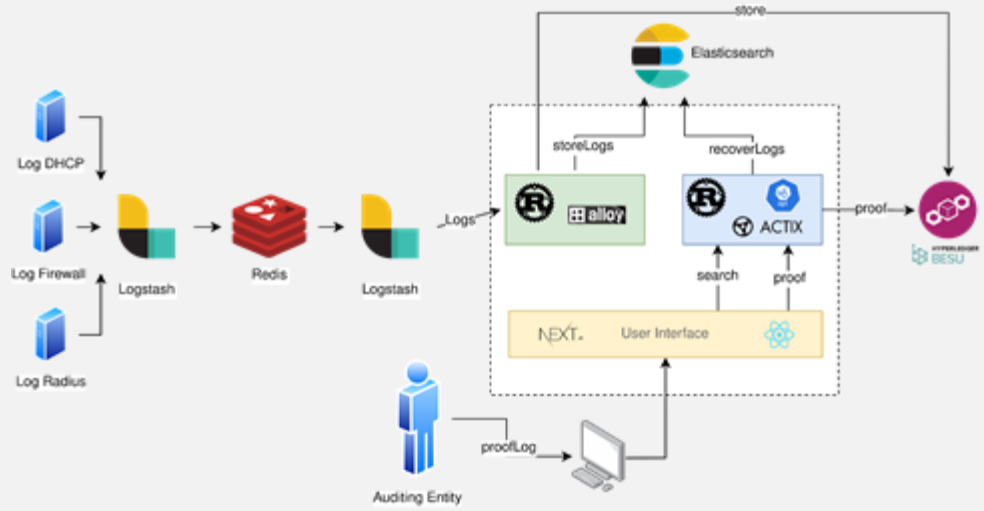
Grupo de Trabalho	Coordenador	Instituição
Audita: Auditoria Transparente em Redes usando Blockchains	Magnos Martinello	UFES
BBPQ: Benchmark de Blockchain Pós-Quântica	Alexandre Augusto Giron	UTFPR
DroneChain-UTM: Blockchain for Drone Traffic Management	Lourenço Alves Pereira Júnior	ITA
Inter: Grupo de Trabalho em Interoperabilidade de Blockchains	Alex Borges Vieira	UFJF
Padlock: Garantindo Privacidade e Proteção de Dados Pessoais Usando Aprendizado e Desaprendendo de Máquina em cima de uma Solução de Blockchain de Camada 2	Antonio Augusto de Aragão Rocha	UFF
PIDDF: Desenvolvimento de uma Plataforma de Identidade Digital Descentralizada com autenticação Federada	Diogo Menezes Ferrazani Mattos	UFF
SBS: Soluções para Blockchains Seguras	Marco Aurelio Amaral Henriques	UNICAMP
SmartSeg: Grupo de Trabalho em Segurança de Contratos Inteligentes	José Augusto Miranda Nacif	UFV

GT-Audita

PoP ES
PONTO DE PRESENÇA
DA RNP ESPÍRITO SANTO

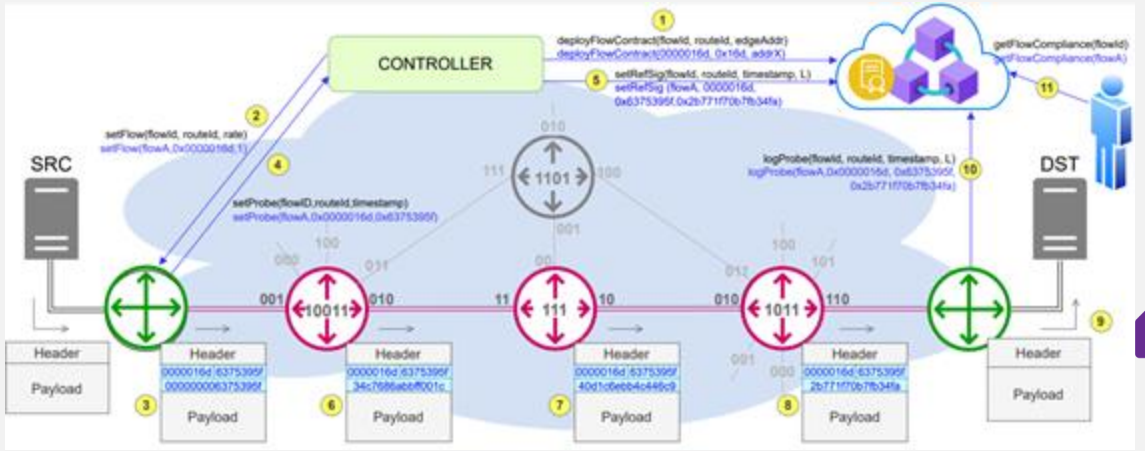
Sistema de "*provas-de-conexão*" baseadas em blockchain

- Registro criptográfico que atesta a relação entre dispositivo e atividade na rede
- Combina informações de múltiplas fontes (Firewall, DHCP, Radius)
- Estabelece vínculo verificável de integridade de uma informação



Modelo de "prova-de-trânsito" para auditoria de caminhos

- Integração da blockchain com uma rede ciente de caminho (PathSec) por meio da assinatura criptográfica salto a salto
- Demonstração em ambiente emulado bmv2/mininet integrado com Ethereum



Blockchain em evolução.

