



*Blockchain  
em evolução.*



## **Atividades de PD&I no Projeto ILÍADA**

Resultados do  
Grupos de Trabalho

## Atividades Envolvidas

---

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

Pesquisa e Desenvolvimento em soluções para viabilizar a evolução de tecnologias e implementação de novas funcionalidades para testbed

### **Atividade 4.3** - Desenvolvimento de Aplicações Piloto

Pesquisa e Desenvolvimento em aplicações de blockchain em áreas selecionadas

Desenvolvimento de Provas de Conceito para avaliação de viabilidade de implantação de blockchain em diferentes setores da economia

### **Atividade 5.3** – Desenvolvimento de Aplicações de IDD

Desenvolvimento e testes de aplicações de identidade digital descentralizada, tais como identidade digital de pessoas físicas, jurídicas ou coisas (IoT)

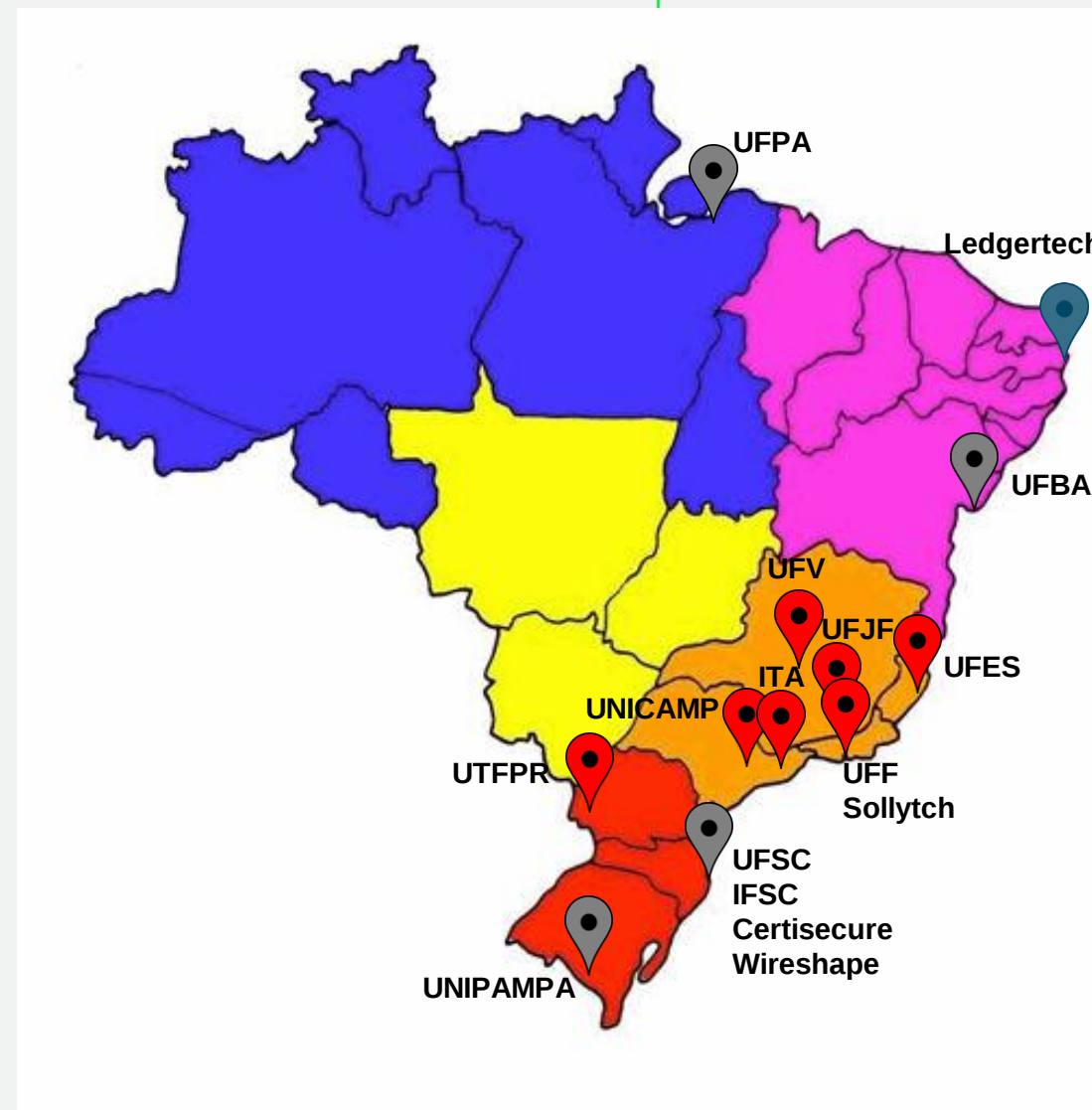
# Ações de Pesquisa, Desenvolvimento e Inovação

