

26^o
Workshop
RNP

Resultados dos GTs de P&D em Blockchain – Projeto ILIADA

Reinaldo Gomes

Coordenador de P&D
Gerência de P&D em Cibersegurança – RNP

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

SBS - Soluções para Blockchains Seguras

Marco Aurélio Amaral Henriques
Unicamp/Professor
Reinado Gomes
RNP/Coordenador de P&D

Introdução

Segurança de blockchains depende de vários fatores

Segurança criptográfica:

Criptografia usada nas blockchains é vulnerável a ataques dos futuros computadores quânticos.

Adequar os protocolos de comunicação e de geração de blocos para sanar essa vulnerabilidade

Eficiência de mecanismos de consenso:

Consenso Proof-of-Stake usado em várias blockchains requer uma complexa gestão de comitês de validação de blocos.

Implementar outro mecanismo de consenso que não requeira a criação e gestão de comitês de validação de blocos.

Objetivos

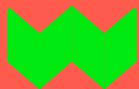
Aprimorar a segurança e eficiência das blockchains em duas frentes

Aumentar resistência a ataques de computadores quânticos

Implementar, testar e avaliar diferentes tipos de algoritmos de criptografia pós-quântica em blockchains Besu, buscando manter protocolos e características operacionais originais como desempenho, eficiência e confiabilidade.

Simplificar mecanismo de consenso sem perder segurança

Portar para blockchain Besu o novo mecanismo de consenso Committeeless Proof-of-Stake (CPoS) a fim de eliminar o uso de comitês de validação de blocos, simplificando o processamento por nó da rede e aumentando a eficiência sem perda de confiabilidade.



26

Workshop
RNP

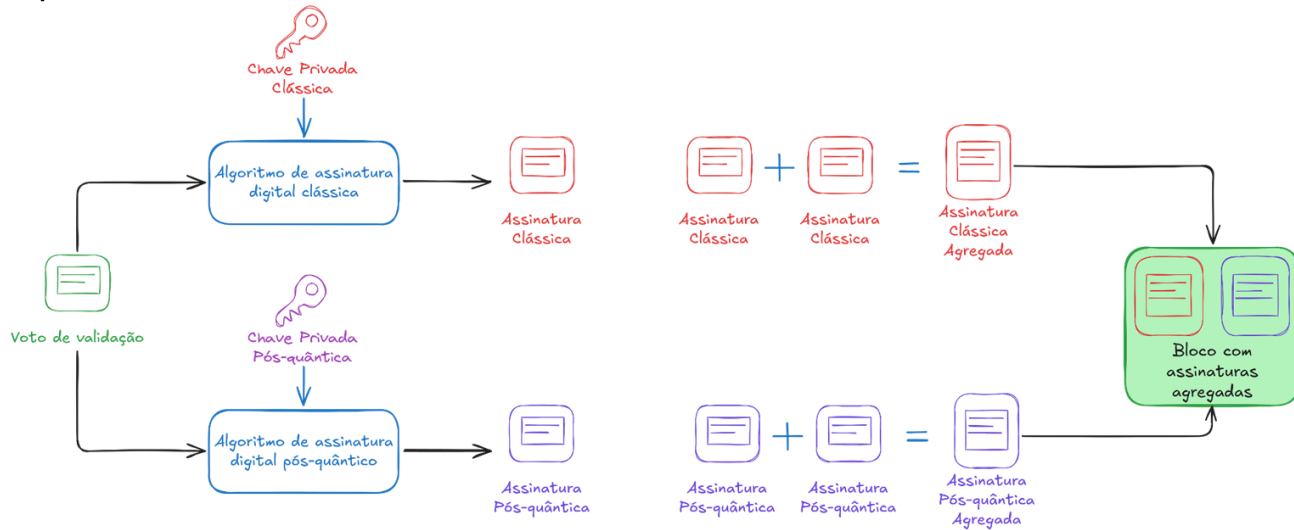
Onde o futuro
se encontra.

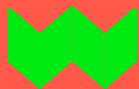
Resultados Preliminares

Adoção de Criptografia Pós-Quântica

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 em andamento





26

Workshop
RNP

Onde o futuro
se encontra.

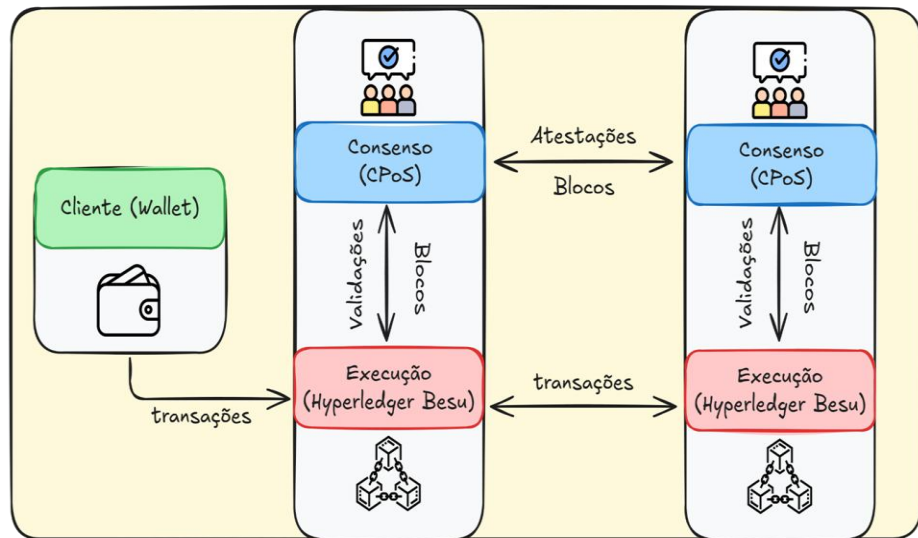
Resultados Preliminares

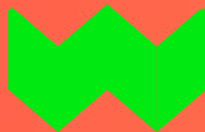
Esquema com troca do PoS pelo Committeless PoS

Módulos com papéis distintos identificados:
execução de transações (Besu) e consenso (Teku)

Comunicações entre
módulos mapeadas a fim
de substituir apenas o
elementos de consenso

Ajustes no CPoS para
adequá-lo à rede Besu





26

Workshop
RNP

***Onde o futuro
se encontra.***

OBRIGADO!

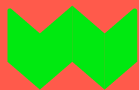
Marco Amaral Henriques
maah@unicamp.br

*Coord. do GT-SBS e do Grupo
de Pesquisa em Segurança
Aplicada ReGrAS da Unicamp*

GT-Padlock

Antônio "Guto" Rocha

UFF/Professor



26

Workshop
RNP

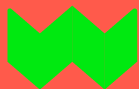
*Onde o futuro
se encontra.*

Problema Fundamental 1

Nos últimos anos, com o avanço crescente da presença da tecnologia na vida das pessoas, surge a necessidade de se discutir mecanismos legais que protejam a privacidade dos indivíduos

Questão fundamental que é colocada neste projeto é: como garantir que, modelos gerados através de técnicas de AM e Inteligência Artificial (IA), uma vez que tenham sido treinados com dados revogados, estejam em conformidade com a LGPD?

Nova subárea da IA chamada Desaprendizado de Máquina, que surge como uma necessidade para atender à legislação



26

Workshop
RNP

*Onde o futuro
se encontra.*

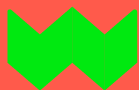
Problema Fundamental 2

Modelos de IA não estão necessariamente associados aos dados

Questão fundamental 2:

Como garantir que os algoritmos AM usados sejam de fato os declarados pela empresa com a posse dos dados do usuário?