GT-BBPQ

Desafio: atualizar criptografia em blockchains

- Algoritmos de criptografia não são “negociados” como em um protocolo (e.g., TLS), Nodos distribuídos, Blockchains persistentes e imutáveis
- Recomendar melhores escolhas de PQC - Conformidade, Escalabilidade, etc.
- Disponibilizar implementação para a comunidade
- Experimentar em Estudos de Caso

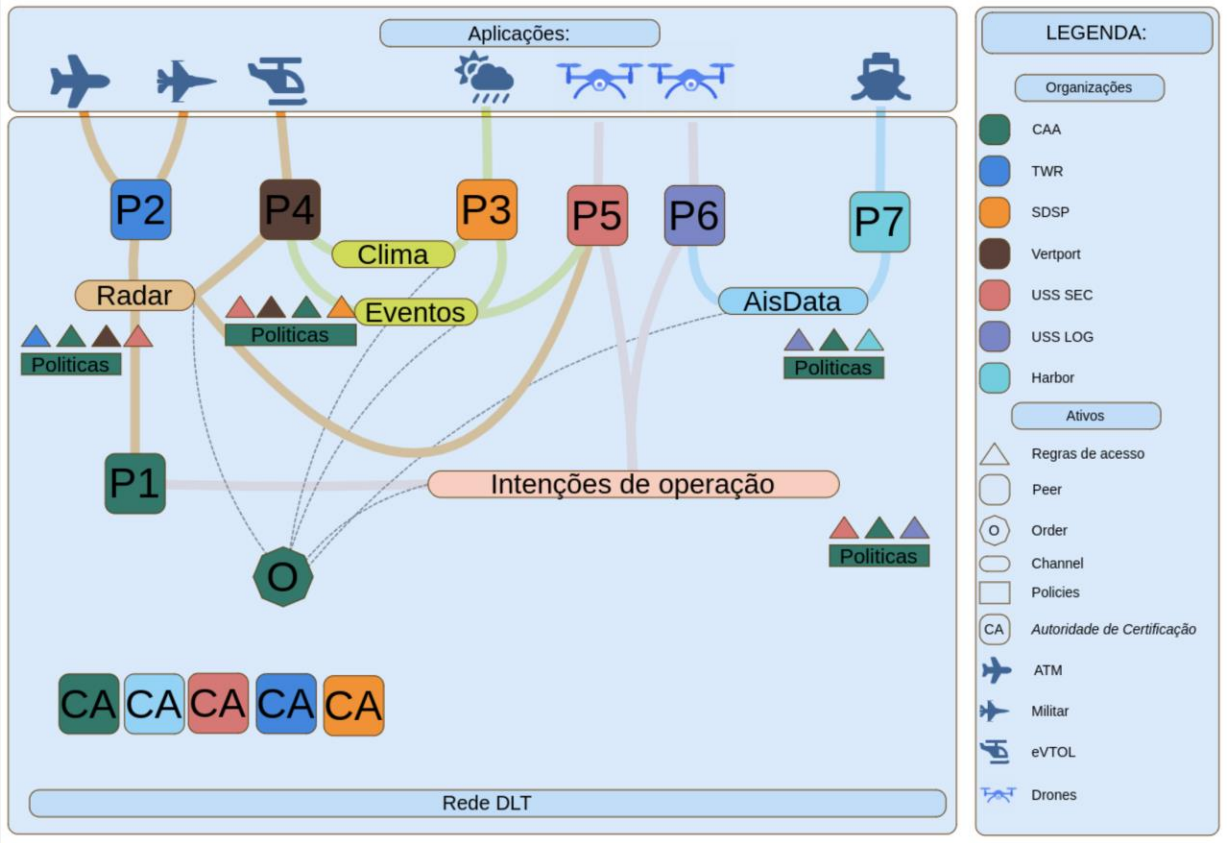
GT-DroneChain-UTM

Propor uma arquitetura descentralizada baseada em blockchain para tráfego de drones

- Solução atual (InterUSS) enfrenta limitações em confiabilidade e integridade
- Concorrência entre provedores
- Regulamentação no setor
- Autorização prévia para realização da operação
- Aumentar transparência, auditabilidade e segurança nas operações UTM

Integrar provedores, reguladores e operadores em consórcio permissionado

Estar em conformidade com as diretrizes do setor

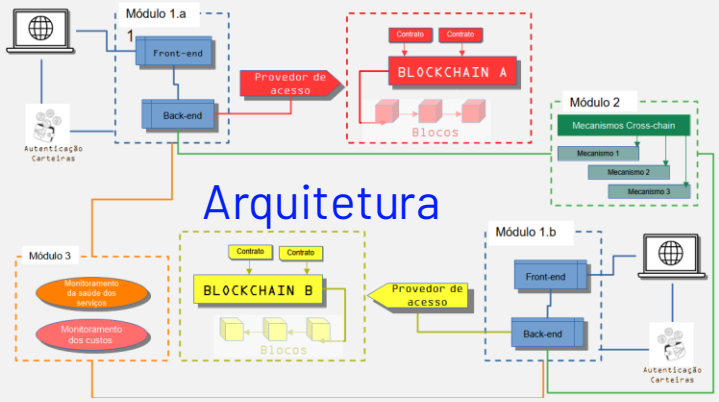


Blockchain em evolução.

