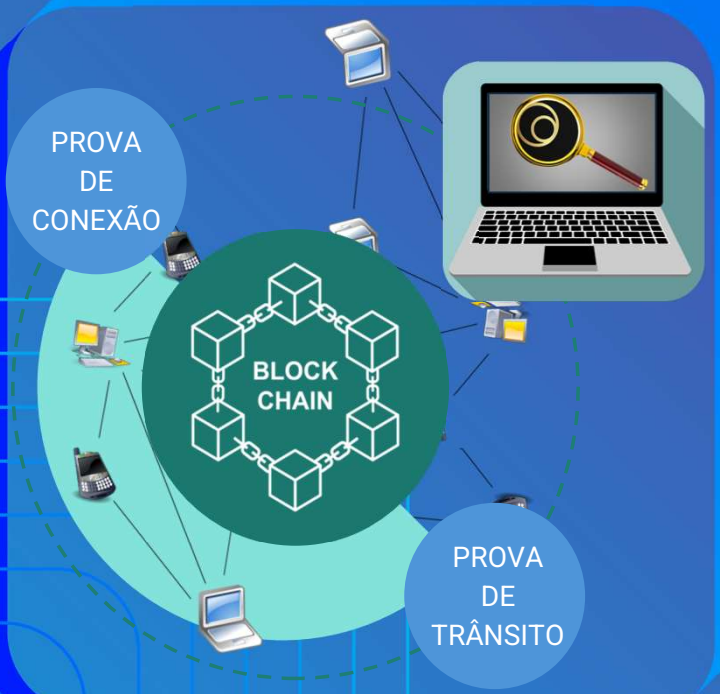
PROJETO ILIADA

Blockchain
em evolução.



GT-Audita

Auditoria Transparente em Redes usando Blockchains

Motivação

- Provedores de acesso precisam atender obrigações regulatórias e estarem em conformidade com políticas de segurança
    - Os registros são frequentemente a única evidência de um ataque bem-sucedido
    - Dados provenientes dos múltiplos sistemas (acesso, autenticação, endereço, etc.)
    - Precisam ser coletados, armazenados e recuperados de modo consistente para garantir análises forenses e facilitar os processos de auditorias internas
    - Estão sujeitos a serem alterados, apagados e eventualmente refutados

- Deve ser mantida sob constante monitoramento e utilização, pois os atacantes sabem que muitas organizações mantêm logs de auditoria por razões de conformidade, mas raramente os analisam

Proposta do Grupo de Trabalho

- Adicionar uma camada de armazenamento de informações para verificação dos registros usando blockchain

- Viabilizar a auditabilidade a partir de hashes criptográficos que serão armazenados na blockchain
  - Logs
  - Caminhos percorridos por pacotes