Para responder positivamente esta questão, é preciso recorrer a outra solução tecnológica: Blockchain com Escalabilidade



26

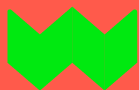
Workshop
RNP

*Onde o futuro
se encontra.*

GT-Padlock

Garantindo Privacidade e Proteção de Dados Pessoais Usando Aprendizado e Desaprendendo de Máquina em cima de uma Solução de Blockchain de Camada 2

- (i) desenvolvimento de uma interface (API) de integração ao projeto Iliada de uma das principais soluções de Blockchain de camada 2 existentes, a Cartesi;
- (ii) a 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; e,
- (iii) 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



26

Workshop
RNP

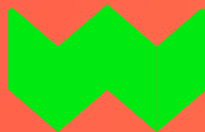
Onde o futuro
se encontra.

GT-Padlock

Garantindo Privacidade e Proteção de Dados Pessoais Usando Aprendizado e Desaprendendo de Máquina em cima de uma Solução de Blockchain de Camada 2

- (i) desenvolvimento de uma interface (API) de integração ao projeto Iliada de uma das principais soluções de Blockchain de camada 2 existentes, a Cartesi;
- (ii) 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; e,
- (iii) 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

- NitBus, NitBike ...



26

Workshop
RNP

*Onde o futuro
se encontra.*

OBRIGADO!

arochoa@ic.uff.br



MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

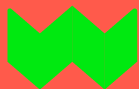
MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO



BBPQ – Benchmark de Blockchain Pós-Quântica

Alexandre Augusto Giron

UTFPR/Professor



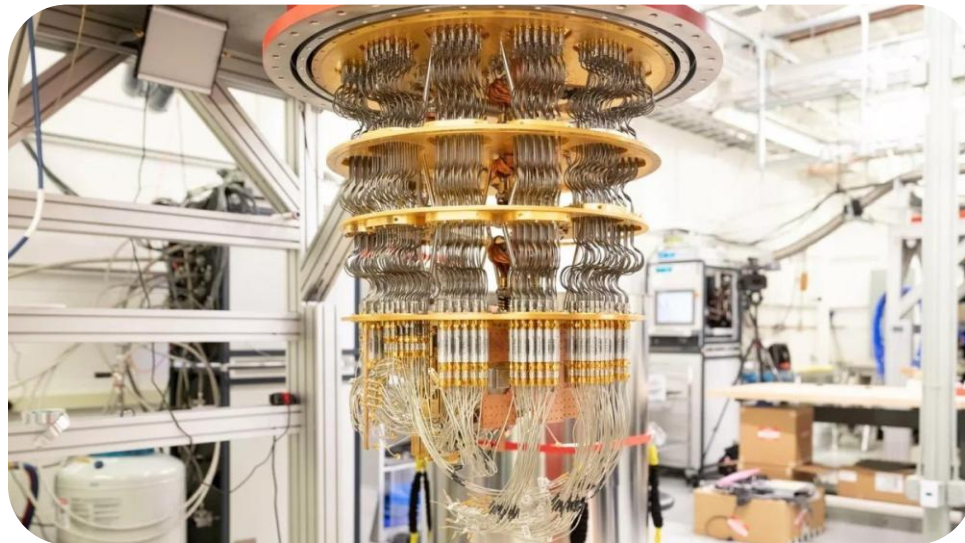
26

Workshop
RNP

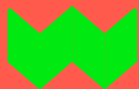
Onde o futuro
se encontra.

Introdução

Ameaça: Algoritmo Quântico de Peter Shor



- Criptografia de Chaves Públicas - Essencial para autenticação de transações em blockchains - **vulnerável!**
- Solução recomendada
 - Criptografia Pós-Quântica ("PQC")
- Desafio: atualizar criptografia em blockchains ->
 - Algoritmos de criptografia não são "negociados" como em um protocolo (e.g., TLS), Nós distribuídos, Blockchains persistentes e imutáveis



26

Workshop
RNP

Onde o futuro
se encontra.

Status atual do desenvolvimento

Integração de PQC em Hyperledger Fabric



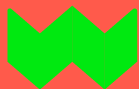
Integração de PQC
Híbrida para linguagem
Go (*go-std*)



Integração do
repositório *go-std*
em Fabric



Configuração e
Experimentação



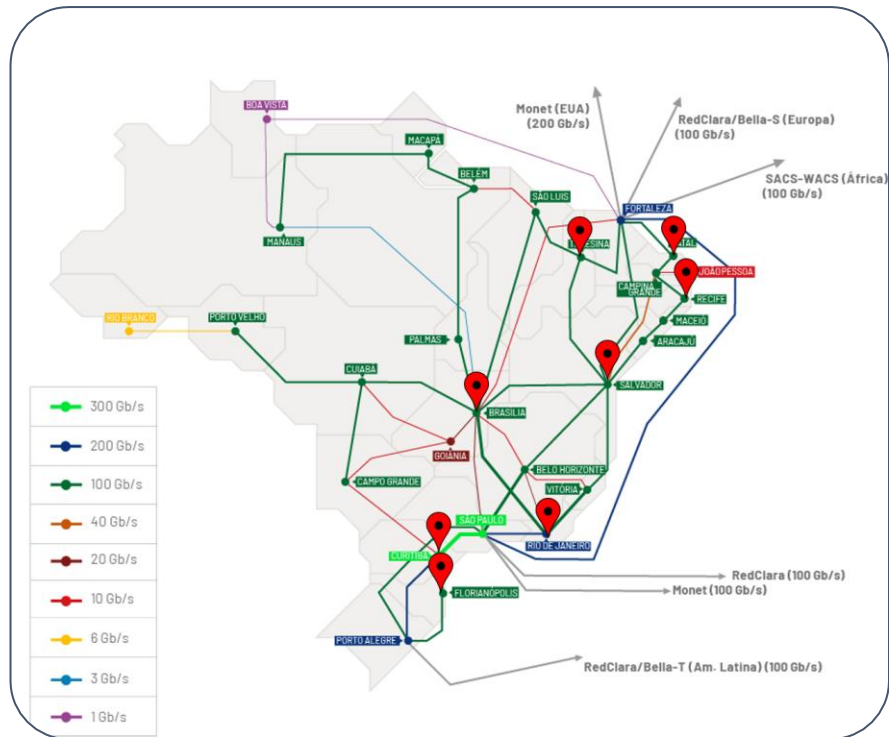
26

Workshop
RNP

Onde o futuro
se encontra.

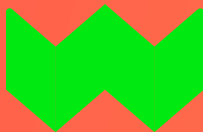
Resultados Esperados

- **Recomendar** melhores escolhas de PQC
 - Conformidade, Escalabilidade, etc.
- **Disponibilizar** implementação para a comunidade
- **Experimentar** em Estudos de Caso:



OBRIGADO PELA ATENÇÃO

alexandregiron@utfpr.edu.br



26

Workshop
RNP

*Onde o futuro
se encontra.*

UTFPR

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ



RNP

MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

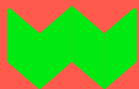


26[•]
Workshop
RNP

DroneChain-UTM - Blockchain for Drone Traffic Management

Lourenço Alves Pereira Junior

ITA/Professor



26

Workshop
RNP

Onde o futuro
se encontra.

Contexto e Motivação

Como lidar com as novas demandas de Mobilidade Aérea Avançada?