## 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                                                                                                                                           | Tópico de Pesquisa                                     | Instituição |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-------------|
| Audita: Auditoria Transparente em Redes usando Blockchains                                                                                                  | Auditabilidade e Transparência                         | UFES        |
| BBPQ: Benchmark de Blockchain Pós-Quântica                                                                                                                  | Criptografia Pós-Quântica                              | UTFPR       |
| DroneChain-UTM: Blockchain for Drone Traffic Management                                                                                                     | DLT para Gestão de Espaço aéreo                        | ITA         |
| Inter: Grupo de Trabalho em Interoperabilidade de Blockchains                                                                                               | Interoperabilidade entre blockchains                   | 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 | Privacidade e Auditabilidade                           | UFF         |
| PIDDF: Desenvolvimento de uma Plataforma de Identidade Digital Descentralizada com autenticação Federada                                                    | Identidade Digital Descentralizada                     | UFF         |
| SBS: Soluções para Blockchains Seguras                                                                                                                      | Criptografia Pós-Quântica                              | UNICAMP     |
| SmartSeg: Grupo de Trabalho em Segurança de Contratos Inteligentes                                                                                          | Avaliação de vulnerabilidade em contratos inteligentes | UFV         |

© 2006 The Authors



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

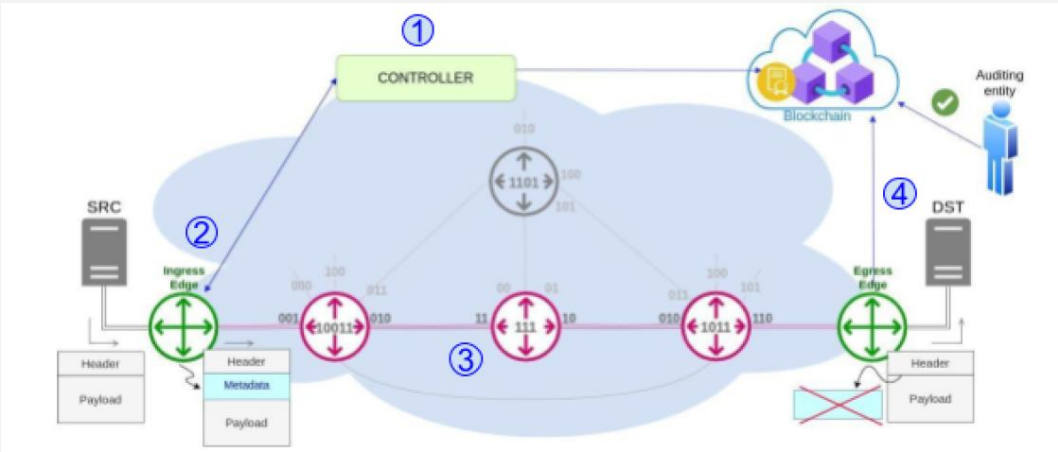
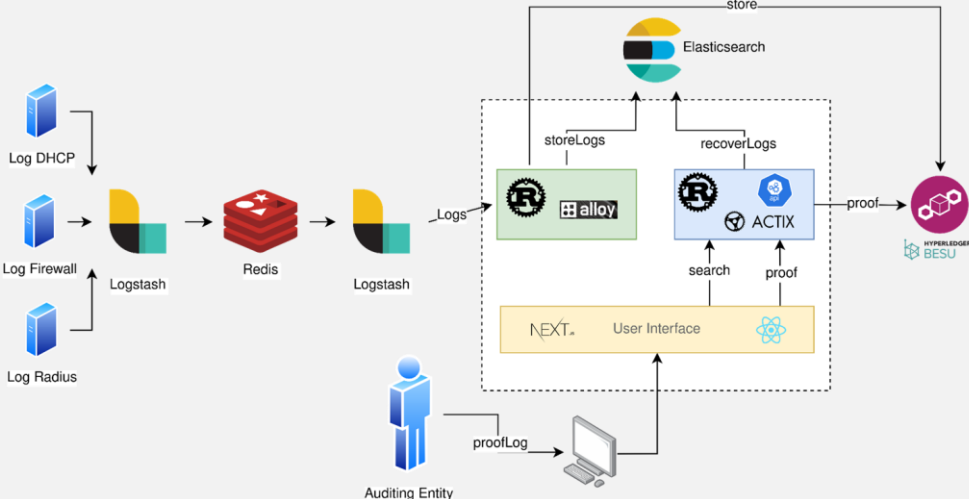
- Pipeline de logs (firewall, DHCP, RADIUS) com ingestão, normalização e indexação
- Interface gráfica para análise e validação de integridade dos registros e relação entre dispositivo e atividade na rede

