

**Título: Auditoria Transparente e Rastreabilidade em Redes Utilizando BlockChains**

**Coordenador : Prof. Magnos Martinello**

**Equipe: Luiz Guilherme Bergamaschi Bueloni, Luiz Felipe Machado**

**Everson Scherrer Borges, Rafael Guimarães, Roberta Lima Gomes e Yuri Victoria**

# GT-Audita

## AGENDA: Motivação, Objetivo, Resultados e Futuro

- Motivação
- Fundamentação do projeto
- Objetivos do Projeto
- Resultados Atuais
- Planejamento Futuro



# Motivação : Prova de Conexão

Provedores precisam atender obrigações regulatórias e estarem em conformidade como PNSI

- Provedores de acesso precisam atender obrigações regulatórias e estarem em conformidade com políticas de segurança
  - Por exemplo : um problema comum é que os **dados provenientes dos múltiplos sistemas coletores de logs** estão sujeitos a serem *alterados*, *apagados* e eventualmente *refutados*.
- **Registros** de acesso, autenticação, atribuição de endereços IP , ....
  - Precisam ser coletados, armazenados e recuperados de modo consistente para garantir análises forenses e facilitar os processos de auditorias

# Casos de auditoria em um incidente de segurança

Exemplo : o CAIS envia uma descrição de violação de segurança (e.g. *copyright*) :

1. Endereço do IP público da rede da instituição
2. Porta de origem e
3. O horário de acesso

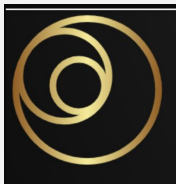
Problema:

- **Garantir de forma irrefutável**, a autoria na sequência de eventos relacionados

# O que significa garantir de forma irrefutável, a autoria na sequência de eventos relacionados ?

Para que cada etapa possa ser comprovada de maneira íntegra e incontestável, precisamos

1. Consultar **os logs do firewall** para identificar o endereço IP interno (NAT) utilizado durante o acesso remoto.
2. A partir desse IP interno, analisar os **logs do servidor DHCP** para determinar o endereço **MAC associado**.
3. Em seguida, verificam-se os registros do **servidor RADIUS** a fim de identificar o **usuário autenticado** correspondente ao endereço MAC.

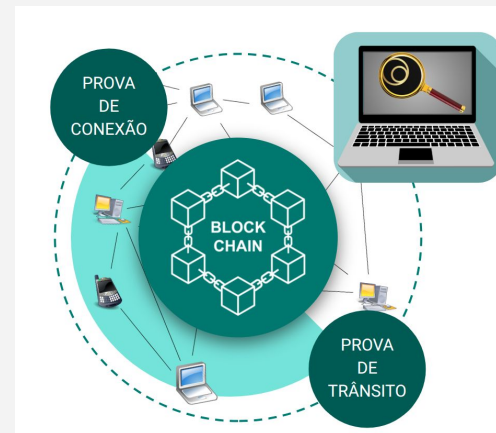


# Objetivo do projeto : Prova de Conexão

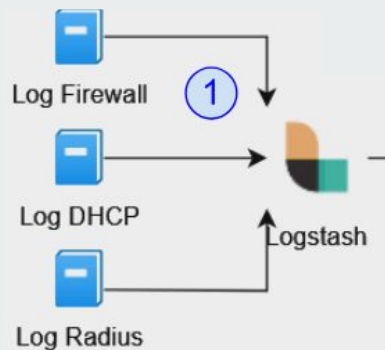
Adicionar uma camada de verificação  
de registros

- Viabilizar a auditabilidade de **acesso à rede** a partir de **hashes criptográficos (em bloco de registros)** que serão armazenados de *modo cirúrgico* na blockchain