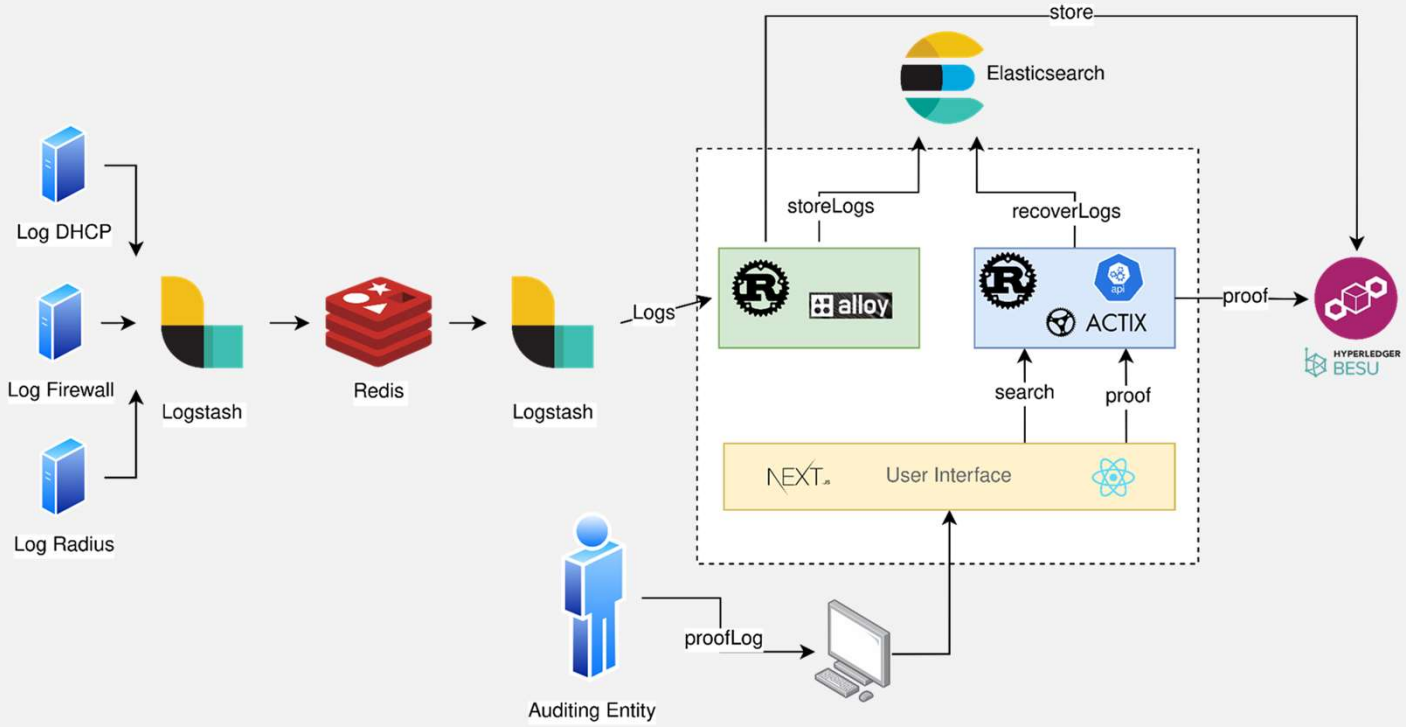
- Garantir transparência e que o acesso pelo ***dispositivo/naquela conta/pelo endereço IP/no tempo Z*** não possa ser refutado

Arquitetura do sistema para armazenamento de Logs

Envio de logs gerados firewall, DHCP, Radius, ...