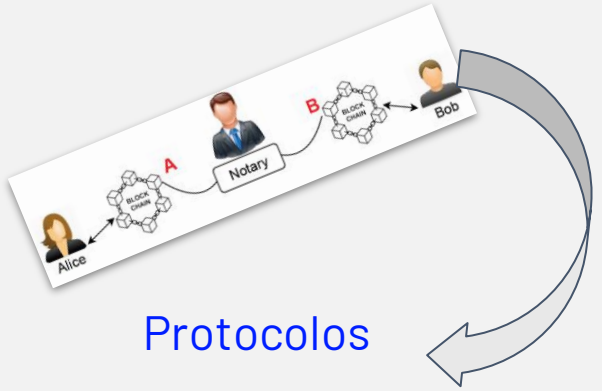
GT-Inter

Interoperabilidade entre blockchains

- Implementação de mecanismos de interoperabilidade direta
- Utilização de Cacti para incorporar novos mecanismos

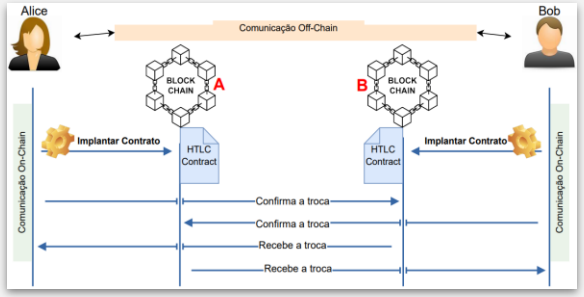


Arquitetura

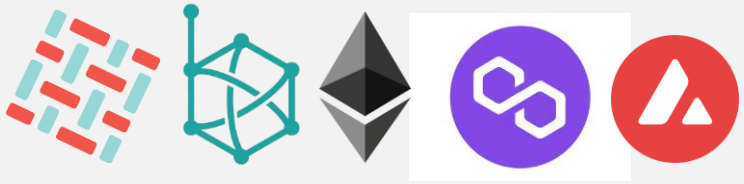


Protocolos

Hash Time Lock Contract(HTLC)



Redes



Blockchain em evolução.

GT-Padlock

Desenvolvimento de uma interface (API) de integração ao projeto Iliada de uma das principais soluções de Blockchain de camada 2 existentes, a Cartesi

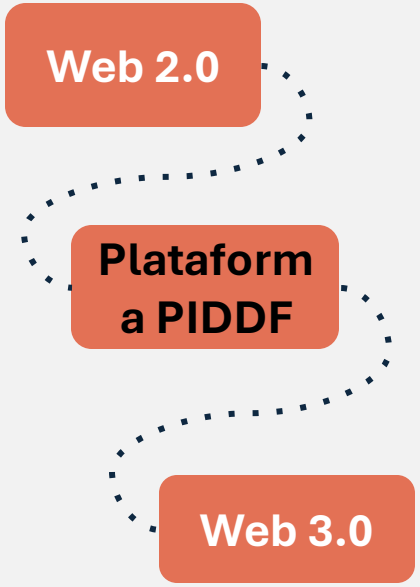
Implementações de algoritmos de DM dentro de máquinas Cartesi, que são executados na forma de contratos inteligentes de camada 2, à partir de chamadas da Blockchain principal do projeto Iliada

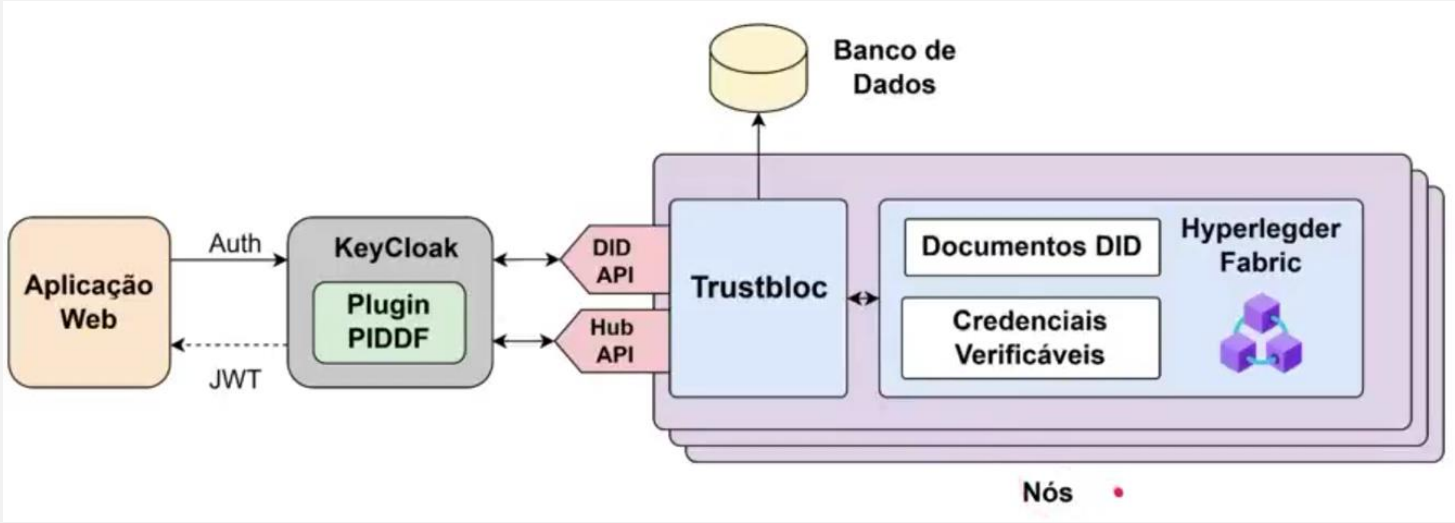
Desenvolvimento de uma Prova de Conceito (PoC) de DApp que faz uso do arcabouço como solução para o uso de modelos de AM, garantindo conformidade às leis de proteção de dados, com a remoção dos dados e esquecimento por parte dos modelos, de forma confiável através da segurança da Blockchain e sendo escalável com a execução em camada 2