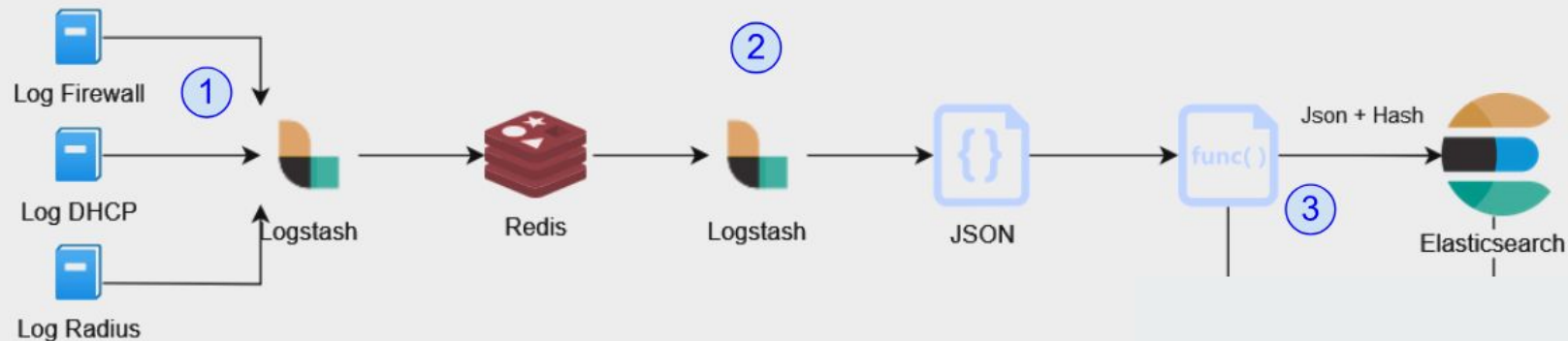
Garantir transparência e que o acesso pelo **dispositivo/naquela conta/ pelo endereço IP/no tempo Z** não possa ser refutado.



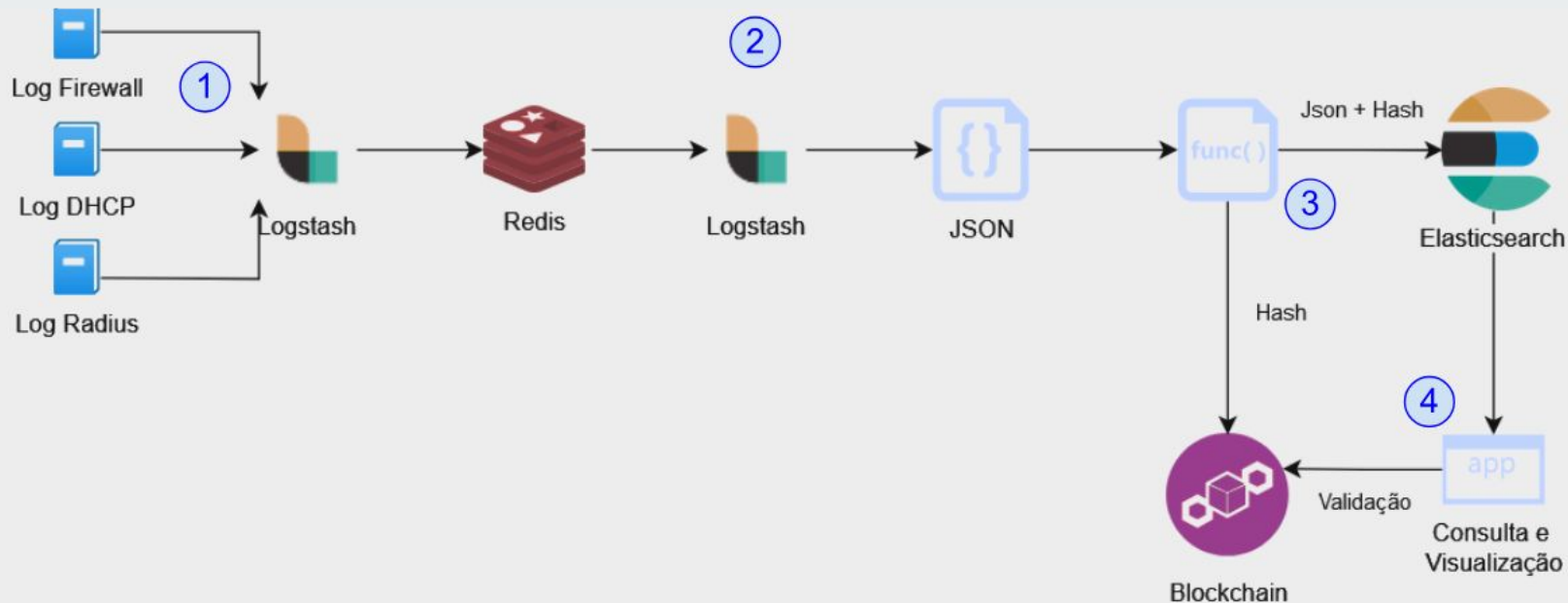
# Arquitetura em microserviços para registros das conexões : logs gerados firewall, DHCP e Radius via syslog