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

- Monitoramento de rotas de pacotes com geração de provas criptográficas de caminho armazenados em blockchain

## Principais Resultados

- Integração entre infraestrutura tradicional de logs e blockchain possibilitando auditoria e responsabilização com dados auditáveis e íntegros
- Solução aplicável a segurança institucional e redes corporativas
- Escalabilidade para grandes volumes de logs

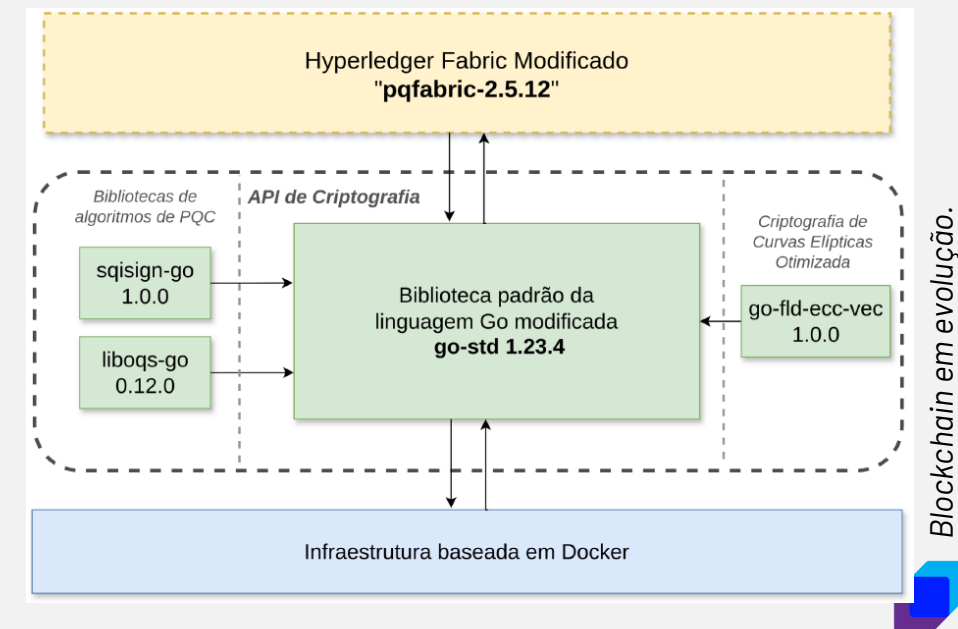


### Evolução do Hyperledger Fabric para suportar criptografia pós-quântica (PQC)

- Implementação de assinaturas híbridas (tradicional + PQC)
- Certificados digitais híbridos e infraestrutura baseada em containers
- Ambiente automatizado para testes e benchmarks de desempenho