GT-PIDDF

Desenvolver uma plataforma de identidade digital descentralizada, segura e interoperável, permitindo

- Integração com mecanismos de autenticação federada
- Compatibilidade com sistemas e infraestruturas legados





Blockchain em evolução.

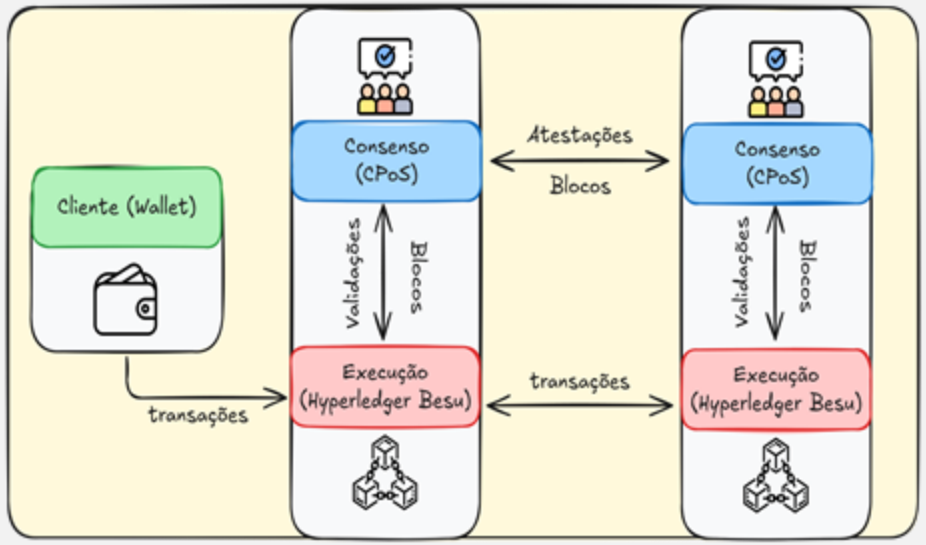
GT-SBS

Adaptação dos algoritmos criptográficos pós-quânticos ao código Besu (ML-DSA (NIST) e XMSS (IETF-RFC))

Avaliação de esquemas de agregação de múltiplas assinaturas pós-quânticas usando XMSS e STARKS

Avaliação de novo modelo de consenso

- Módulos com papeis distintos identificados
- Comunicações entre módulos mapeadas a fim de substituir apenas o elementos de consenso