- Crescimento do uso de drones impõe desafios ao gerenciamento do espaço aéreo
- Provedores USS (*UAS Service Suppliers*) autorizam operações de voo
- Modelo brasileiro permite concorrência entre provedores
- Necessidade de sincronização e compartilhamento seguro de dados
- Solução atual (InterUSS) enfrenta limitações em confiabilidade e integridade

Objetivos

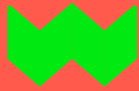
Estudar o desempenho de Blockchain para backend

- Propor uma arquitetura descentralizada baseada em blockchain
- Aumentar transparência, auditabilidade e segurança nas operações UTM
- Integrar provedores, reguladores e operadores em consórcio permissionado
- Estar em conformidade com as diretrizes do setor

Descrição da Solução

PLATAFORMA EDUCACIONAL PARA TREINAMENTO EM DEFESA

- Fase 1: Estudo e Benchmarking
 - Levantamento de oportunidades
 - Avaliação de frameworks Hyperledger Fabric
- Fase 2: Implementação e Testes
 - Desenvolvimento de arquitetura e contratos inteligentes
 - Integração com BR-UTM e execução de testes de carga



26

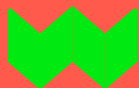
Workshop
RNP

*Onde o futuro
se encontra.*

Arquitetura

Backend

- Rede blockchain permissionada entre atores autorizados
- Ledger imutável com registros de voos e transações
- Substitui DSS tradicional por contratos inteligentes
- Permite tokenização e programação do espaço aéreo
- Interoperabilidade com soluções legadas do BR-UTM

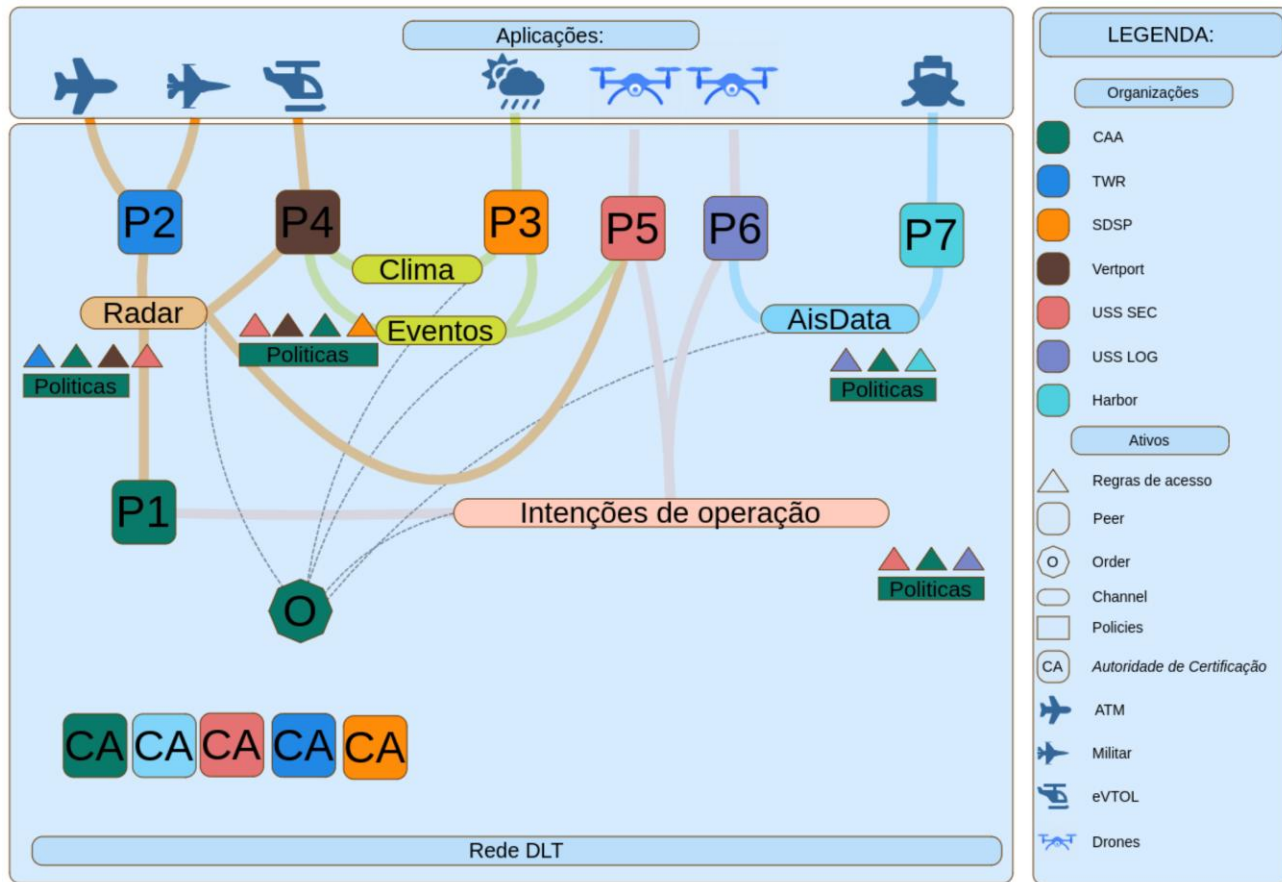


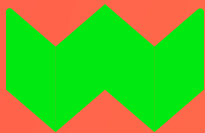
26

Workshop
RNP

Onde o futuro
se encontra.

Arquitetura





26

Workshop
RNP

*Onde o futuro
se encontra.*

OBRIGADO!

Lourenço Alves Pereira Júnior

ljp@ita.br



MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

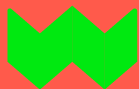
MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO



GT-SmartSeg - Segurança de Contratos Inteligentes

José Augusto Miranda Nacif

UFV/Professor

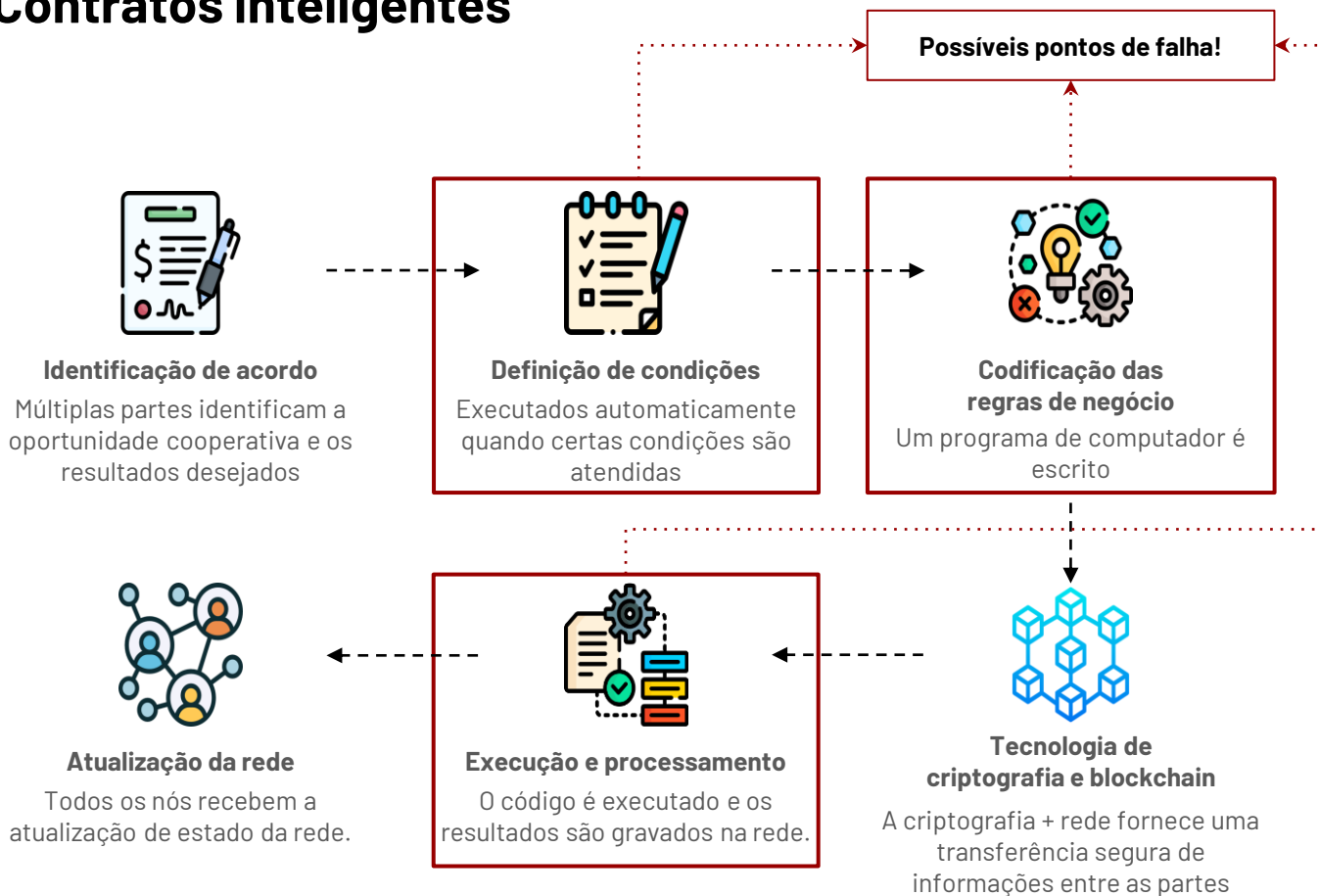


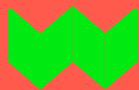
26

Workshop
RNP

Onde o futuro
se encontra.

Contratos Inteligentes





26

Workshop
RNP

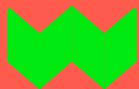
Onde o futuro
se encontra.

Objetivos

“O objetivo geral do GT é desenvolver um framework que facilite a execução automatizada de ferramentas de verificação em contratos inteligentes escritos na linguagem de programação Solidity”

Benefícios

- Redução de custos de auditorias convencionais
- Disponibilização de ferramentas de análise de contratos que demandam grande esforço de instalação e configuração
- Ambiente de experimentação modular
- Sugestões de boas práticas de codificação

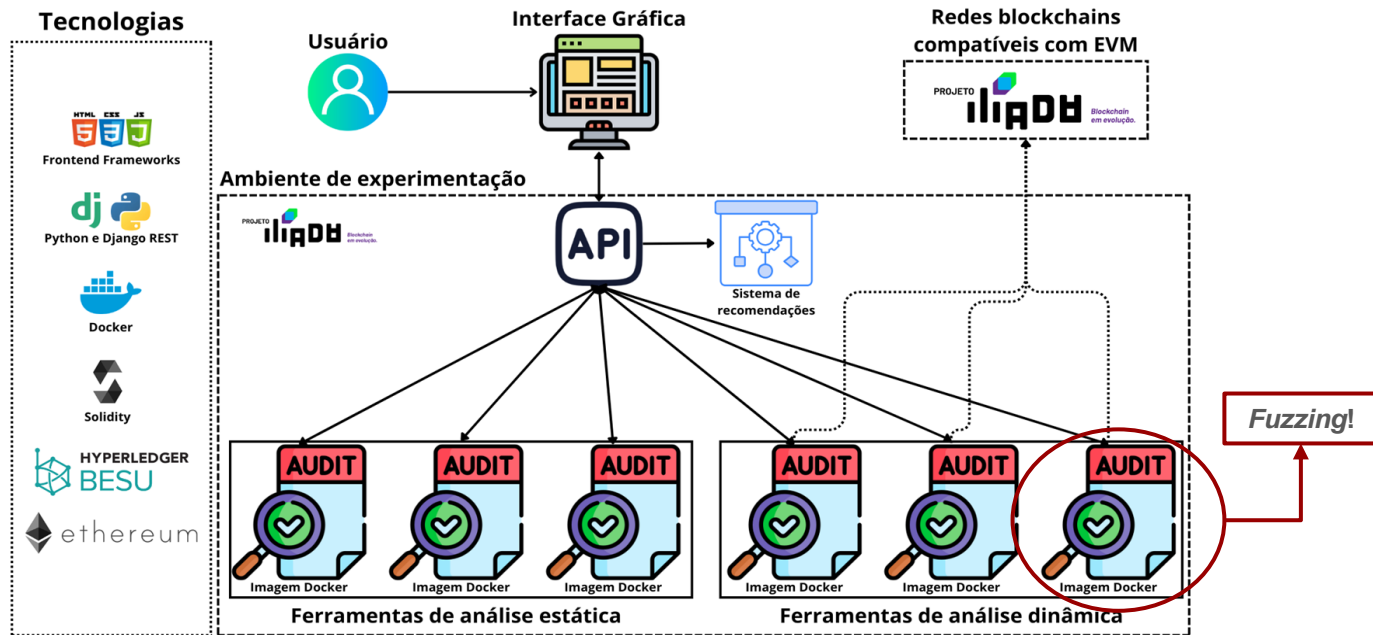


26

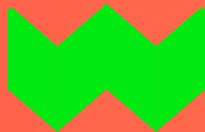
Workshop
RNP

Onde o futuro
se encontra.

Arquitetura proposta



- Incorporado aos Testbeds atuais da RNP, contribuindo para avanços no ecossistema ILIADA
- Foco em Solidity mas facilmente expansível para contratos inteligentes de outras redes, como a Hyperledger Fabric



26

Workshop
RNP

*Onde o futuro
se encontra.*

OBRIGADO!

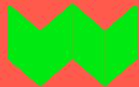
jnacif@ufv.br

GT-Inter

Interoperabilidade de Blockchains

Alex Borges/Ronan Dutra

UFJF/UFV



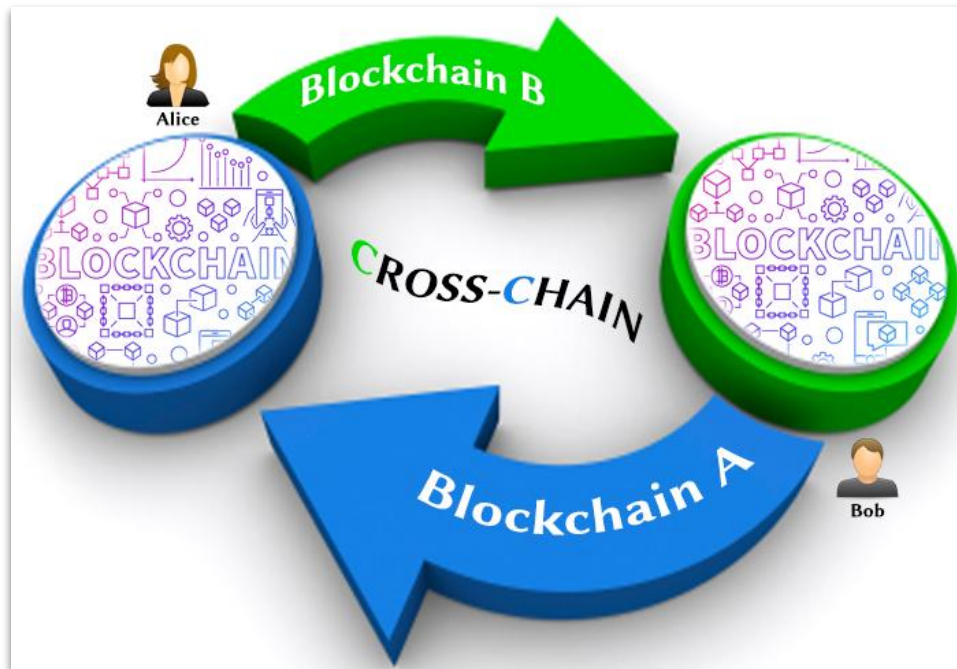
26

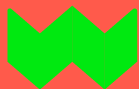
Workshop
RNP

Onde o futuro
se encontra.