Processamento dos logs gerando JSON e um hash

Indexação e armazenamento (onchain e offchain)



Caso de uso: Auditoria de incidente de segurança

CAIS envia uma descrição do ataque com :

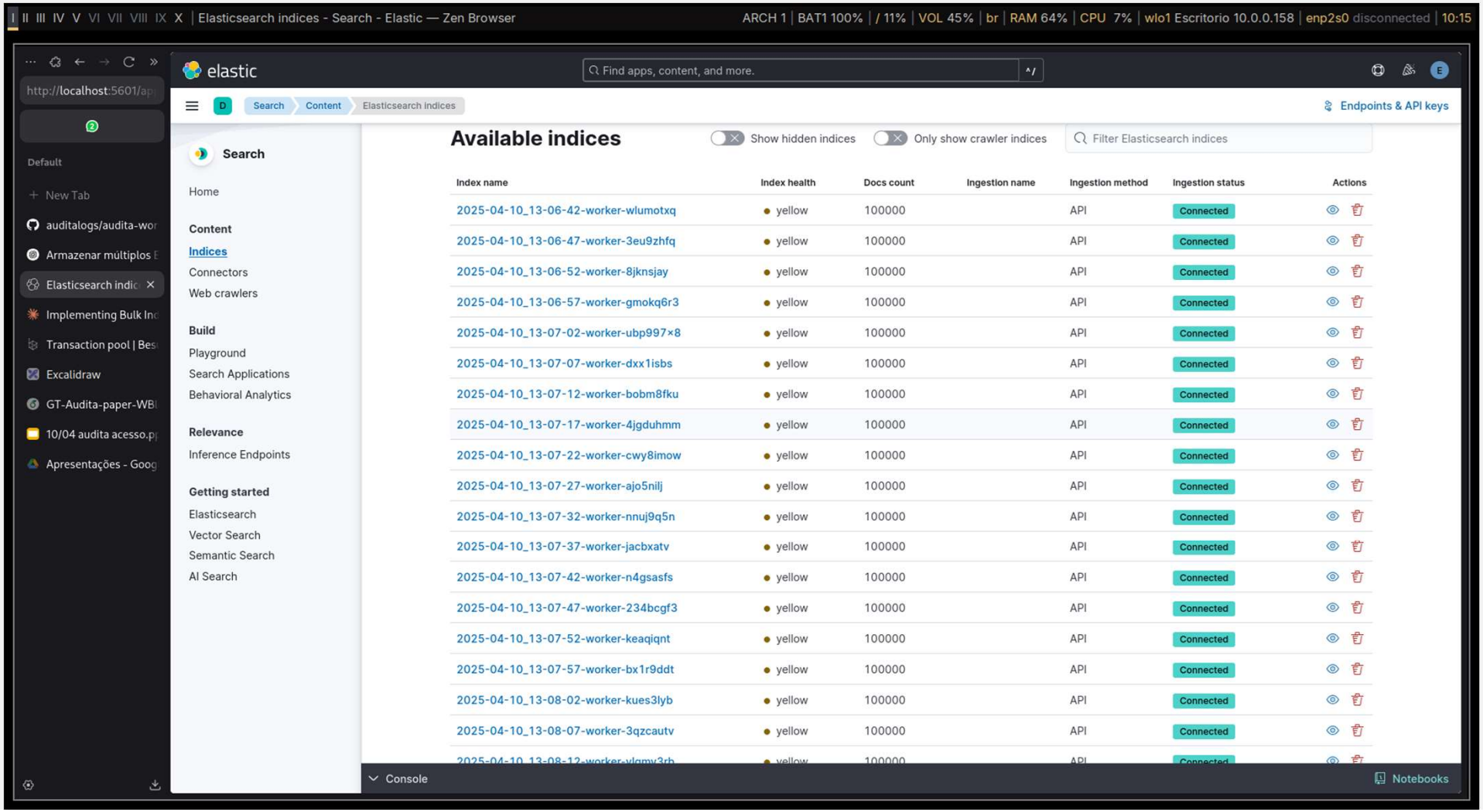
1. Endereço IP público da rede
2. Porta de origem e
3. O horário de acesso