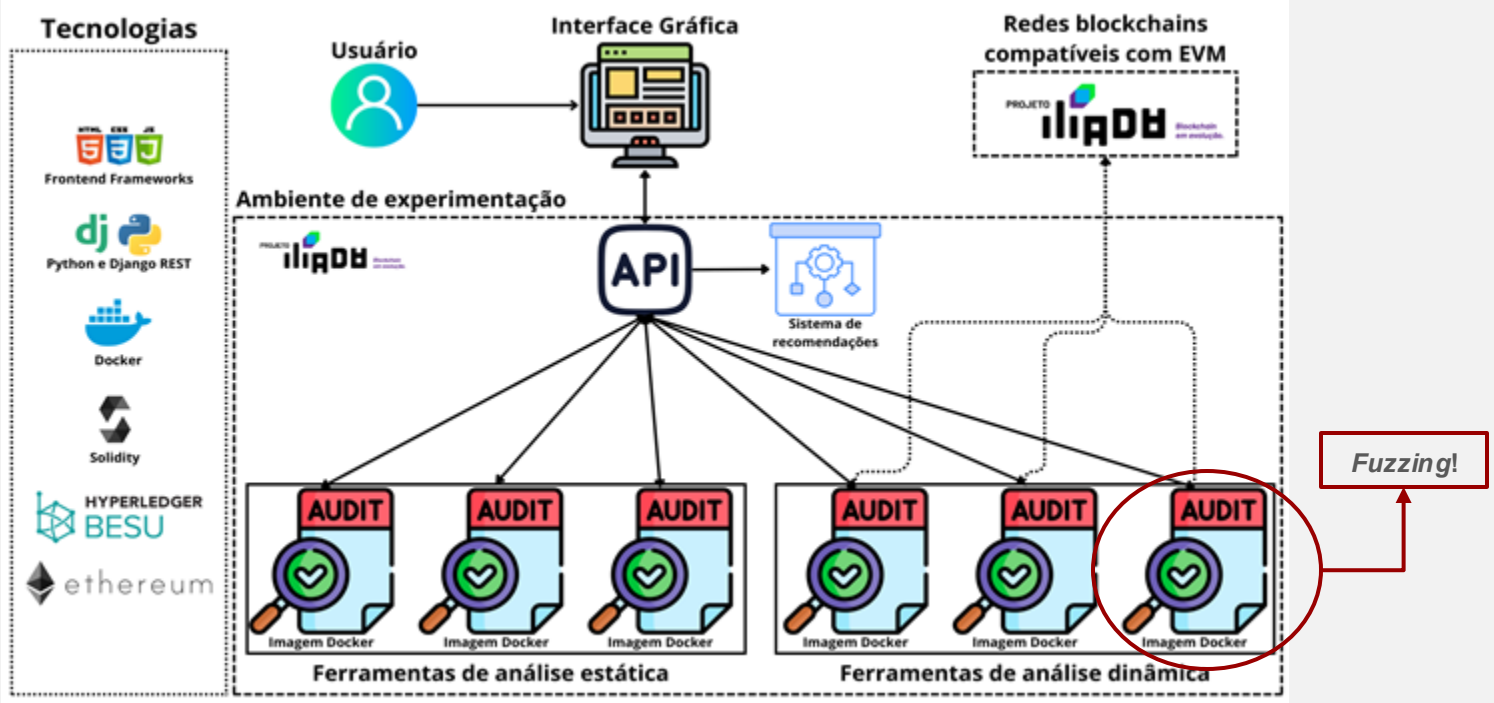


GT-SmartSeg

Ferramentas de análise de códigos para detecção de potenciais vulnerabilidades

Utilização de fuzzing para geração de novas versões e sugestão de correções

Foco em Solidity mas facilmente expansível para contratos inteligentes de outras redes, como a Hyperledger Fabric



Grupos de Trabalho selecionados para desenvolvimento de aplicações

Grupo de Trabalho	Coordenação	Instituição
GT-CarbonID - Plataforma de Tokenização de Créditos de Carbon	Leobino 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 Mansilha	UNIPAMPA
GT-SWARM - Self-sovereign Wi-Fi Authentication Roaming	Carla Westphall	UFSC
GT-ACREDITA: Aplicação de credenciais verificáveis para identidade digital e acesso	Emerson Mello	IFSC

GT-CarbonID

Uma plataforma descentralizada que apoia o gerenciamento do ciclo de vida dos créditos de carbono do mercado voluntário por meio de Identidades Digitais Descentralizadas

Facilitar a tokenização de créditos de carbono para o mercado voluntário através de serviços que gerenciem o ciclo de vida dos créditos de carbono, da submissão do projeto até a comercialização dos tokens, passando pelas certificações

- Gerenciamento do ciclo de vida dos créditos de carbono, da submissão do projeto até a comercialização dos tokens, passando pelas certificações
- Utilização de Identidades Digitais Descentralizadas (IDD) para assegurar autenticidade e rastreabilidade dos créditos
- Blockchain e Contratos inteligentes como garantia de rastreabilidade, imutabilidade, auditabilidade e conformidade regulatória

ChainID
PLATAFORMA DE GESTÃO
DE IDENTIDADE DIGITAL
DESCENTRALIZADA

Blockchain em evolução.

GT-Chainguard

Solução para implementar a cadeia de custódia de vestígios digitais utilizando a infraestrutura blockchain

- Gerenciamento desde a coleta até a utilização por diversos entes envolvidos
- Viabiliza a comprovação de que as evidências digitais foram mantidas íntegras e não adulteradas