### Principais Resultados

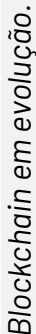
- Suporte a 32 variantes de algoritmos pós-quânticos
- Avaliação prática da migração para PQC em blockchains permissionadas
- Perfis de configuração para diferentes cenários (desempenho, conformidade, compactação)
- Contribuição para preparação antecipada contra ameaças quânticas
- Base para guias de adoção de PQC em blockchain



\_\_\_\_\_

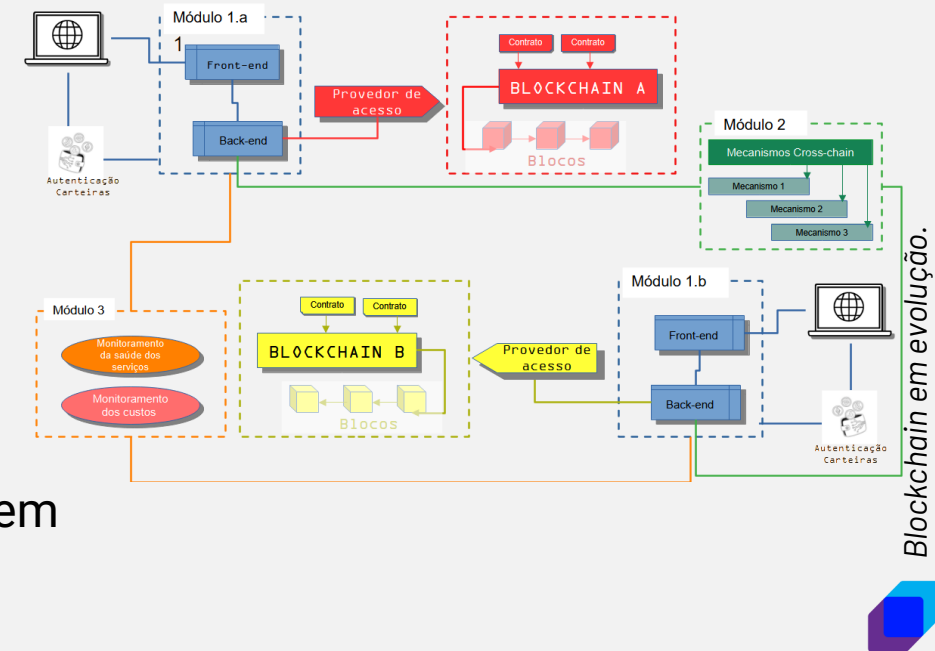
- Solução atual (InterUSS) enfrenta limitações em confiabilidade e integridade
- Registro de operações/eventos críticos de voo
- Tokenização de reservas de espaço aéreo
- Arquitetura para ambientes com múltiplos operadores e provedores

- Trilha de auditoria imutável para operações de drones
- Uso de geohashes para indexação eficiente do espaço aéreo
- Suporte à coordenação entre múltiplas organizações
- Comparação entre redes e distribuições diferentes (Fabric x Besu)