# Arquitetura do sistema : processamento dos logs gerando JSON e um hash



# Arquitetura do sistema : indexação, armazenamento e criação do contrato inteligente na Blockchain

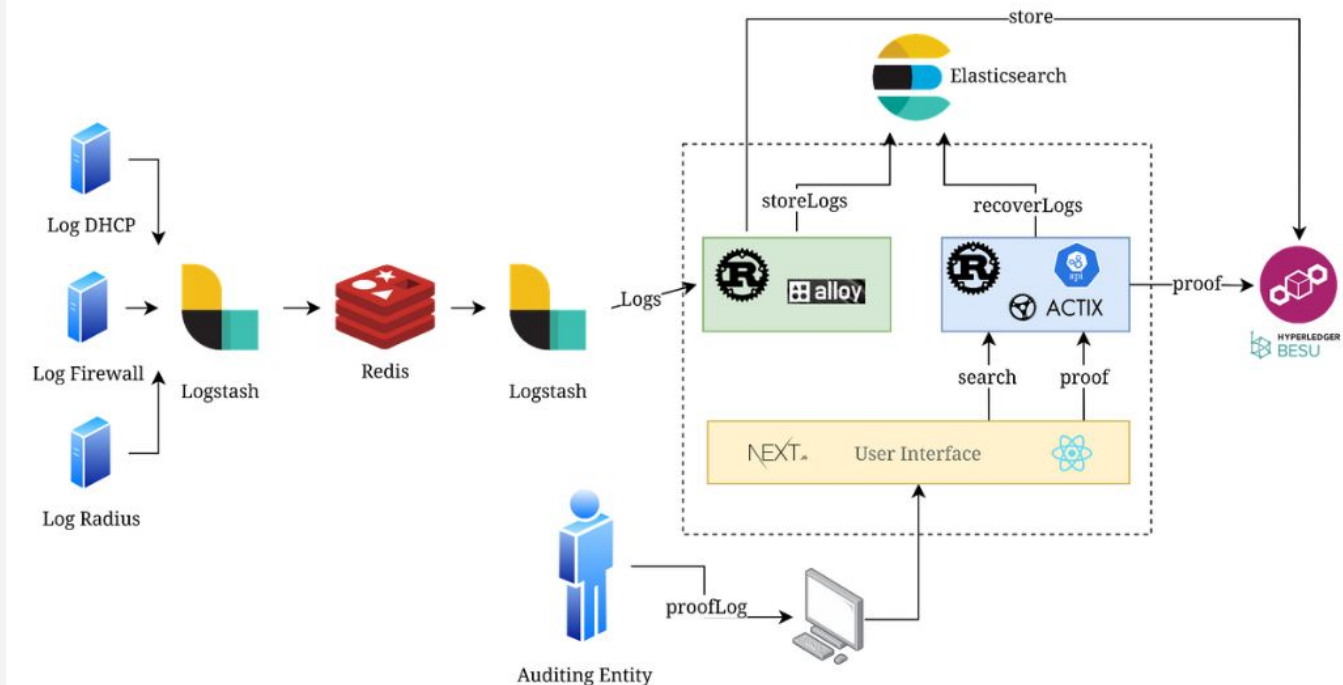


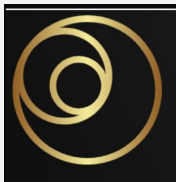
# Auditoria : Verificação da Integridade na Blockchain

Buscar o “evento” no Storage e calcular o hash

Consultar Hash na Blockchain

Comparar se não houve alteração, então evento íntegro de modo irrefutável





# Resultados

Sistema para auditabilidade transparente  
em casos de incidentes de segurança

## Auditabilidade transparente em casos de violações de segurança

- Um sistema para verificação dos registros de conexões (oferecer prova de conexão)
  - Processamento de logs dos múltiplos coletores escalável em microserviços, indexação, armazenamento em BD e inserção na estrutura de blockchain do projeto Ilíada (integrado e funcionando)
  - Interface de consulta para eventos

# Caso de uso no POP-ES (CAIS)

---

Recebemos um alerta do CAIS sobre uma violação, gerado a partir dos seguintes parâmetros (exemplo demonstrativo):


Endereço IP: 200.137.65.102

Porta de Origem: 57738

Timestamp: 2025-07-14T11:04:00-03:00

Nosso objetivo é **rastrear o responsável** pela requisição e validar a integridade dos dados envolvidos.