Parceria com o MPPA, tendo um “cliente” real participando do processo

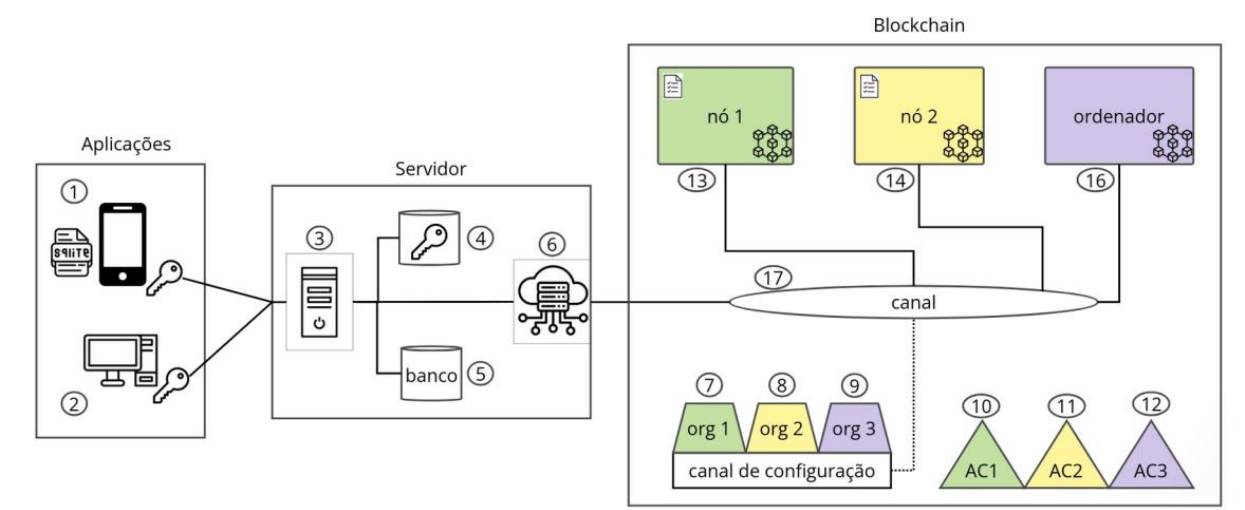


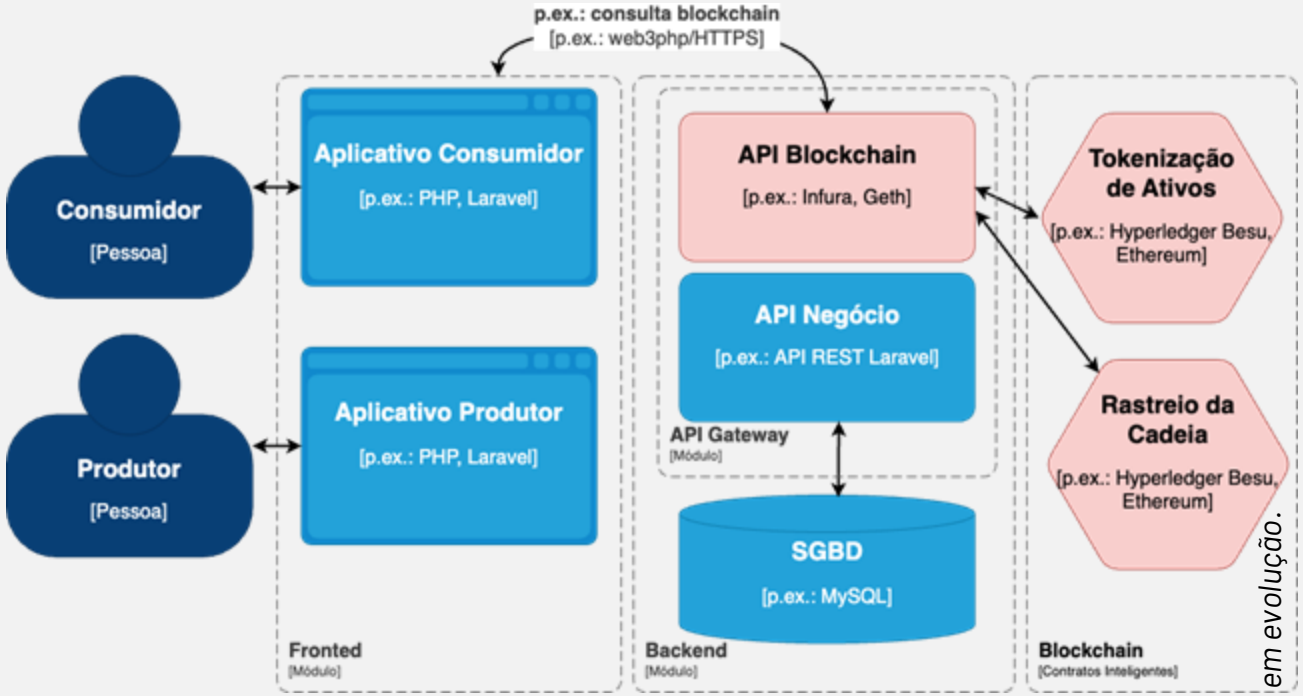
Figura 1: Arquitetura da solução ChainGuard.

GT-SmartAgroRaf

Solução de rastreamento de produtos da agricultura familiar baseada em blockchains e tokens em acordo com a INC 02/2018

- Projetar contratos inteligentes para rastreamento da agricultura familiar
- Implementar contratos inteligentes para agricultura familiar e integrar a uma interface acessível
- Avaliar blockchains para os contratos inteligentes da agricultura familiar

Solução Offchain já era desenvolvida através de um projeto de extensão junto a uma cooperativa da região