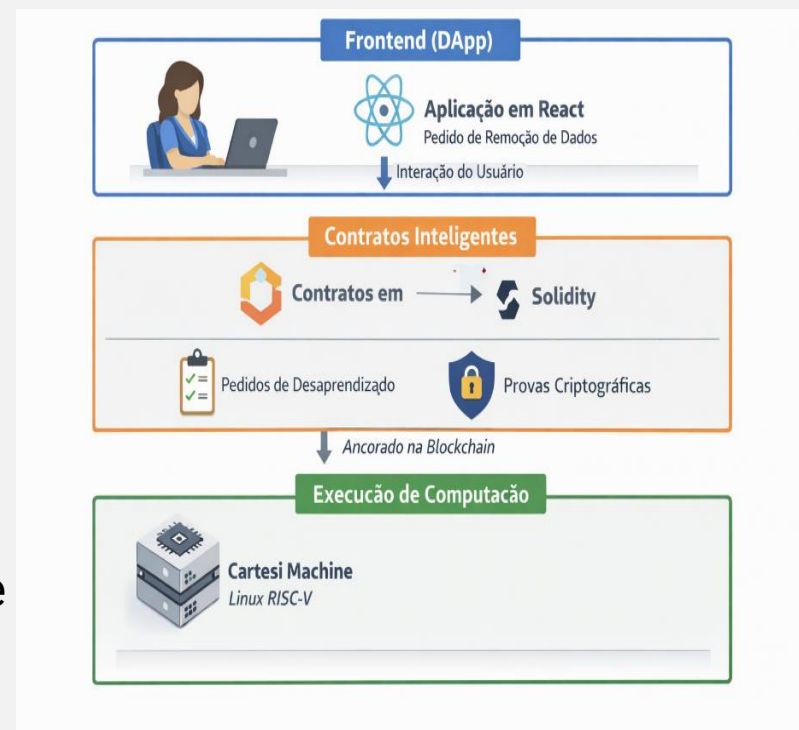
# GT-Inter

- Plataforma para interoperabilidade entre blockchains públicas e permissionadas
  - Avalanche Fuji, Polygon Amoy, Hyperledger Besu e Fabric
- Transferência segura de ativos digitais entre redes distintas
- Implementação de mecanismos de interoperabilidade
  - Notarial e HTLC (trocas atômicas)
- Principais Resultados
  - Suporte multi-rede (Avalanche, Polygon Besu e Fabric)
  - Transferências interchain com rastreabilidade completa
  - Avaliação de métricas operacionais (latência, custo de transação)
  - Demonstração prática de interoperabilidade blockchain em ambiente acadêmico
  - Arquitetura modular e escalável
  - Caso de uso: diplomas digitais como NFTs



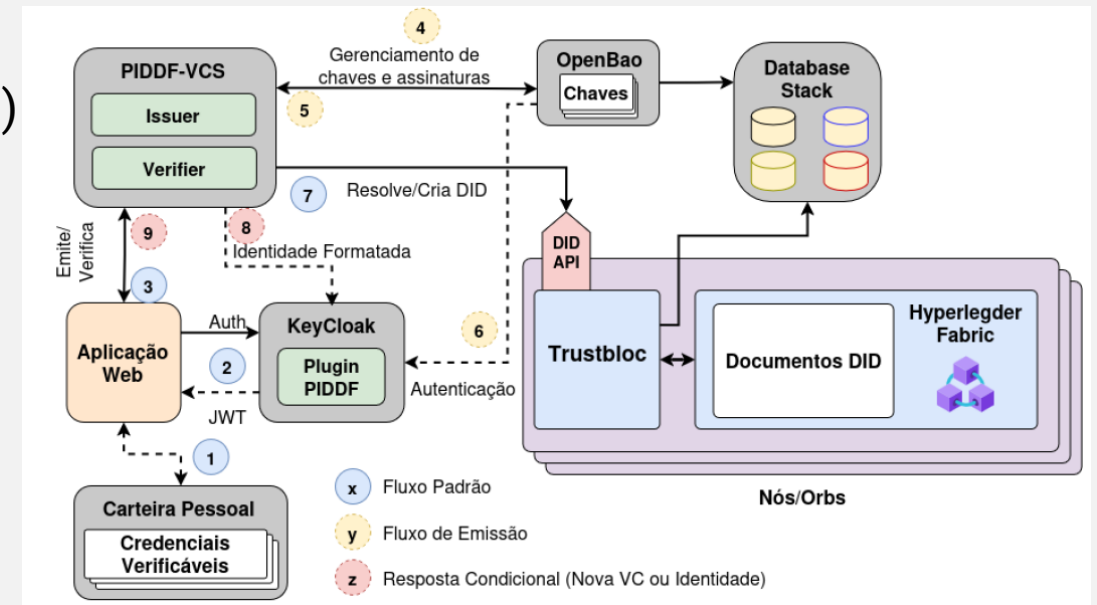
# GT-Padlock

- Framework de DApps com suporte a Desaprendizado de Máquina (Machine Unlearning)
- Registro de solicitações de remoção de dados em blockchain
- Execução dos algoritmos em camada escalável (Cartesi)
- Integração com contratos inteligentes e aplicações Web
- Principais Resultados
  - Implementação do direito ao esquecimento com rastreabilidade
  - Conformidade com legislações de proteção de dados (ex.: LGPD)
  - Execução escalável de algoritmos de ML fora da blockchain
  - Provas criptográficas de remoção de dados
  - Abordagem inovadora combinando IA, privacidade e blockchain