Gt-Inter - Interoperabilidade entre Blockchains

A capacidade de conexão entre Blockchains já não precisa mais de terceiros





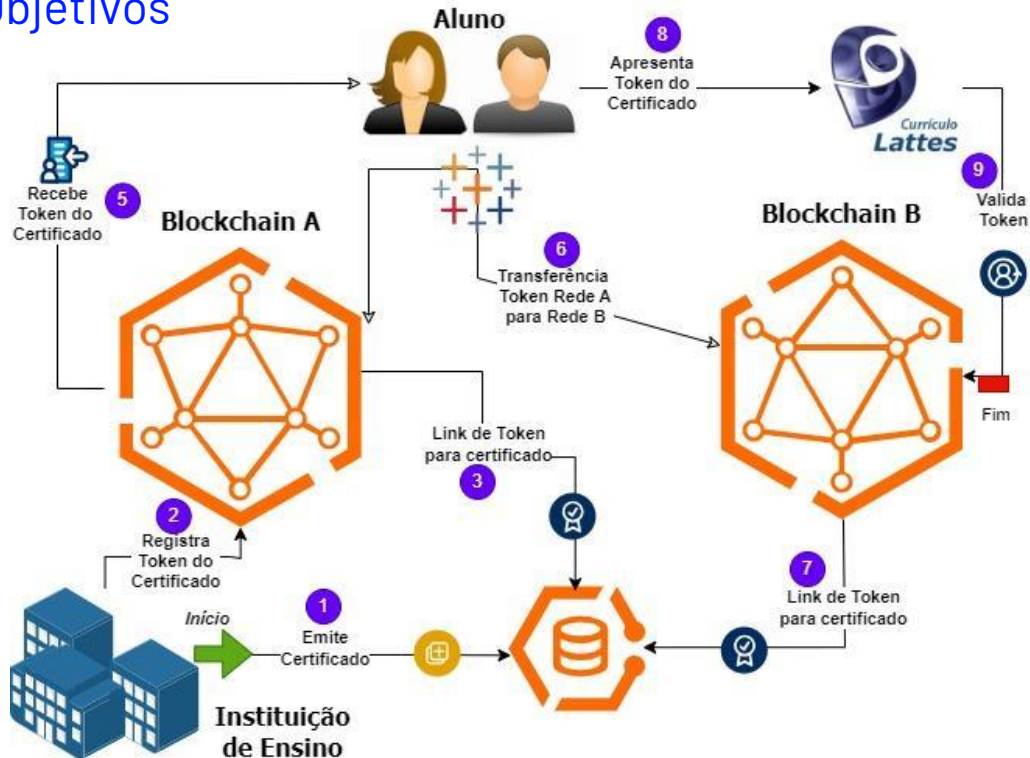
26

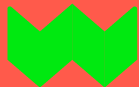
Workshop
RNP

Onde o futuro
se encontra.

Gt-Inter - Interoperabilidade entre Blockchains

Motivação e Objetivos





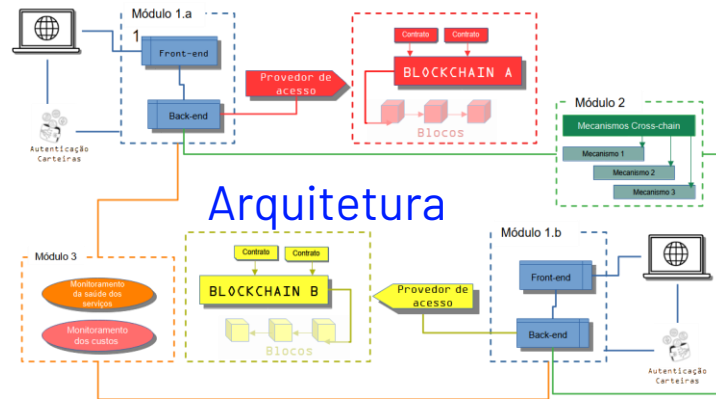
26

Workshop
RNP

Onde o futuro
se encontra.

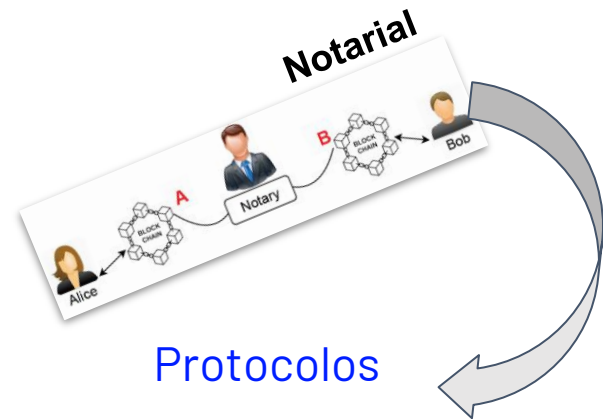
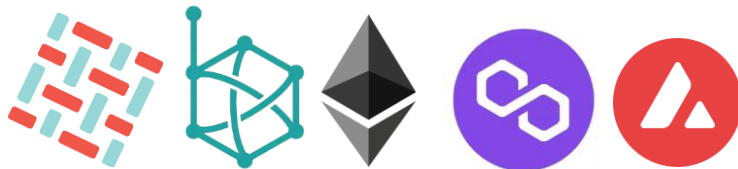
Gt-Inter - Interoperabilidade entre Blockchains

Status

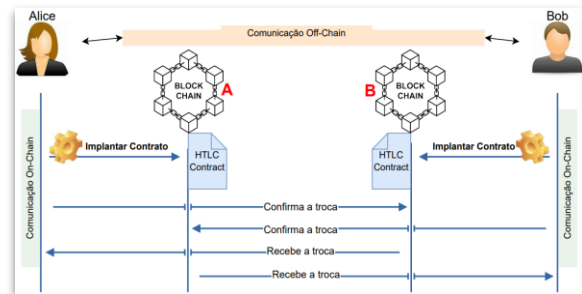


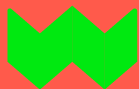
Arquitetura

Redes



Hash Time Lock Contract (HTLC)





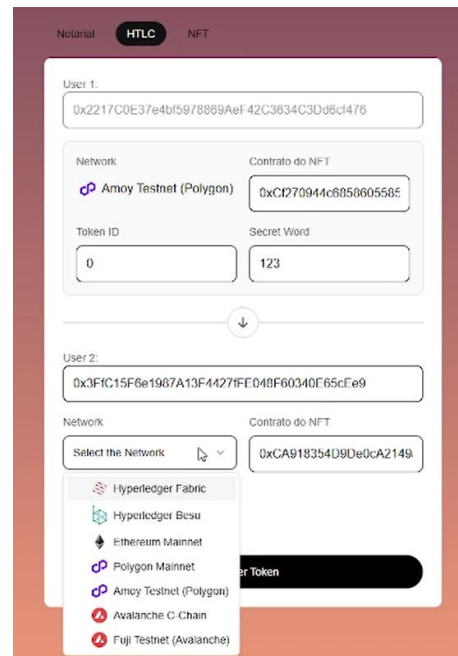
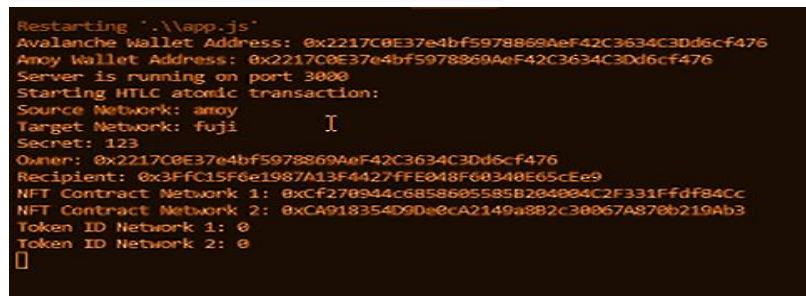
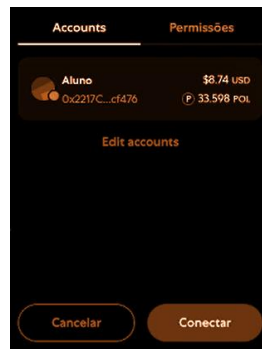
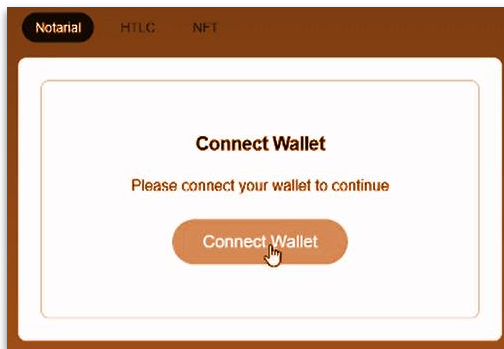
26