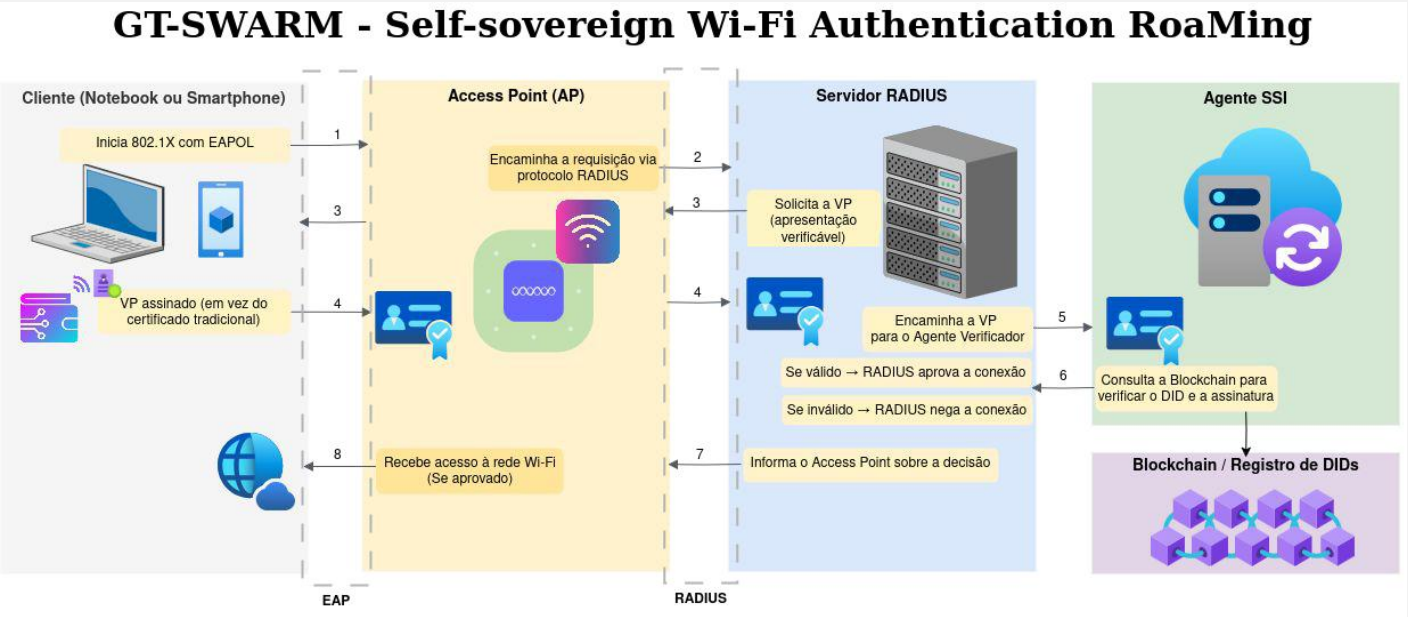


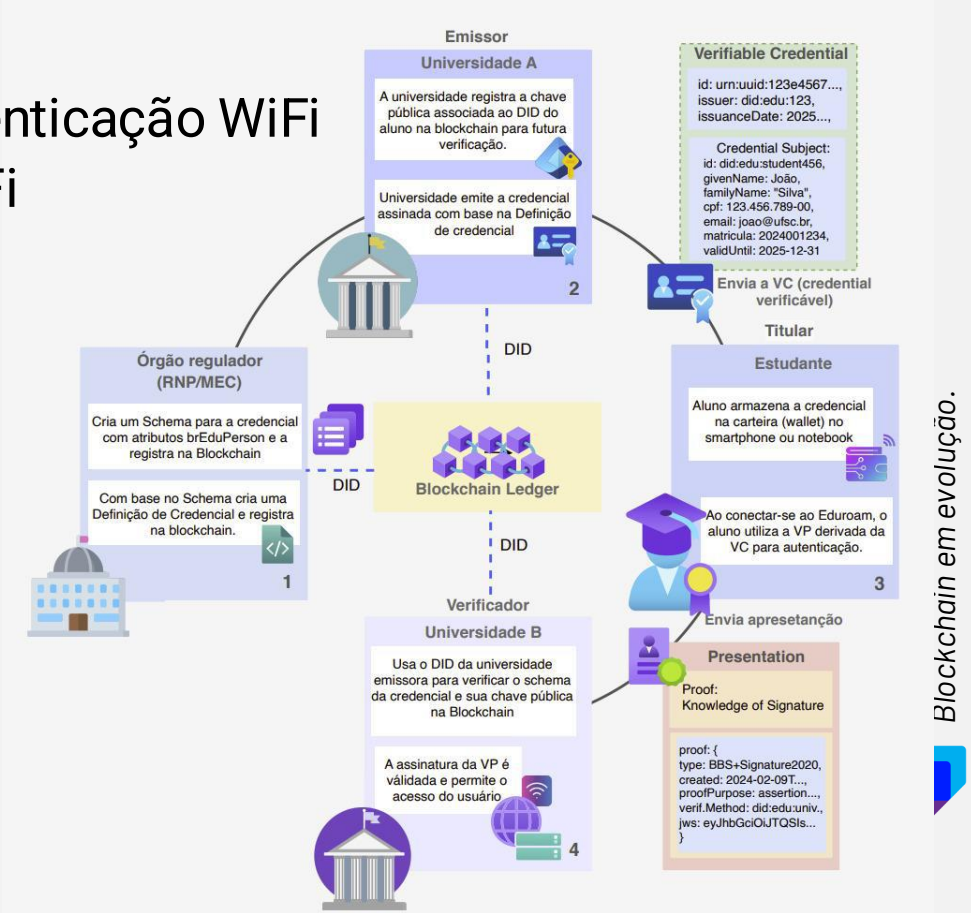
Blockchain em evolução.