# Interface da aplicação

 Pop ES

Destination Mapped IP


Destination Mapped Port

Timestamp (±10 minutes range)

Search will include 10 minutes before and after the specified time

# Retorno das consultas

Busca retornou resultados no range de +/- 10 min, selecionamos o mais próximo do timestamp

 **Firewall Log** FIREWALL  
Contains dst\_ip for DHCP lookup

Batch ID `f1c7d9a1-d78...3875`

✓ Authentic Document


# Signer `47862d59...ea77`

Storage `47862d59...ea77`

Source Data 13 fields

@timestamp: 2025-07-14T14:04:33.000Z  
cisco: Object  
dst\_ip: 172.21.29.221  
+ 10 more

→ Search DHCP

 **DHCP Record** DHCP  
Contains MAC address for Radius authentication lookup

Batch ID `231722c4-b7d...64a9`

✓ Authentic Document


# Signer `11e270a7...c3e3`

Storage `11e270a7...c3e3`

Source Data 6 fields

@timestamp: 2025-07-14T12:35:23.543136437Z  
ip: 172.21.29.221  
lease\_time: 4000  
+ 3 more

→ Search Radius

 **Radius Authentication** RADIUS  
Final authentication record

Batch ID `8fac9263-349...0bfe`

✓ Authentic Document

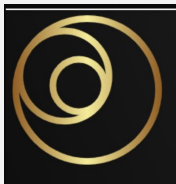
# Signer `5814b877...9a53`

Storage `5814b877...9a53`

Source Data 4 fields

JSON SOURCE

```
{
  "@timestamp": "2025-07-14T14:00:51.97758",
  "mac": "58-6c-25-a0-ba-6d",
  "type": "radius",
  "username": " "
}
```



# Resultados

Sistema para auditabilidade transparente  
em casos de incidentes de segurança

## Auditabilidade transparente em casos de violações de segurança

- Um sistema para verificação dos registros de conexões (oferecer prova-de-conexão)
  - Processamento de logs dos múltiplos coletores escalável em microserviços, indexação, armazenamento em BD e inserção na estrutura de blockchain do projeto Ilíada (integrado e funcionando)
  - Interface de consulta para eventos
  - [API completa](#) de todas as partes do sistema para reprodutibilidade e extensão
    - [Vídeo da demonstração passo a passo](#) (com [git](#))
  - Implantação e uso do sistema de auditabilidade na UFES
    - [Casos reais identificados, notificados e respondidos](#)

## Objetivo 2 : Desafios referentes à “prova de trânsito”

Provedores precisam responder aos desafios na segurança de trânsito dos fluxos

- Provedores de acesso precisam atestar que um determinado fluxo de pacotes transitou por um caminho (switches/roteadores) previamente planejado
- Os requisitos específicos para *auditabilidade de caminho* podem variar conforme o ambiente regulatório, o tipo de rede e os serviços oferecidos.
  - Exemplos : Trânsito de um fluxo em um *caminho soberano (i.e. caminho assinado)* na rede do ISP, precisa ter registros suficientes para **confirmar a trajetória** dos pacotes.

# IETF : PANRG Forwarding Path Auditing

## 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)**

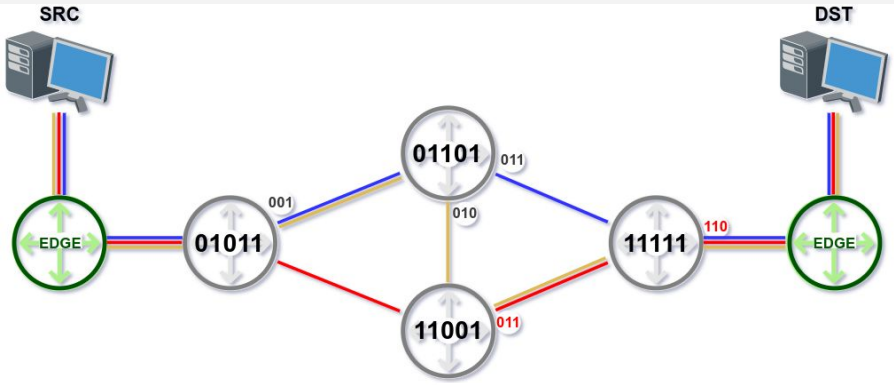


# Proposta : Verificação de Caminho com base no Sistema Numérico de Resíduos (RNS)

1. Associar polinômios irreduzíveis aos nós  
01011, 01101, 11001, 11111
2. Para um dado caminho, calcular um RouteID usando "Chinese Remainder Theorem"

**Path-1**

routeID = 100101111  
 nodeID - 01011, 01101, 11111  
 portID - 001, 011, 110



$$\begin{cases} X \bmod 01011 = 001 \\ X \bmod 01101 = 011 \\ X \bmod 11111 = 110 \end{cases}$$

$X = 100101111$

(polinômio  $x^8 + x^5 + x^3 + x^2 + x + 1$ ).