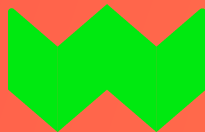
Workshop
RNP

Onde o futuro
se encontra.

Gt-Inter - Interoperabilidade entre Blockchains

Status - Frontend





26

Workshop
RNP

***Onde o futuro
se encontra.***

OBRIGADO!

Contato:



*alex.borges@ufjf.br
ronan.dutra@ufv.br
<https://netlab.ice.ufjf.br/gt-inter>
<https://github.com/GT-Inter>*



MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

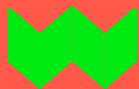
MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO



GT-PIDDF – Plataforma de IDD com Autenticação Federada

Diogo Menezes Ferrazani

UFF/Professor



26

Workshop
RNP

Onde o futuro
se encontra.

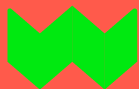
Motivação

- Sistemas tradicionais de gestão de identidade altamente centralizados
- ✗ Vulnerabilidade a ataques
- ✗ Falta de autonomia
- ✗ Dependência do provedor de identidade

Objetivo

- Desenvolver uma plataforma de identidade digital descentralizada, segura e interoperável, permitindo...
- ✓ Integração com mecanismos de autenticação federada
- ✓ Compatibilidade com sistemas e infraestruturas legados





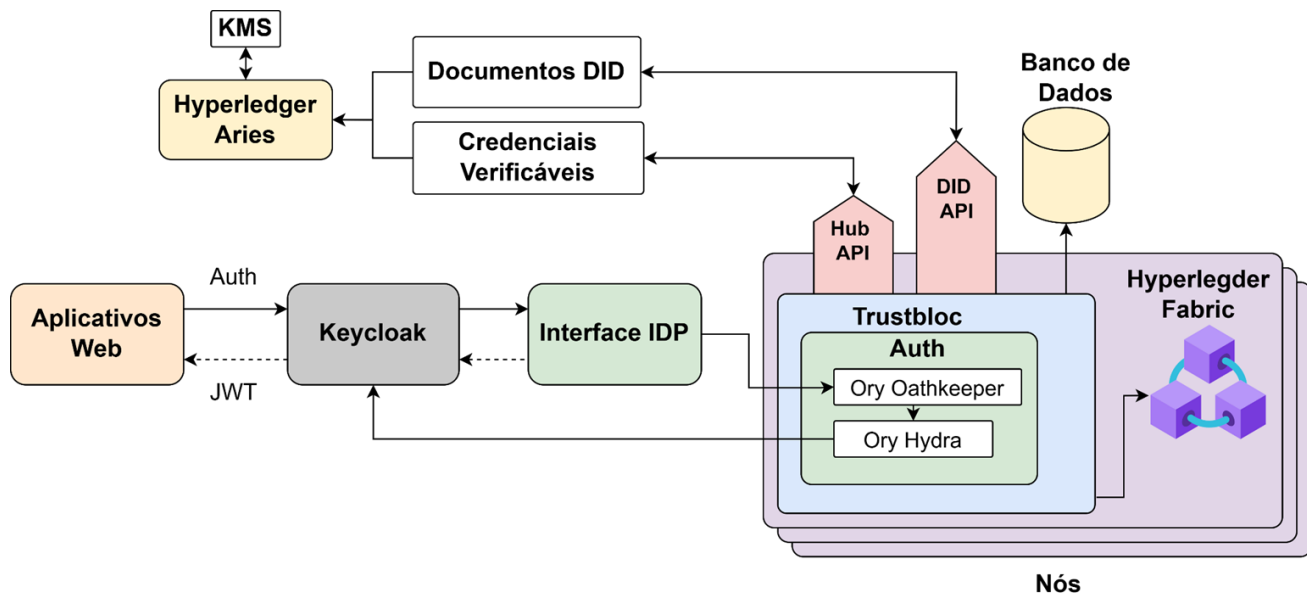
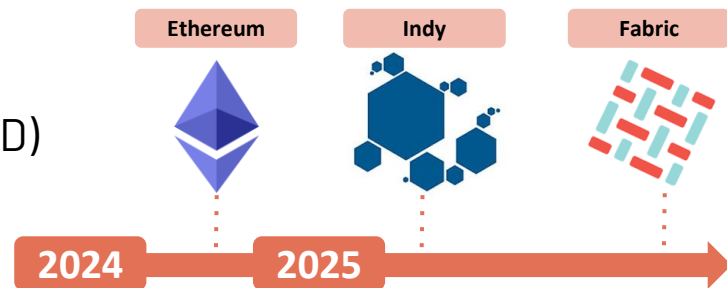
26

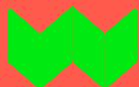
Workshop
RNP

Onde o futuro
se encontra.

Status Atual de Desenvolvimento

- ✓ Rede *blockchain* implantada e integrada ao Trustbloc e identidades descentralizadas (DID)
- ✓ Autenticação no Keycloak via certificados





26

Workshop
RNP

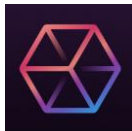
Onde o futuro
se encontra.

Próximos Passos

Implantação da
infraestrutura isolada



KEYCLOAK



Desenvolvimento da Lógica de
Autenticação e Autorização



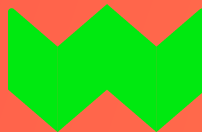
Utilizando
certificados digitais

Gestão de
Identities
Descentralizadas

Desenvolvimento e Teste da
Aplicação Cliente

Avaliação no
testbed Ilíada





26

Workshop
RNP

*Onde o futuro
se encontra.*

Contato

<https://labgen.com.br/gt-piddf>
menezes@midia.com.uff.br



MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

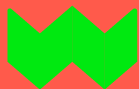


GT-Audita

Auditoria Transparente em Redes usando Blockchains

Magnos Martinello

UFES/Professor



26

Workshop
RNP

Onde o futuro
se encontra.

Provas-de-Conexão imutáveis em Blockchain para garantias de integridade dos logs de acesso à Internet

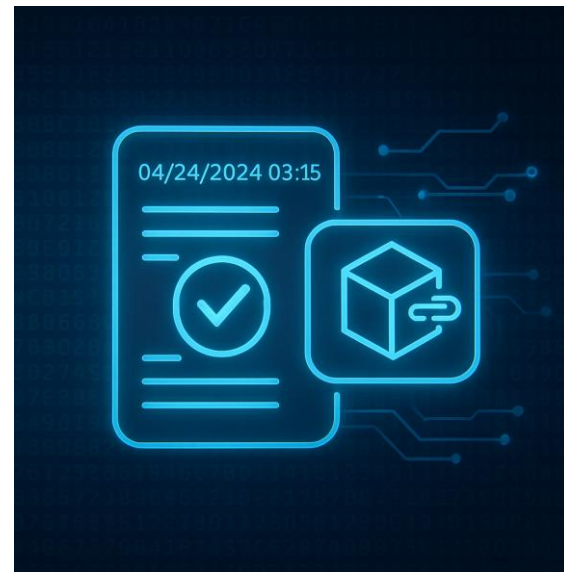
Problemática

Provedores de acesso (ISP) enfrentam desafios significativos no cumprimento de exigências regulatórias e normas de conformidade.