Utiliza-se os logs do firewall para encontrar um Endereço IP interno (NAT) usado no acesso remoto

Com base no IP, verifica-se os logs do DHCP para encontrar o MAC , depois no RADIUs o usuário autenticado

Buscar os logs no banco, calcular o hash e verificar na blockchain

Implementação atual



Implementação atual

```
2025-04-10T13:07:32.893069Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-07-27-worker-ajo5nilj (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:07:37.880712Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-07-32-worker-nnuj9q5n (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:07:42.808369Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-07-37-worker-jacbxatv (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:07:47.795717Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-07-42-worker-n4gsasfs (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:07:52.772853Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-07-47-worker-234bcgf3 (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:07:57.907995Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-07-52-worker-keaqiqnt (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:02.903955Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-07-57-worker-bx1r9ddt (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:07.710771Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-02-worker-kues3lyb (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:12.648642Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-07-worker-3qzcautv (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:17.495268Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-12-worker-vlqmv3rb (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:22.607783Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-17-worker-uezml1sd (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:27.448841Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-22-worker-3shelcfs (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:32.569870Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-27-worker-kiwk9t48 (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:37.500264Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-32-worker-n2kfmyei (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:42.609920Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-37-worker-s77gwqvb (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:47.498859Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-42-worker-xh2ftqmi (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:52.503515Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-47-worker-h2kraqws (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:08:57.411095Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-52-worker-aftxfi4v (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:09:02.373119Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-08-57-worker-spqjyq3m (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:09:07.257870Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-09-02-worker-c26h1vek (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:09:12.175902Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-09-07-worker-au3dh2vx (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:09:17.037158Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-09-12-worker-zq95axmp (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:09:22.129235Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-09-17-worker-2thwcegn (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:09:27.194155Z  INFO audita_server::task::worker: batch processing completed. items processed: 100000, index: 2025-04-10_13-09-22-worker-zlyo06dy (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:09:30.627955Z  INFO audita_server::task::ethereum: ethereum batch processing completed tx_count=100
```