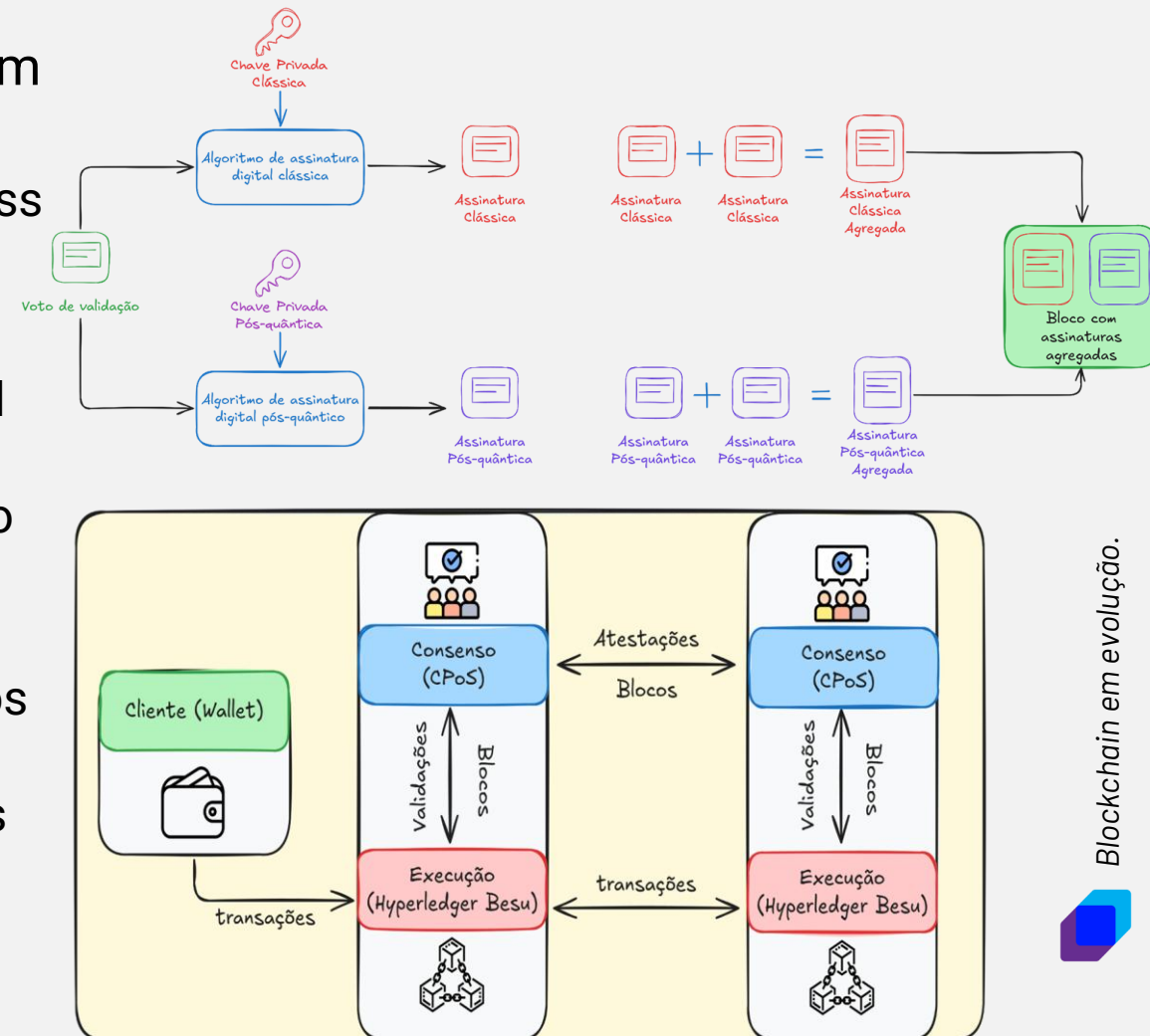
# GT-PIDDF

- Plataforma de Identidade Digital Descentralizada com autenticação federada
- Uso de DIDs e Credenciais verificáveis (VCs) integrados a sistemas Web 2.0
- Arquitetura modular com Keycloak, Hyperledger Fabric e TrustBloc
- Principais Resultados
  - Controle de identidade com o usuário
  - Interoperabilidade entre Web2 e Web3
  - Integração com padrões internacionais (W3C)
  - Segurança reforçada com gestão de segredos e blockchain
  - Base para novos modelos de gestão de identidade digital



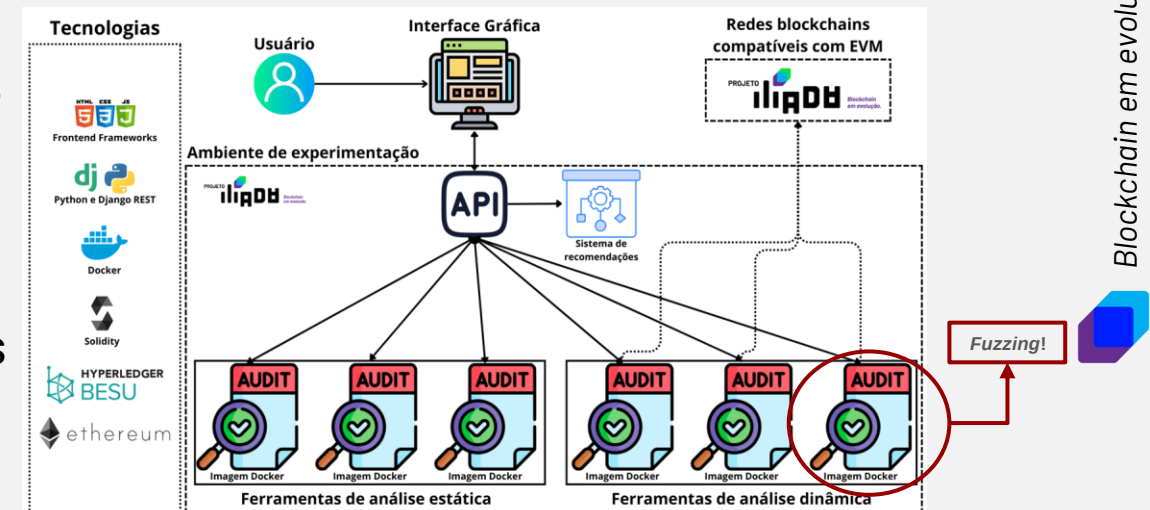
# GT-SBS

- Mecanismos de segurança blockchain com foco em
  - Assinaturas pós-quânticas híbridas
  - Novo algoritmo de consenso CPoS (Committeeless Proof of Stake)
- Principais Resultados e Diferenciais
  - Compatibilidade mantida com arquitetura original do Besu
  - Redução de dependência de comitês de validação
  - Sorteio criptográfico verificável para seleção de validadores
  - Maior robustez frente a ataques e cenários futuros de computação quântica
  - Arquitetura modular para evolução de algoritmos de consenso
  - Implementação compatível com redes baseadas em Ethereum (Hyperledger Besu)



# GT-SmartSeg

- Framework automatizado para auditoria de contratos inteligentes
  - Foco em Solidity mas facilmente expansível para contratos inteligentes de outras redes, como a Hyperledger Fabric
  - Integração de ferramentas (Slither, Mythril, ConFuzzius)
    - Análise estática, dinâmica e fuzzing para geração de novas versões e sugestão de correções
- Principais Resultados
  - Redução do esforço manual na auditoria de contratos Solidity
  - Geração automática de relatórios com classificação de vulnerabilidades
  - Normalização de resultados e recomendações de mitigação
  - Integração com padrões de segurança (CWE e EthTrust)
  - Escalabilidade e reprodutibilidade das análises