- Logs de sistemas de acesso à Internet, provenientes dos múltiplos sistemas coletores, **são vulneráveis** :
 - Podem ser alterados ou excluídos;
 - Difíceis de verificar em caso de disputas;
 - Manipuláveis após incidentes de segurança.

Proposta para garantir integridade no registro dos logs

- 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.



Blockchain como camada de confiança

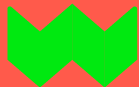
- Oferecer uma verificação irrefutável dos registros de conexões
- Imutabilidade dos registros;
- Transparência nas verificações;



Caso de uso (POP-ES/RNP)

- Desafio na escalabilidade e desempenho: volume alto de logs gerados no POP-ES/RNP
- 10 milhões de conexões por hora





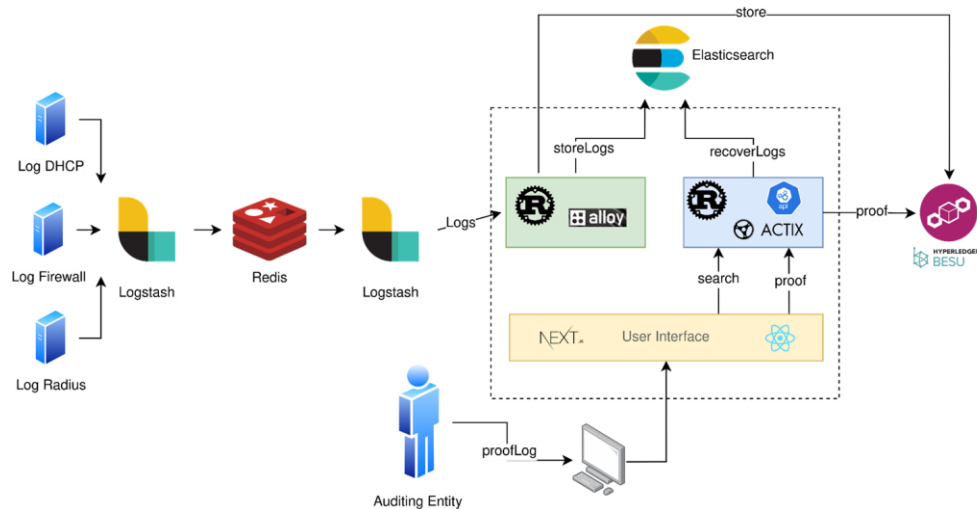
26

Workshop
RNP

Onde o futuro
se encontra.

Resultados do GT-Audita

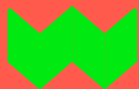
Arquitetura do sistema



Resultados

Contribuições esperadas

- Modelo de "*provas-de-conexão*" para auditoria de rede;
- Aplicação escalável para registro imutável de logs;
- Análise de desempenho e otimização de parâmetros;
- Implementação prática em ambiente controlado.



26

Workshop
RNP

Onde o futuro
se encontra.

Provas-de-Trânsito em Blockchain para verificação de caminho

Problemática

Provedores de acesso precisam atestar que um determinado fluxo de pacotes transitou por um caminho (switches/roteadores) previamente planejado

- Trânsito de um fluxo (malicioso ou de ataque DDoS) na rede do ISP, precisa ter formas de **confirmar a trajetória** dos pacotes.

**IETF121
PANRG**

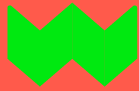
NASR main objectives

- Clients with high security and privacy requirements are not anymore satisfied with pure encryption-based data security measures in the application or transport layer that do not allow any control over the underlay networks. Clients now require their data to exclusively traverse the network through trusted devices, trusted operating environments, trusted links and trusted services, avoiding any exposure to insecure or untrusted devices. Hence, how to establish routing trustworthiness and transparency so as to achieve predictable forwarding behaviors becomes the main challenge.
- The goal of Network Attestation for Secure Routing WG is to address the challenges associated with routing data on top of trusted devices, trusted operating environments, trusted links and trusted services only, so as to achieve transparent and predictable forwarding behavior. Verifiable operational correctness proofs should also be given to serve as a trusted evidence for visualization, internal inspection and external auditing.

Forwarding Path Auditing

- Prove traffic went through specific elements (Proof of Transit)
- Prove traffic went through elements with certain properties (Trustworthiness)

I E T F



26

Workshop
RNP

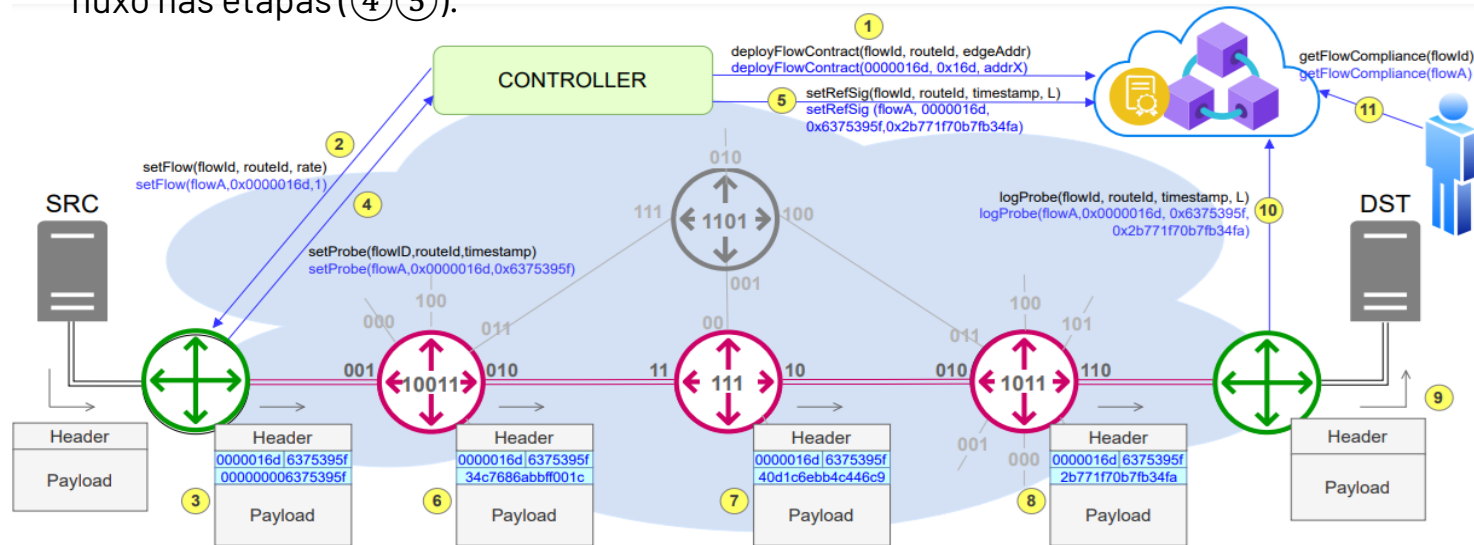
Onde o futuro
se encontra.

Sonda é registrada na blockchain com o valor da assinatura calculada no caminho (logProbe)

Supondo que precisamos verificar se um fluxo está atravessando um caminho

Um contrato inteligente é implantado para cada fluxo, atribuindo um flowID a um routeID.