Envio para a blockchain em lote

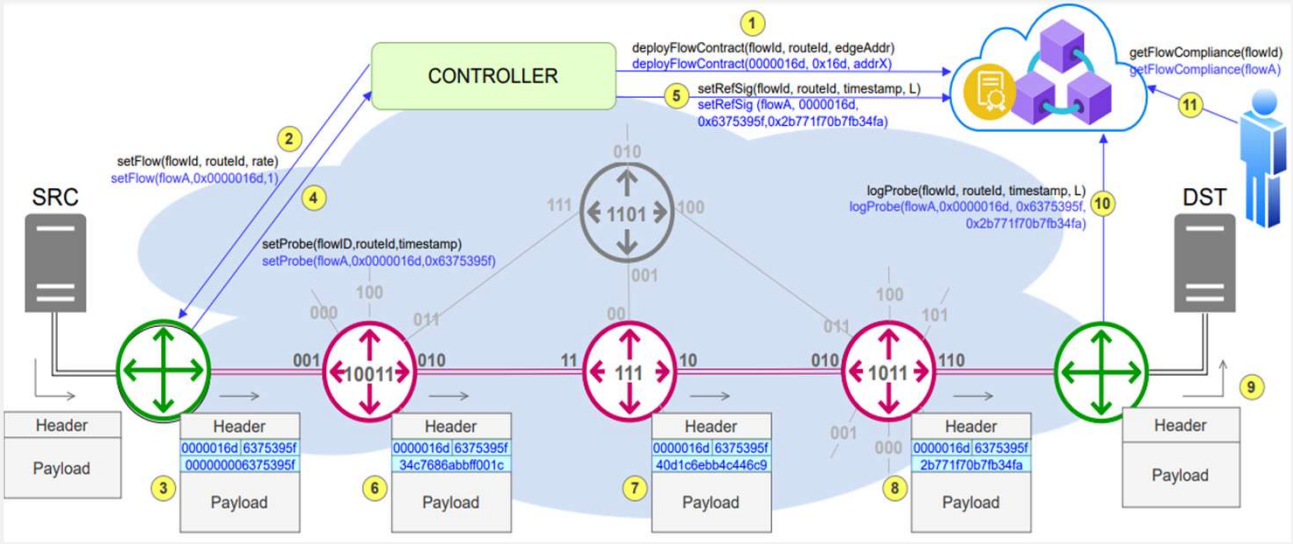
10 Milhões de logs processados

Batch Size de 100 mil -> 100 hashes para a blockchain

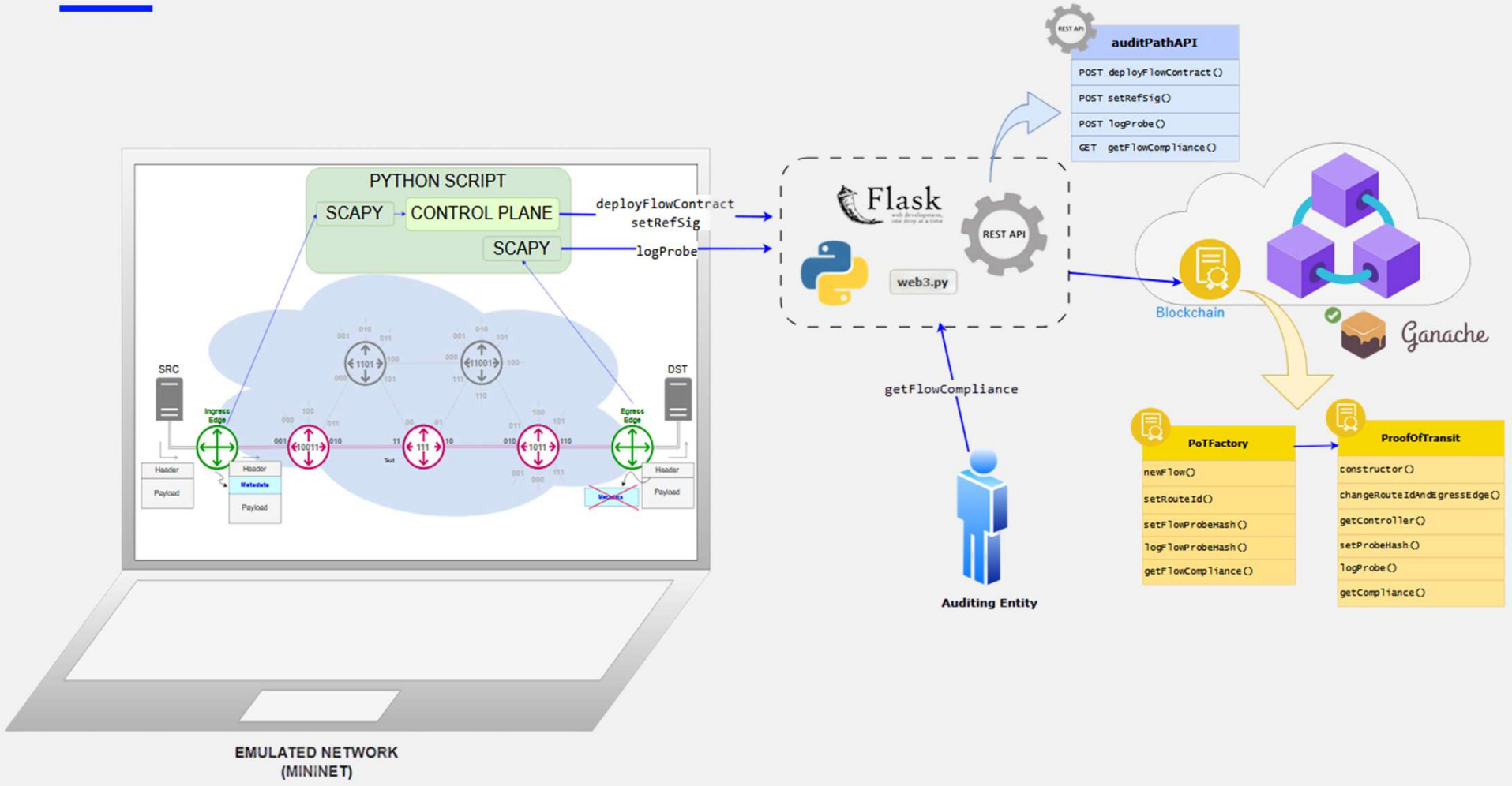
Blockchain em evolução.