# Assinatura do Caminho a partir de hashing encadeado salto a salto

- O Route-ID é a solução de um sistema de congruência resolvido para um conjunto de S e O.  
 $\{(s_1(t), o_1(t)), [(s_2(t), o_2(t)), \dots, [(s_N(t), o_N(t))]\}$
- Ao explorar a unicidade do par, uma propriedade nativa do sistema de roteamento  
 $s_i(t) = \text{nodeID}, \quad o_i(t) = \text{portID}$
- Propomos uma **assinatura de caminho (path signature) que encadeia a assinatura de cada nó usando CRC32**, mantendo assim o tamanho do cabeçalho fixo.

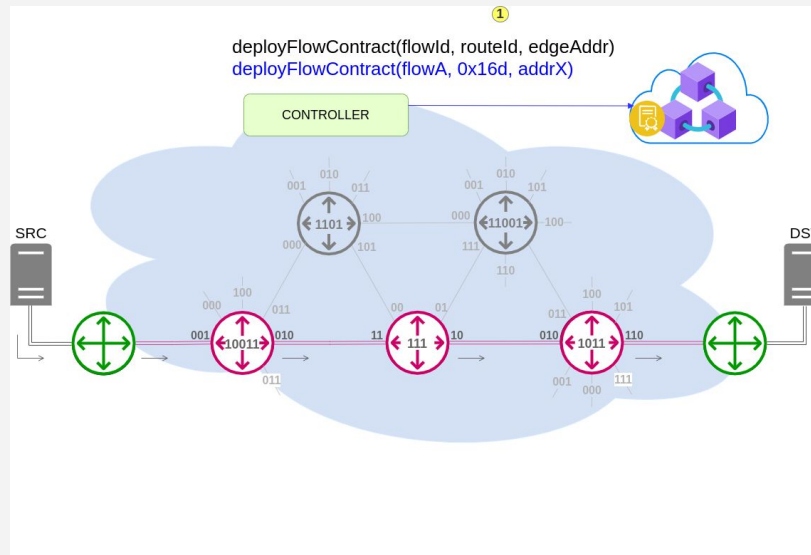
$$L_i = H(s_i(t) || o_i(t) || L_{i-1})$$

# Proposta verificação de caminho com assinatura a partir de hash encadeado

[“PathSec: Path-Aware Secure Routing with Native Path Verification and Auditability” IEEE NFV SDN 2024, M Martinello et. al](#)

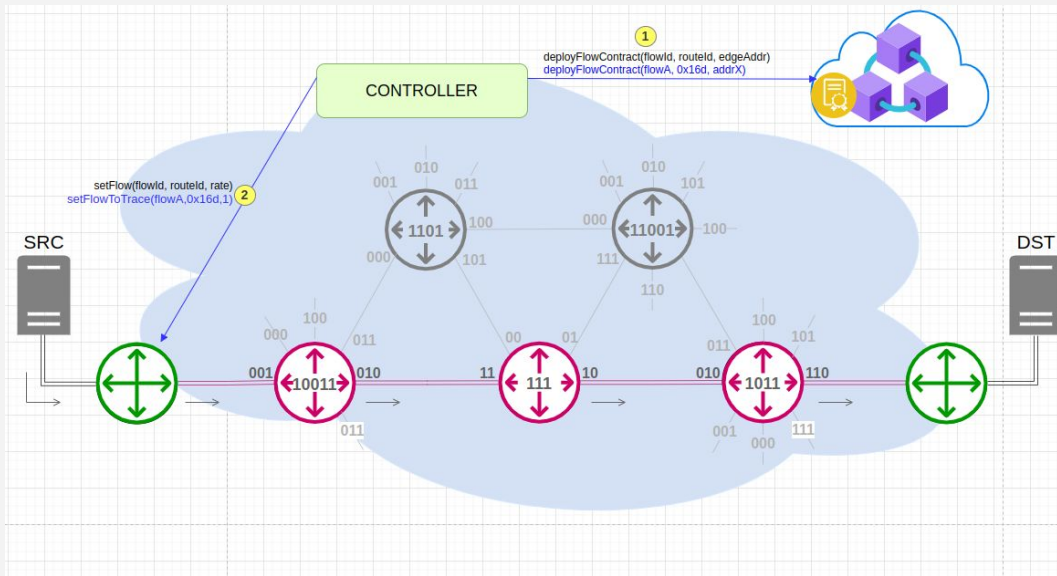
Supondo que precisamos verificar se um fluxo está atravessando o caminho planejado: Calcula-se um hash para obter seu flowID e seleciona-se um caminho com seu routeID específico ( $R(t) = 0x16d$ ).