Uma taxa de amostragem para este fluxo é especificada (por exemplo, 1 pacote/seg). O controlador configura o Ingress Edge enviando as informações do fluxo na etapa (2). Calcula e registra na blockchain **a assinatura de referência no contrato inteligente** do fluxo nas etapas (4)(5).



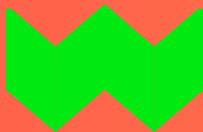
Resultados

Contribuições esperadas

- Modelo de "*prova-de-trânsito*" para auditoria de caminhos;
- Implementação no bmv2 para prototipação de rede emulada.
- 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

OBRIGADO !

Agradecimentos ao projeto Iliada da RNP



26

**Workshop
RNP**

Contato :

magnos.martinello@ufes.br

Git:

<https://github.com/nerds-ufes/GT-Audita>

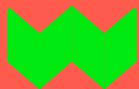
***Onde o futuro
se encontra.***



Outras ações de P&D do Projeto ILIADA

Reinaldo Gomes

Gerência de P&D em Cibersegurança - RNP



26

Workshop
RNP

Onde o futuro
se encontra.

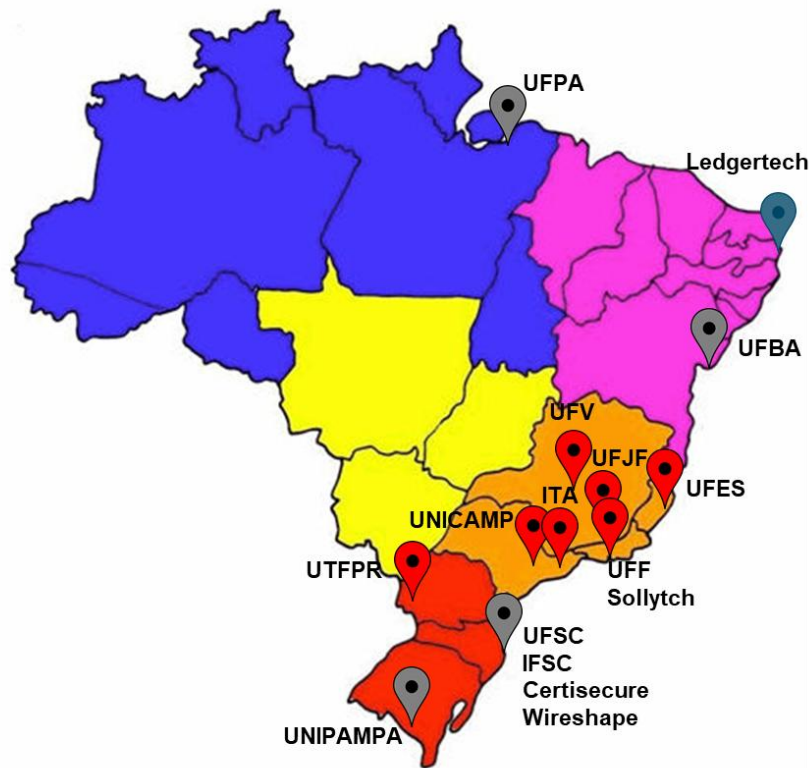
Ações de P&D do Projeto ILIADA

13 Grupos de trabalho em execução

- 8 GTs selecionados 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

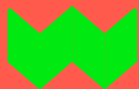


Grupos de Trabalho selecionados para desenvolvimento de Aplicações

Grupo de Trabalho	Coordenador	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

Startups para Provas de Conceito da Tecnologia Blockchain

Solução	Startup	Setor
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
Rastreabilidade Química Inteligente: Agricultura na Era da Blockchain	Sollytch	Agropecuária



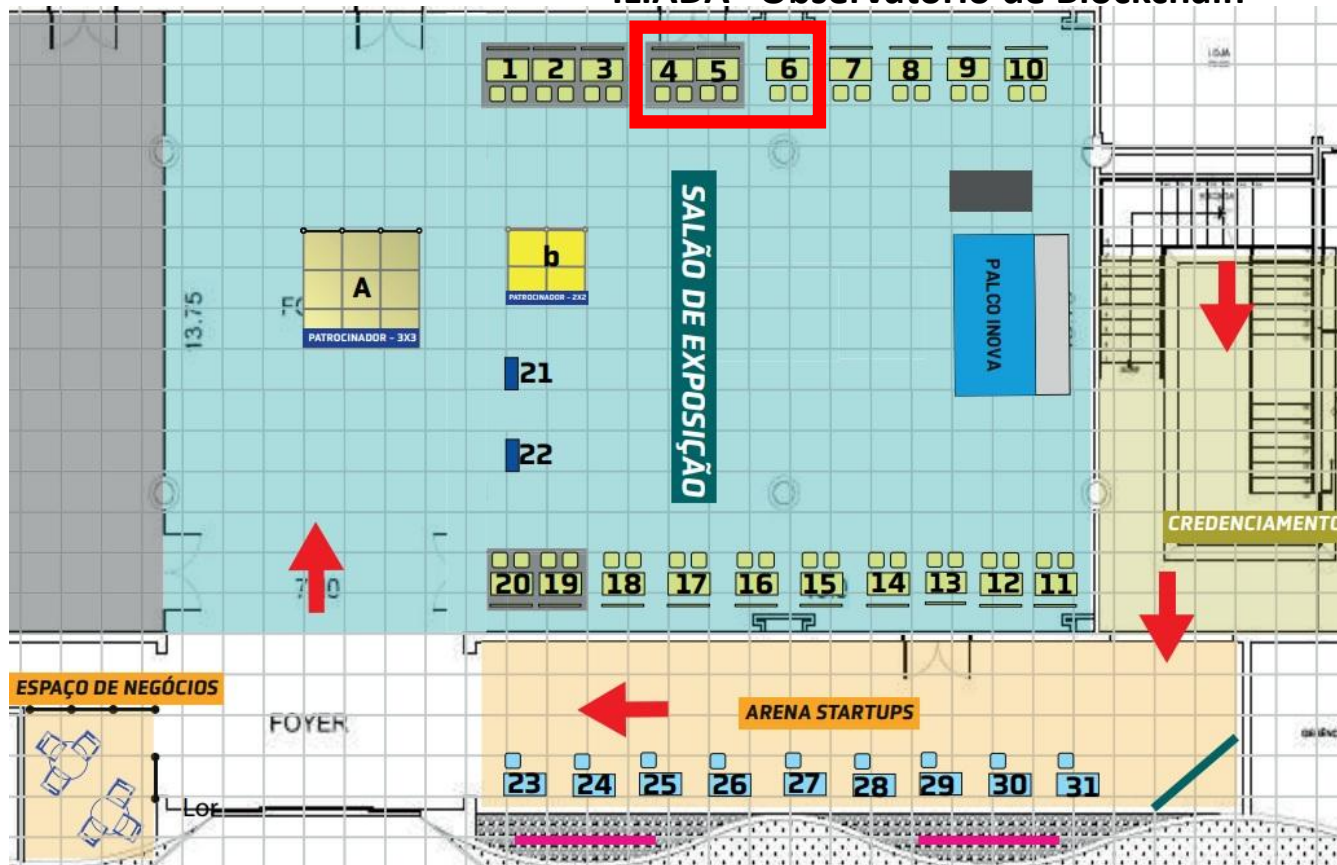
26

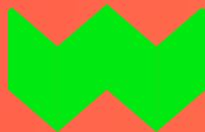
Workshop
RNP

Onde o futuro
se encontra.

Conheçam mais detalhes do ILIADA

ILIADA Observatório de Blockchain





26

Workshop
RNP

*Onde o futuro
se encontra.*

OBRIGADO!

reinaldo.gomes@rnp.br



MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