Armazenamento de informações para auditoria de caminhos

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

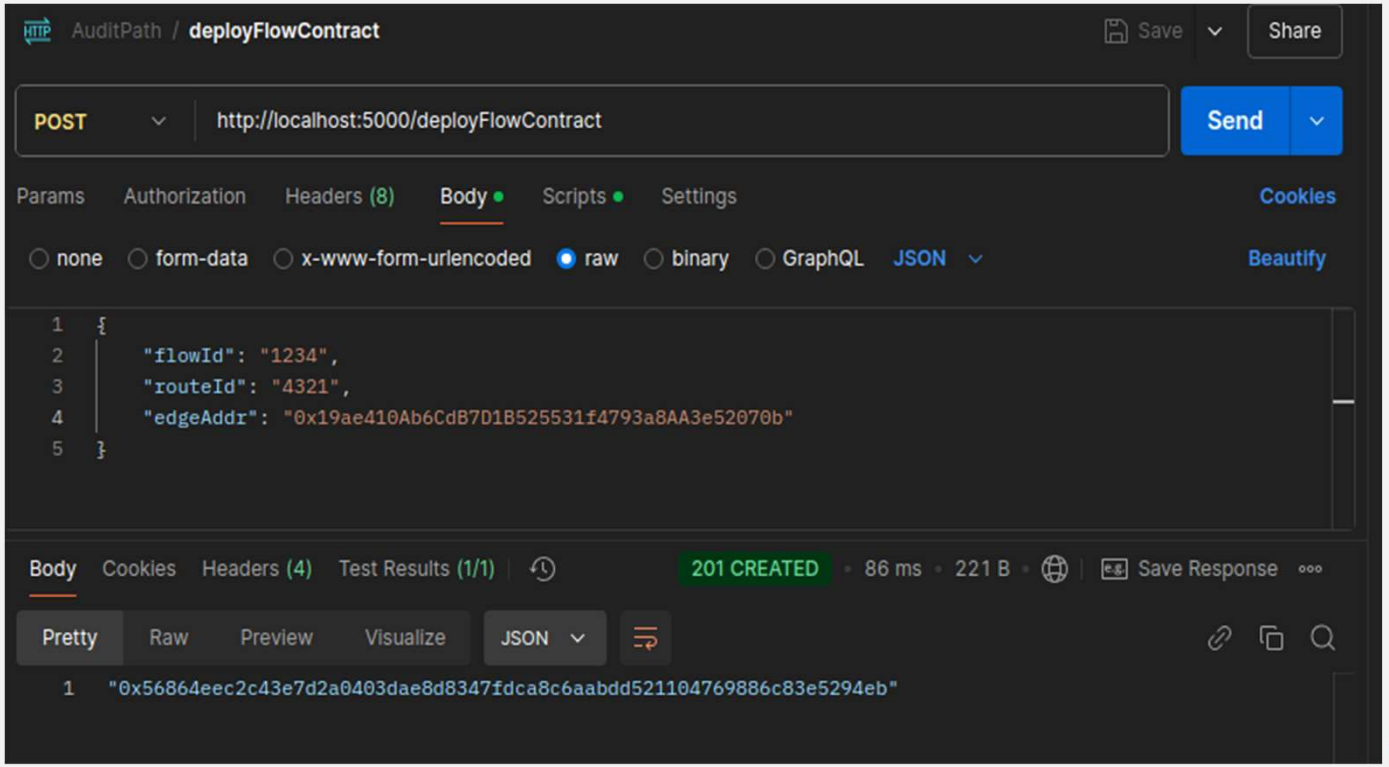


Armazenamento de informações para auditoria de caminhos



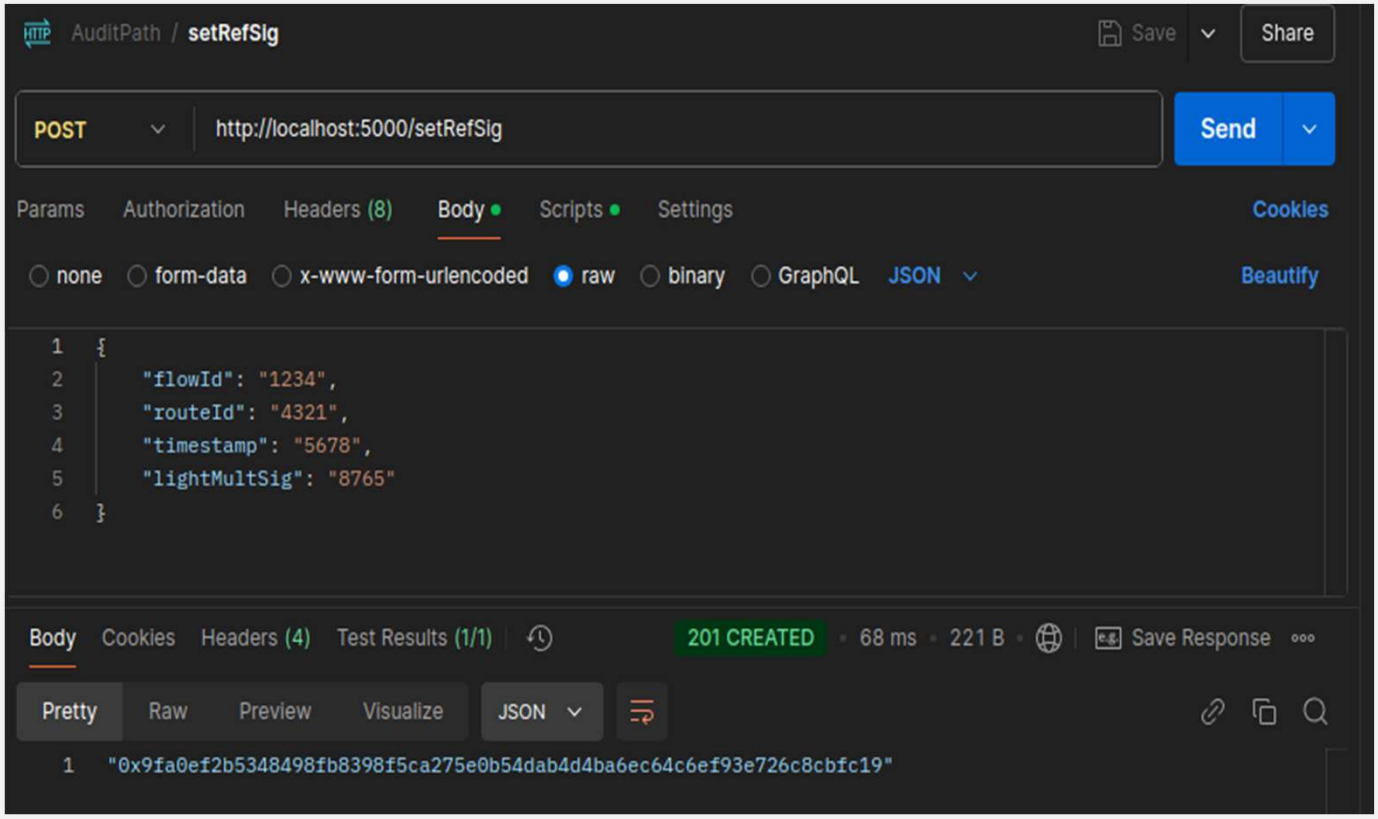