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



# Configurar taxa de amostragem

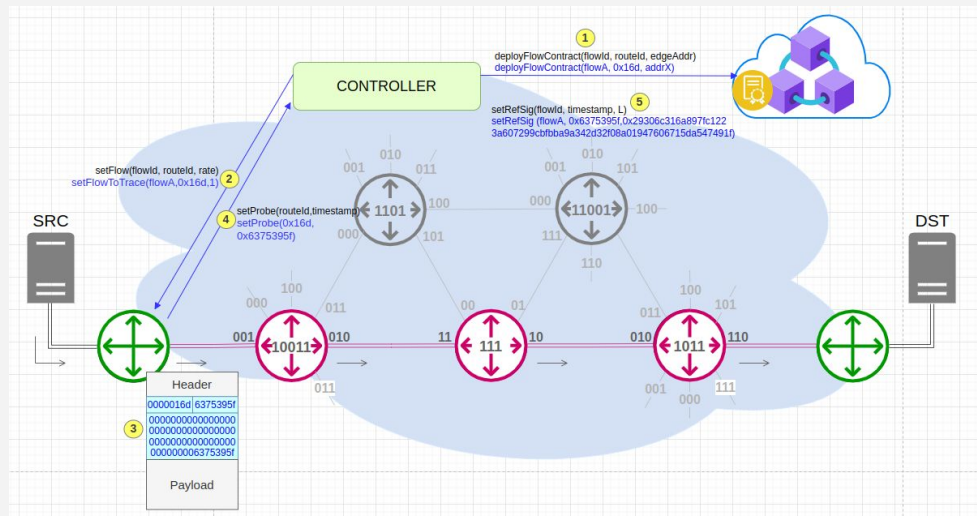
- Uma taxa de amostragem para este fluxo é especificada (por exemplo, 1 pacote/seg). O controlador configura o *Ingress Edge* enviando as informações do fluxo na etapa ②.



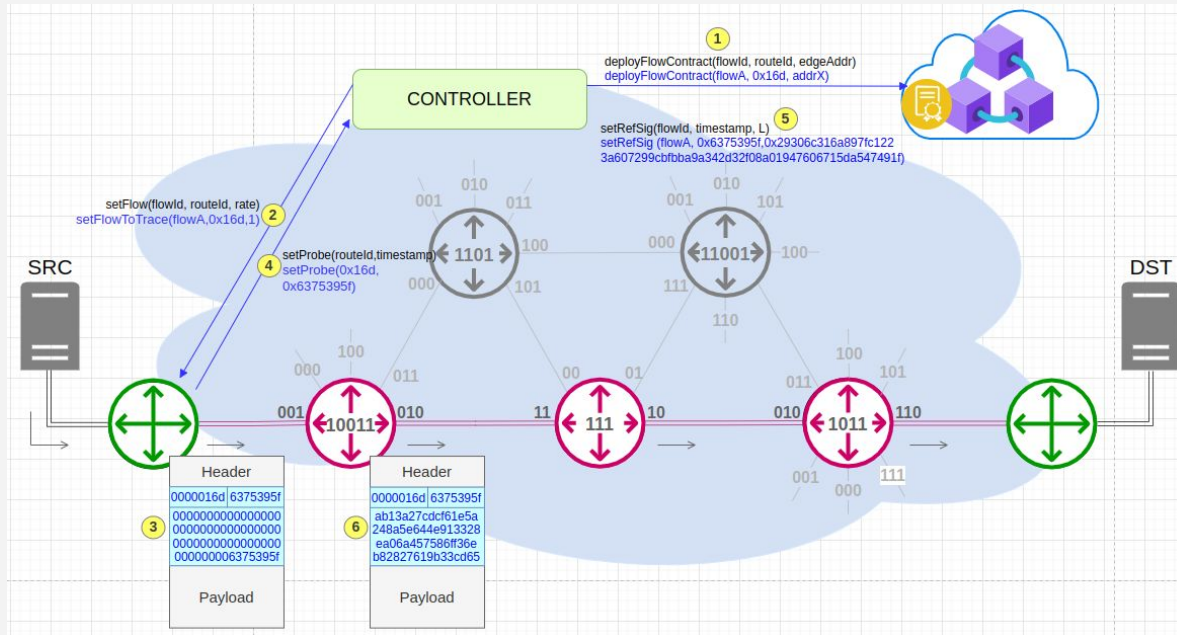
# Assinatura de referência no contrato inteligente Route-ID + timestamp por sonda

Para cada sonda, o nó de borda gera aleatoriamente um timestamp e o incorpora tanto no campo de cabeçalho do timestamp quanto no campo de cabeçalho da assinatura leve (por exemplo, L = L0 = 0x6375395f) na etapa ③.