## 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

Arquitetura híbrida com componentes off-chain e registros imutáveis on-chain

- Motor de regras e workflow configurável para automatizar processos de certificação
- 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

Principais resultados

- Validação da viabilidade técnica da plataforma para o mercado de carbono
- Automação de etapas de submissão, validação e certificação de projetos
- Plataforma escalável e adaptável a diferentes metodologias e regulações

## 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
  - Registro de vestígios e evidências fotográficas
  - Lacres digitais e rastreabilidade completa
  - Gestão de processos e auditoria da cadeia de custódia.
- Viabiliza a comprovação de que as evidências digitais foram mantidas íntegras e não adulteradas

### Principais resultados

- Infraestrutura blockchain privada desenvolvida e validada para uso em segurança pública
- Digitalização de fluxos operacionais da cadeia de custódia
- Demonstração da viabilidade do uso de blockchain em processos legais e investigativos.

### Rastreabilidade da cadeia produtiva da agricultura familiar integrado a blockchain

- Solução Offchain já era desenvolvida através de um projeto de extensão junto a uma cooperativa da região
- Tokenização de ativos para rastrear origem e movimentação dos produtos
- Construção de contratos inteligentes para rastreamento da agricultura familiar (ERC 721 e 1155)

### Principais Resultados e Diferenciais

- Prova de conceito implementada e integrada no testbed
- Avaliação de custo e complexidade

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
- Criação do método EAP-DID para autenticação
- Plataforma de emissão/verificação e autenticação apoiada em VDRs armazenadas em blockchain (Identus/Cardano)

### Principais Resultados

- A criação e implementação do novo método EAP-DID provê encapsulamento de mensagens DIDCommv2 para realizar um fluxo completo de autenticação baseado em apresentações verificáveis (VP), mesmo antes da disponibilização de conectividade IP ao dispositivo cliente
- A implementação do protótipo validou os principais componentes

Prova de Conceito (PoC) para uso de Credenciais Verificáveis (VC) como fator de autenticação

Cenário demonstrativo: autenticação de alunos em sistema de biblioteca universitária

- Emissão de VC via sistema acadêmico (QR Code + carteira digital)
- Armazenamento em wallet do usuário
- Apresentação e verificação da credencial para acesso a serviços

Principais resultados

- Validação completa do fluxo (Emissão de VC, armazenamento em carteira digital, apresentação e verificação para autenticação)
- Implementação de políticas de verificação robustas (assinatura, expiração, revogação)
- Aderência a padrões internacionais em consolidação (W3C, OpenID)
- Estrutura preparada para futura integração com outros sistemas institucionais
- Experimentação com blockchain e abordagens sem blockchain

## Startups selecionadas para desenvolvimento de PoCs

| Grupo de Trabalho                                                                                                                | Startup     | Instituição                                        |
|----------------------------------------------------------------------------------------------------------------------------------|-------------|----------------------------------------------------|
| Leverly: 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                                       |

## Lições Aprendidas

---

Uso da infraestrutura para o desenvolvimento das soluções contribuiu para a evolução do testbed

Perfis de equipe e desenvolvimento de acordo com o objetivo da chamada

Gestão das equipes dos GTs foi um desafio

- Mudanças nas equipes de 9 dos 13 GTs
- Absorção dos profissionais pelo mercado

Necessidade de mais tempo para internalizar as implementações (infraestrutura)

Refinamento das áreas de interesse para aplicações pode potencializar a continuação do desenvolvimento

Startups tem aspectos bem distintos no acompanhamento e desenvolvimento

- Maturidade da empresa é um aspecto tão importante quando o domínio técnico

Divulgação através do Observatório levantou muito interesse da comunidade



BRASIL  
INSTITUTO  
NACIONAL DE  
EDUCAÇÃO

CPQD

RNIP

MINISTÉRIO DA  
EDUCAÇÃO, CULTURA  
E ESPORTE

GOVERNO FEDERAL  
BRASIL  
UNION & TECHNOLOGY