API Rest - Smart Contract

- POST deployFlowContract
- Iniciando um fluxo
- Deploy do contrato



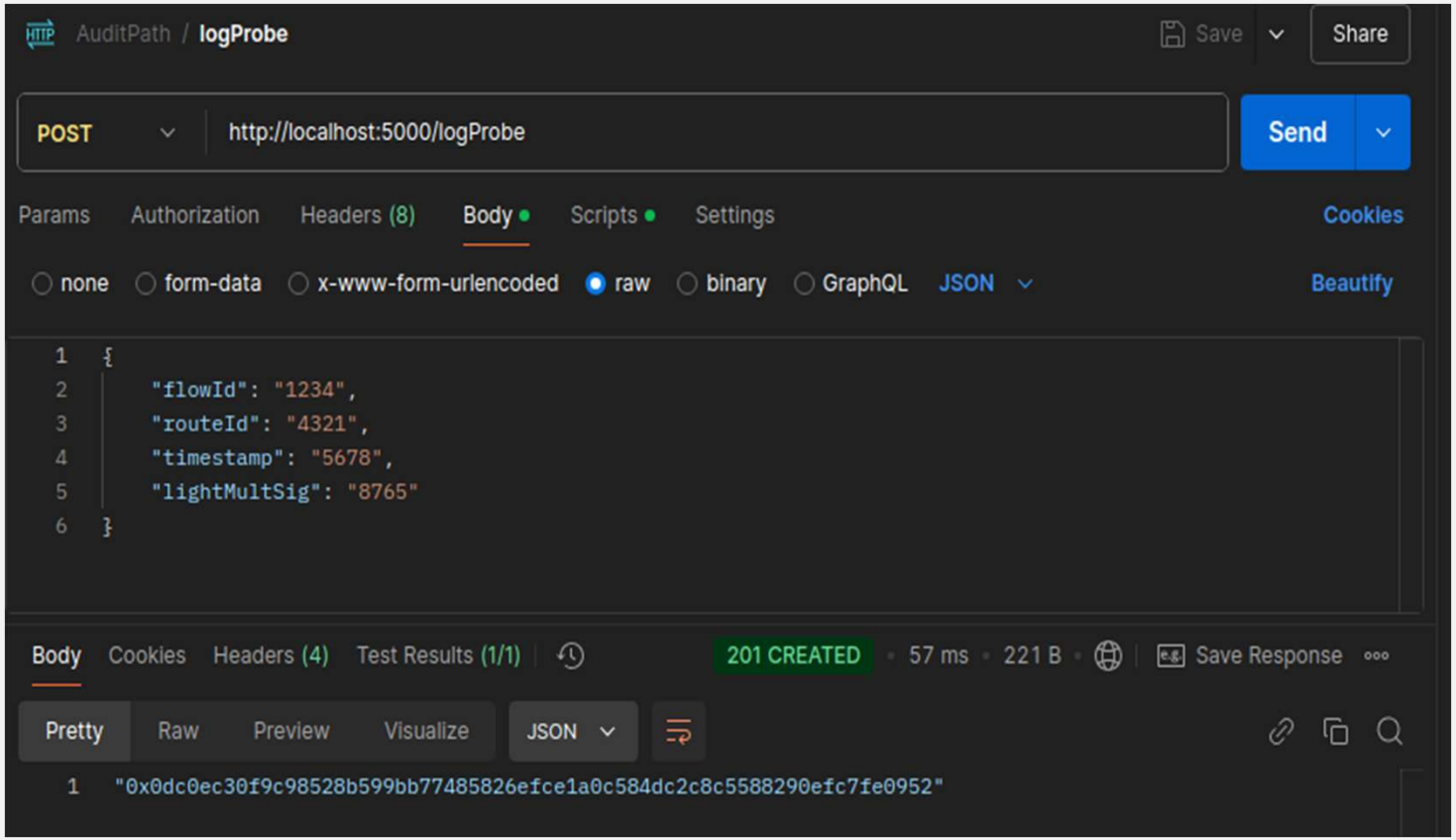
API Rest - Smart Contract

- POST setRefSig
- Definindo assinatura de referência para um determinado RouteId