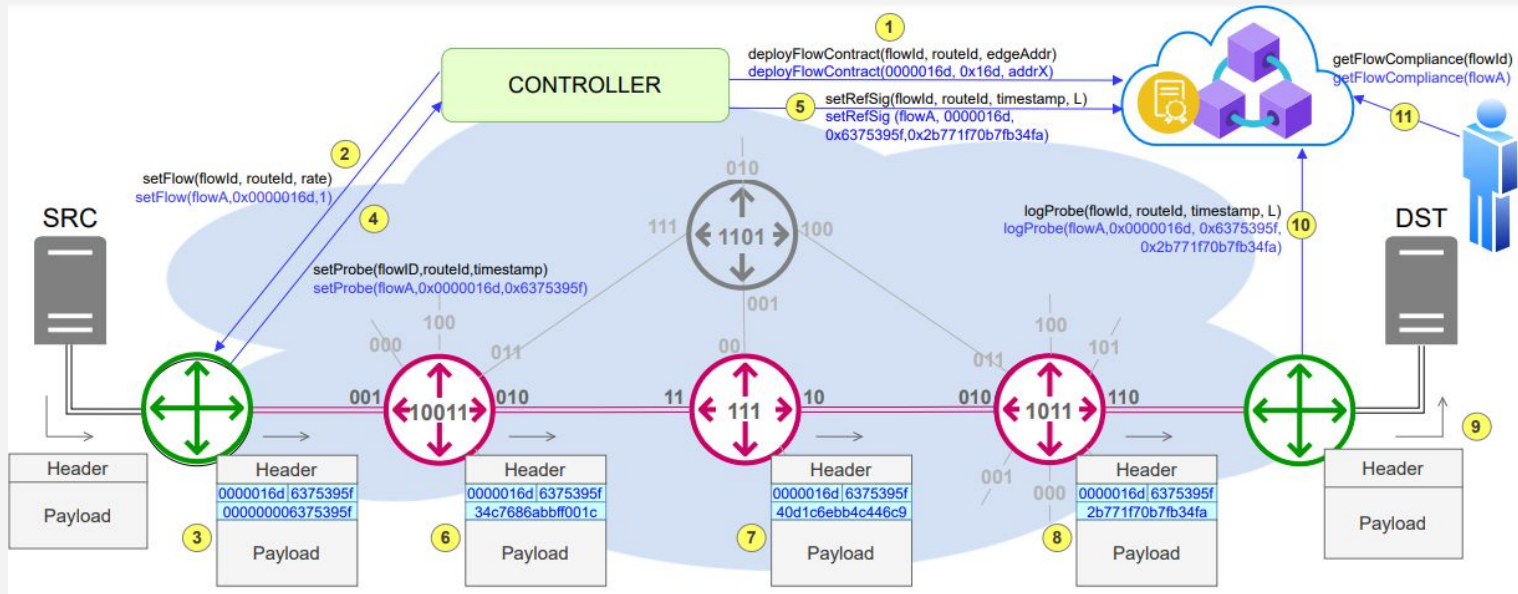
Esse timestamp é enviado ao controlador, que gera e registra a assinatura de referência no contrato inteligente do fluxo nas etapas ④⑤).

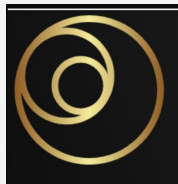


# Computação de hash salto a salto



# Design completo do sistema



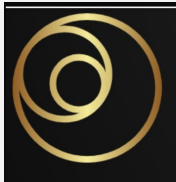


# Resultados

Auditabilidade do trânsito de pacotes em caminhos planejados

## Auditabilidade do trânsito de pacotes em caminhos estabelecidos/planejados

- Integração da blockchain com *uma rede ciente de caminho (PathSec)* por meio da **assinatura de caminho**
- A sonda carregando as assinaturas (hash) salta a salto sendo usada como prova de trânsito e inserida na blockchain para auditabilidade
- **Implementação em ambiente emulado mininet** integrando com projeto Iliada Besu Ethereum



# Resultados

Auditabilidade do trânsito de pacotes em caminhos planejados

Escopo : Casos de desvio no encaminhamento

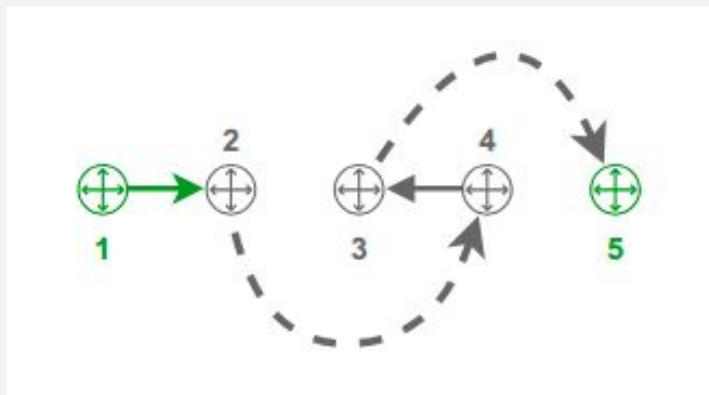


Adição de um nó  
Salto (skipping) de um nó

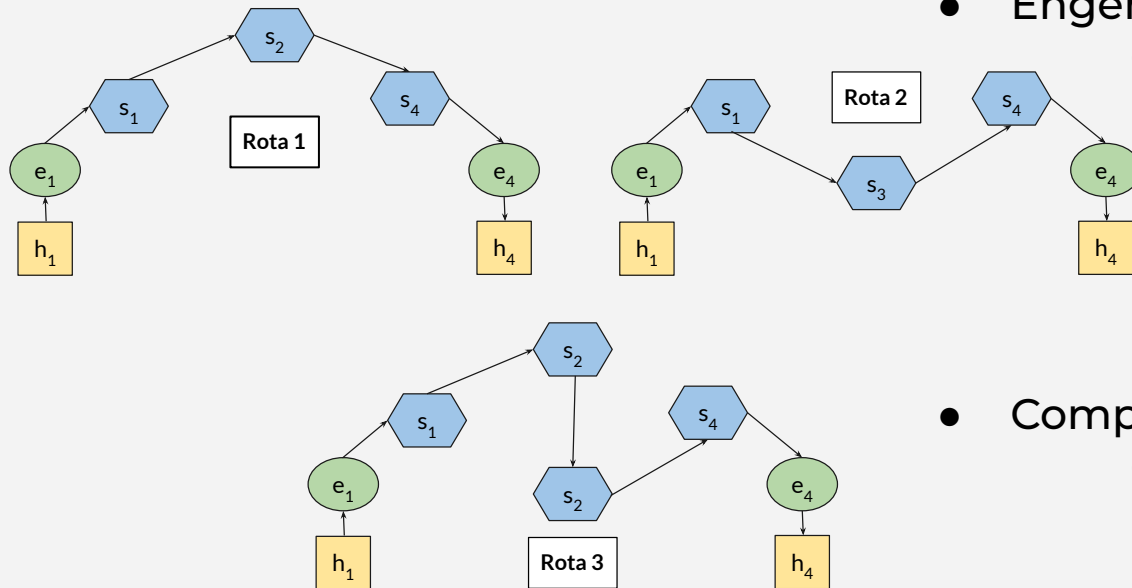


Detour Parcial e completo

Percurso Fora de Ordem



# Caso : Fluxo alterado para uma nova rota



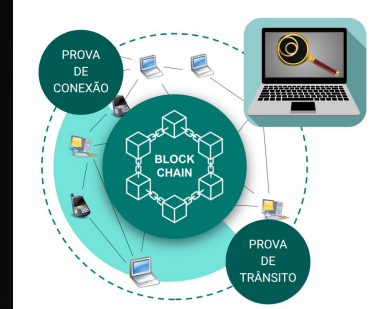
- Engenharia de Tráfego
  - [Vídeo demonstrando um fluxo alterado para uma nova rota](#)
- Compliance de trajeto
  - [Vídeo demonstrando o histórico da auditoria do fluxo](#)

# Planejamento Futuro

---

- Buscar apoio para dar continuidade ao desenvolvimento e uso do sistema de auditabilidade
  - Registro do Software
  - Implantação em outras instituições
  - Plugins para novos coletores
- Implementação da prova de trânsito *feita em Switches Tofino*
  - [Demo no Sigcomm 2025](#)
- Buscar apoio para estender a prova de trânsito em Testbeds (e.g. GP4Lab)
  - Garantir **caminhos soberanos** assinados pela Rede
  - Integrar com Blockchain para auditabilidade de caminhos

# GT-Audita agradece sua atenção !!!



Contato : [magnos.martinello@ufes.br](mailto:magnos.martinello@ufes.br)

Agradecimento especial ao projeto Ilíada da RNP

Ao Reinaldo C Gomes pelas múltiplas orientações



## GT-Audita

AUDITORIA TRANSPARENTE EM REDES USANDO BLOCKCHAINS