GT-SWARM

Permitir autenticação de redes federadas (eduroam) com identificadores descentralizados (DDI) utilizando a infraestrutura padrão de facto do 802.1x

- Adequação do 802.1x ao modelo DID/VC/VDR
- Integrar de novos métodos EAP aos padrões de autenticação WiFi
- Plataforma de emissão de VC para autenticação WiFi





Blockchain em evolução.

GT-ACREDITA

Desenvolvimento de solução de identidade de digital descentralizada voltada para a comunidade acadêmica de computação

- Fazer com que o sistema de submissão de artigos JEMS3 da SBC adote o modelo de identidade digital descentralizada e passe a aceitar credenciais verificáveis como forma de autenticação de usuários
- A SBC será emissora e verificadora de credenciais verificáveis
- Ser uma aplicação de referência para o uso da tecnologia desenvolvida dentro do Projeto ILIADA
- Avaliar a viabilidade de inserção de novo modelo que posteriormente poderia ser adotado para outros sistemas/comunidades

Startups selecionadas para desenvolvimento de PoCs

Grupo de Trabalho	Startup	Instituição
Levery: Plataforma de Carteira Digital e Negociação de Ativos Tokenizados	Wireshape	Financeiro
DAIESEB - Digitalização do Acervo Acadêmico de Instituições de Ensino Superior com base em Inteligência Artificial e Blockchain.	Certisecure	Educacional
Modelagem de Aplicações Piloto Baseadas em NFTs de Ciclo Preditivo Utilizando a Plataforma Ledger NFT	Ledgertech	Informação e comunicação (inclui telecomunicações)
Rastreabilidade Química Inteligente: Agricultura na Era da Blockchain	Sollytch	Agropecuária

Resultados já alcançados

6 publicações durante o SBRC

- GT-Audita: Provendo Provas-de-Conexão para Auditabilidade de Acesso à Rede utilizando Blockchains
- GT-SmartSeg: Análise das Ferramentas de Detecção de Vulnerabilidades para Contratos Inteligentes de Blockchains EVM
- GT-Inter: Análise de Custo e Desempenho de Protocolos para Interoperabilidade de Tokens em Redes Blockchain
- GT-SmartAgro RAF: Smart Contracts para Rastreamento da Agricultura Familiar
- GT-Dronechain-UTM: SkyLedger: Test Bed para o Gerenciamento do Espaço Aéreo para Sistemas de Transportes Inteligentes: Requisitos, Desafios e Oportunidades
- GT-Dronechain-UTM: Benchmarking de Performance de Sistemas Distribuídos Aplicados à Mobilidade Aérea Urbana

Equipe

RNP	CPqD	Externos
Reinaldo Gomes	Antônio Matheus	85 bolsistas
Giovana Silva	Bruno Evaristo	17 instituições
Luiz Campos	Ismael Ávila	
Kauane Cordeiro	Maria Silvina	
Lucas Bondan		
Fiter	Jeffson	
Fernando Farias		
Estefânia		

Entregas Realizadas

Atividade 6.3 - Gestão das bolsas de PD&I

1. Relatório do Processo de Seleção e lista de dos bolsistas contratados na primeira chamada
2. Atualização de relatório com informações sobre o Processo de Seleção e lista de dos bolsistas da segunda chamada

Atividade 2.2 - Pesquisa e Desenvolvimento em Escalabilidade, Segurança, Descentralização e Tecnologias Habilitadoras

Relatório de Prospecção

Atividade 4.3 - Desenvolvimento de Aplicações Piloto

Relatório de planejamento do desenvolvimento e testes

Planejamento até o final do projeto – GTs Meta 2

Atividade 2.2 - Pesquisa e Desenvolvimento em Escalabilidade, Segurança, Descentralização e Tecnologias Habilitadoras

1. Códigos fonte dos artefatos desenvolvidos em repositório e documentação associada em acesso público;

2. Relatório Técnico com a descrição de acompanhamento das soluções desenvolvidas. Códigos fonte e documentação associada.

Planejamento de desenvolvimento e testes

Relatório final

Whitepaper

Transferência de tecnologia para absorver novas soluções desenvolvidas ano testbed

Planejamento até o final do projeto – GTs Meta 4

Atividade 4.3 - Desenvolvimento de Aplicações Piloto

1. Relatório com a descrição das aplicações desenvolvidas
2. Documentação e código fonte das aplicações desenvolvidas

Relatório Final de Acompanhamento

Whitepaper

Material de apoio para reuniões mensais de acompanhamento (slides, demonstrações, etc.)

Relatório de Planejamento

Relatório de Resultados

Atividade 6.3 - Gestão das bolsas de PD&I

Relatório final de atividades de cada bolsista

Desvios, Pendências e Pontos de Atenção que precisam de alinhamento

Desvios do planejamento inicial

Contratação de uma das startups atrasou devido a negociações de cláusulas do contrato

Ajuste na duração do contrato (8 meses) mantendo-se o escopo planejado

Perspectivas para o futuro

Evolução de soluções implementadas

- Auditoria de logs em ambiente mais diversos e com um conjunto maior de informações
- Verificação de vulnerabilidades utilizando LLMs e maior diversidade de versões de contratos
- Criptografia pós-quântica (Fabric e Besu)
- Gestão de Identidade
- Incentivo a produtização de aplicações

Maior interação com a comunidade e outras ações internacionais