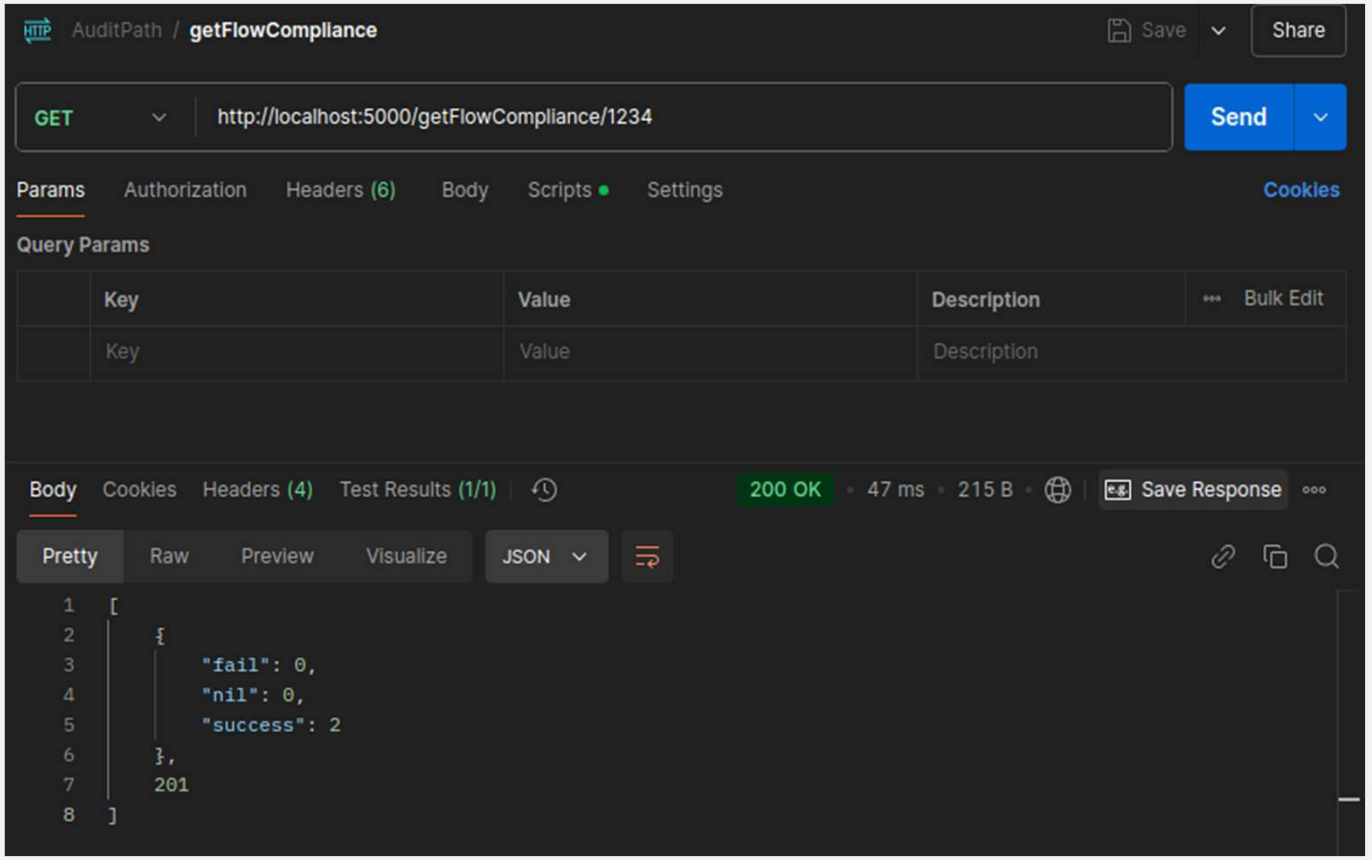
API Rest - Smart Contract

- POST logProbe
- Registrando pelo nó de saída a assinatura gerada na sonda.



API Rest - Smart Contract

- GET getFlowCompliance
- Obtendo os resultados contabilizados



Obrigado

PROJETO ILIADA

CPQD

RNP

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO