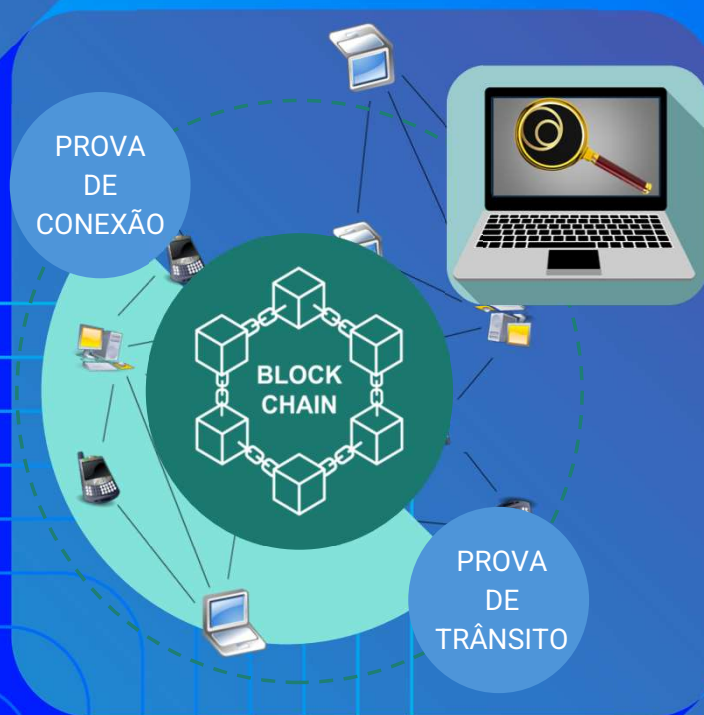


*Blockchain
em evolução.*



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

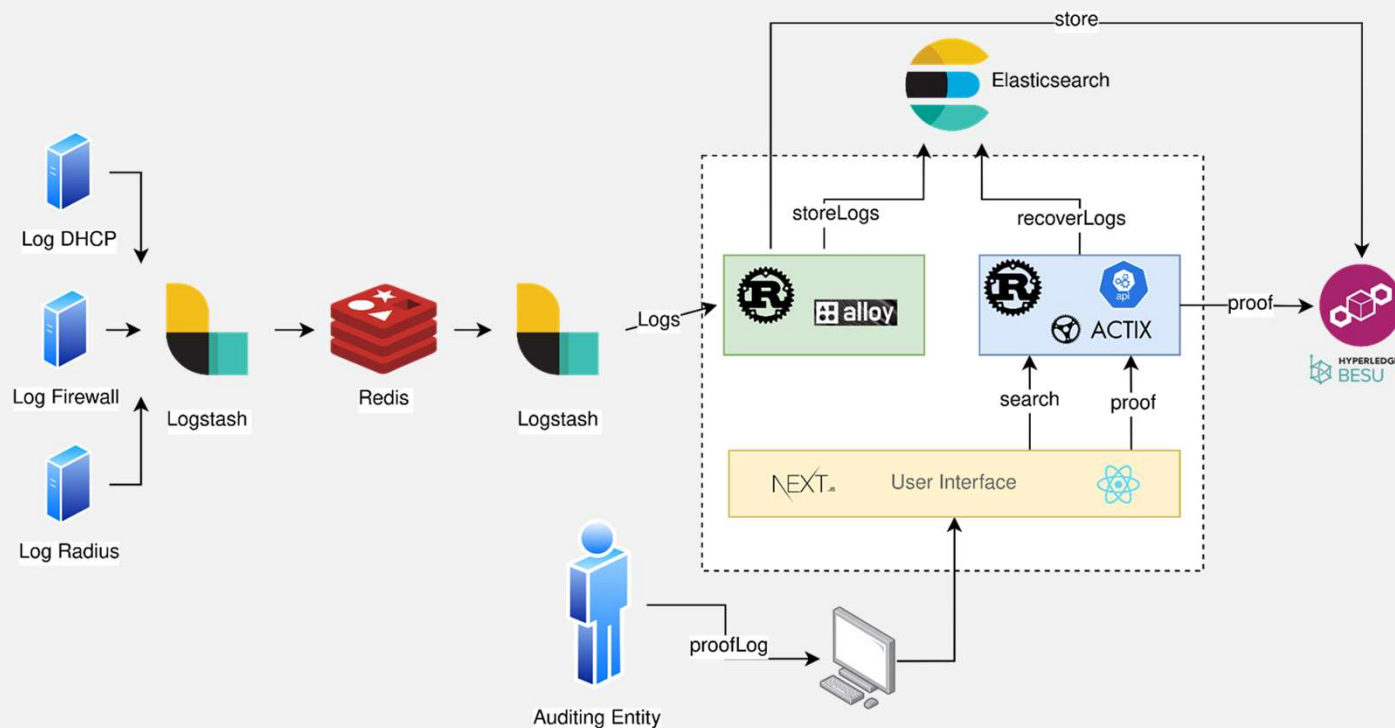
- Adicionar uma camada de armazenamento de informações para verificação dos registros usando blockchain
- Viabilizar a auditabilidade a partir de hashes criptográficos que serão armazenados na blockchain
 - Logs
 - Caminhos percorridos por pacotes
- Garantir transparência e que o acesso pelo ***dispositivo/naquela 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

The screenshot displays the Elastic Search console interface. At the top, the browser address bar shows 'http://localhost:5601/ap'. The main header includes the Elastic logo, a search bar, and navigation tabs for 'Search' and 'Content'. The 'Elasticsearch Indices' section is active, showing a list of 'Available indices'. The table below lists various indices, all with a 'yellow' health status and '100000' documents. Each index is associated with a specific worker ID and an 'API' ingestion method. The 'Ingestion status' for all indices is 'Connected'. The interface also features a sidebar with navigation options like 'Home', 'Content', 'Indices', 'Connectors', 'Web crawlers', 'Build', 'Relevance', and 'Getting started'. The bottom of the screen shows a 'Console' and 'Notebooks' section.

Index name	Index health	Docs count	Ingestion name	Ingestion method	Ingestion status	Actions
2025-04-10_13-06-42-worker-wlumotxq	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-06-47-worker-3eu9zfhq	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-06-52-worker-8jknsjay	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-06-57-worker-gmokq6r3	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-02-worker-ubp997x8	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-07-worker-dxx1isbs	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-12-worker-bobm8fku	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-17-worker-4jgduhmm	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-22-worker-cwy8imow	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-27-worker-ajo5nij	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-32-worker-nnuj9q5n	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-37-worker-jacbxatv	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-42-worker-n4gsasfs	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-47-worker-234bcgf3	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-52-worker-keaqiqnt	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-07-57-worker-bx1r9ddt	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-08-02-worker-kues3lyb	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-08-07-worker-3qzcautv	● yellow	100000		API	Connected	👁️ 🗑️
2025-04-10_13-08-12-worker-ylgmv3rh	● yellow	100000		API	Connected	👁️ 🗑️

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-ajo5nllj (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-keaqiqt (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-n2kfmvei (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-spgjyq3m (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-zly006dy (0bc73dd363ae893dc3c1d083f64a416cb9a4d42fabf02d4efb409c8534940024)
2025-04-10T13:09:30.627955Z INFO audita_server::task::ethereum: ethereum batch processing completed tx_count=100
```

10 Milhões de logs processados

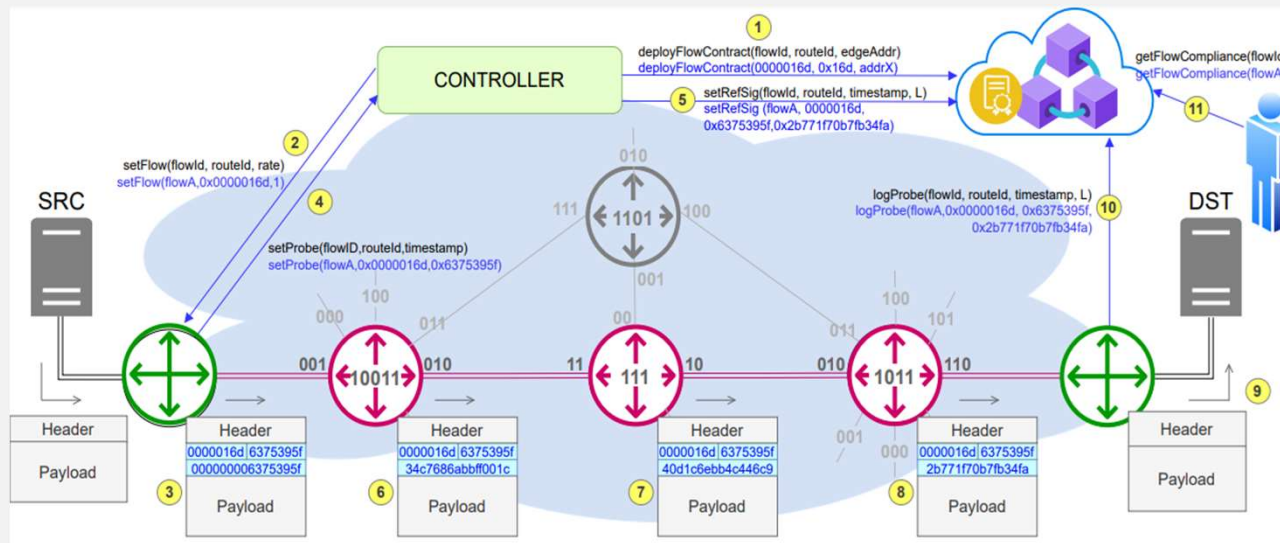
Batch Size de 100 mil -> 100 hashes para a blockchain

Envio para a blockchain em lote

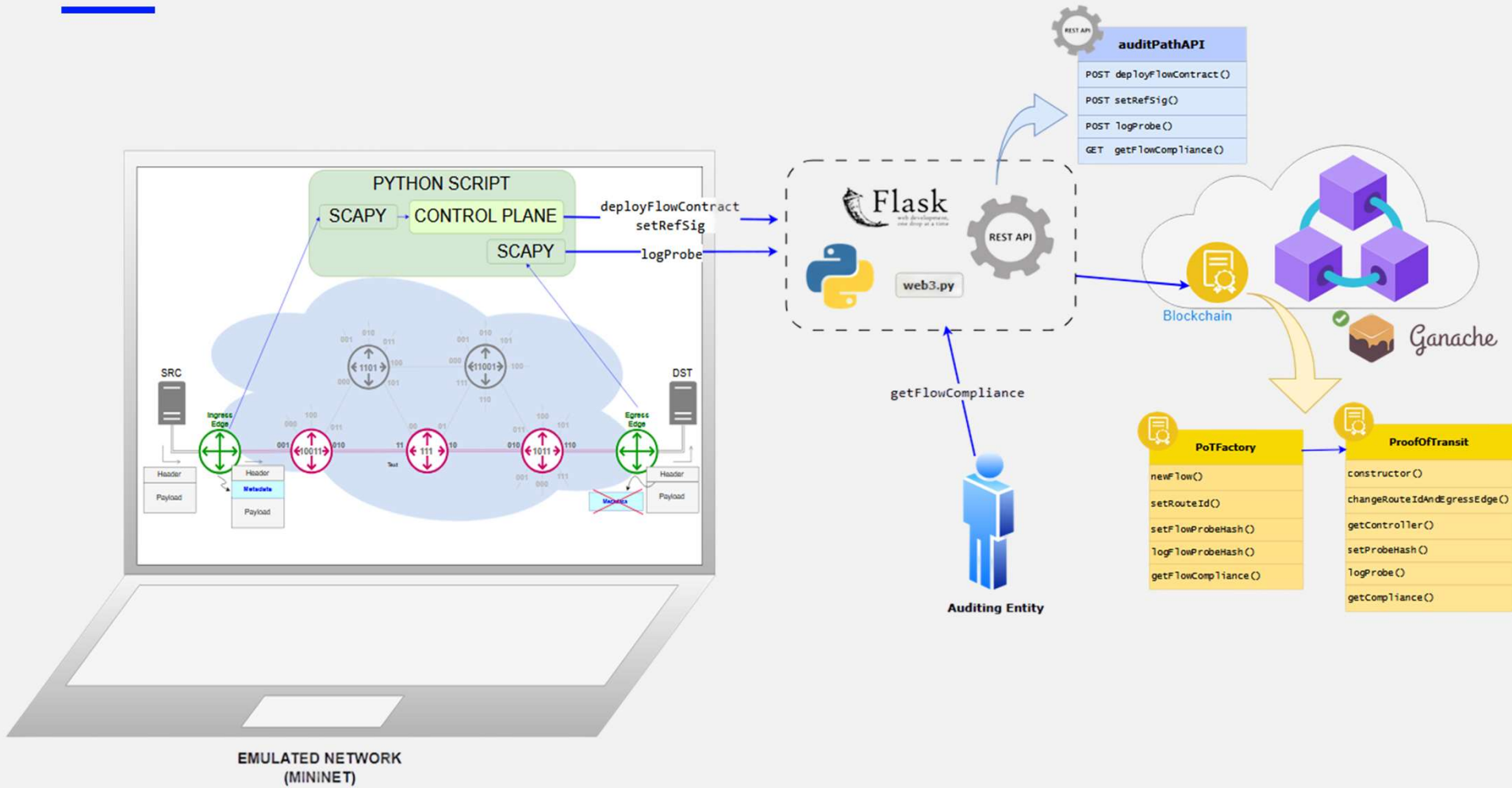


Armazenamento de informações para auditoria de caminhos

- Provedores de acesso precisam atestar que um determinado fluxo de pacotes transitou por um caminho (switches/roteadores) previamente planejado
- Os requisitos específicos para *auditabilidade 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

The screenshot shows a REST client interface for a POST request to `http://localhost:5000/deployFlowContract`. The request body is a JSON object with the following fields:

```
1 {  
2   "flowId": "1234",  
3   "routeId": "4321",  
4   "edgeAddr": "0x19ae410Ab6Cd87D1B525531f4793a8AA3e52070b"  
5 }
```

The response is a single JSON object:

```
1 "0x56864eec2c43e7d2a0403dae8d8347fdca8c6aabdd521104769886c83e5294eb"
```

The status bar indicates a **201 CREATED** response with a duration of 86 ms and a size of 221 B.



API Rest - Smart Contract

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

The screenshot displays a REST client interface for a POST request to `http://localhost:5000/setRefSig`. The request body is a JSON object with the following fields:

```
1 {
2   "flowId": "1234",
3   "routeId": "4321",
4   "timestamp": "5678",
5   "lightMultSig": "8765"
6 }
```

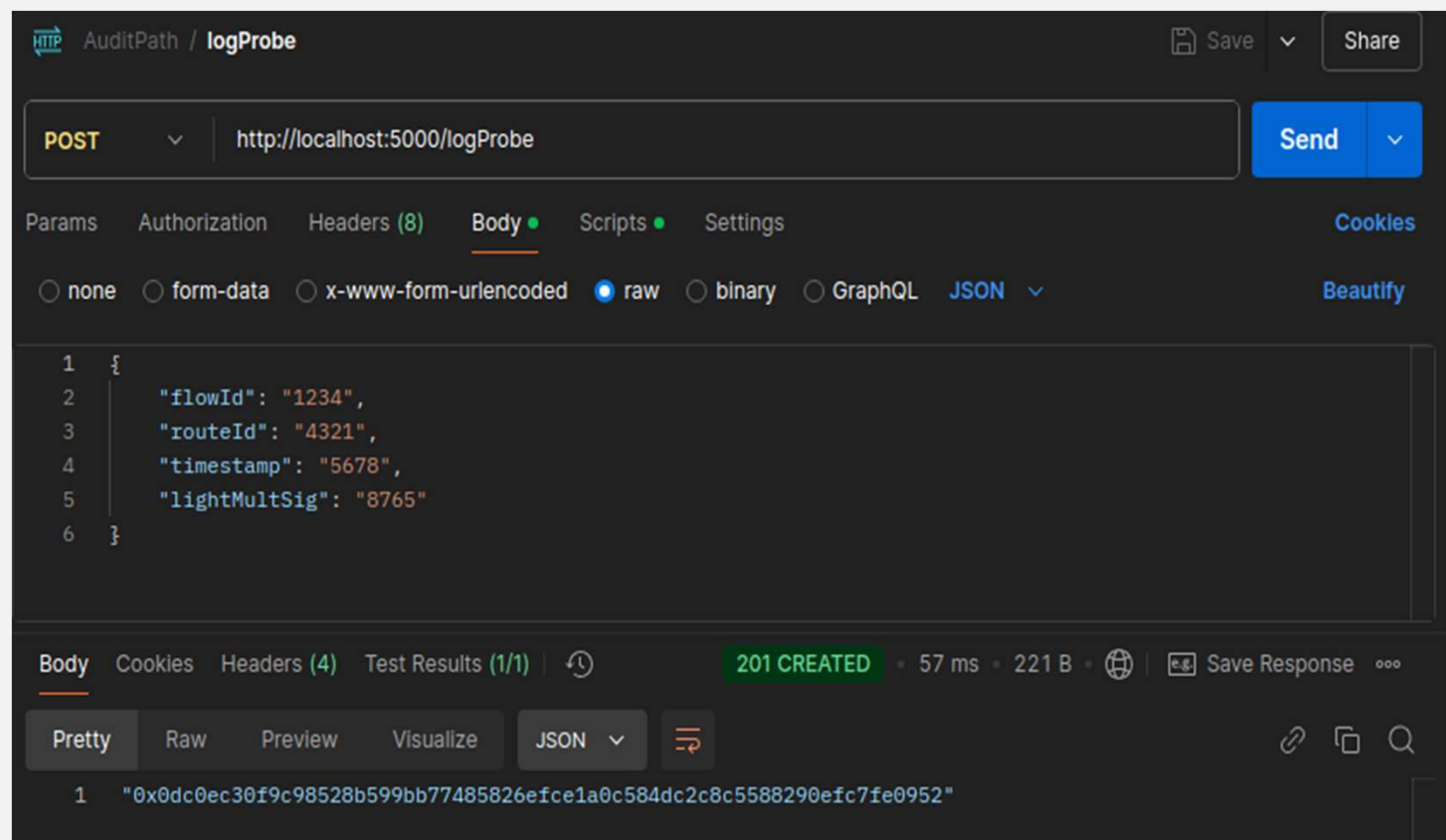
The response is a `201 CREATED` status with a response time of 68 ms and a body size of 221 B. The response body is a long hexadecimal string:

```
1 "0x9fa0ef2b5348498fb8398f5ca275e0b54dab4d4ba6ec64c6ef93e726c8cbfc19"
```



API Rest - Smart Contract

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



AuditPath / logProbe

POST http://localhost:5000/logProbe

Params Authorization Headers (8) **Body** Scripts Settings Cookies Beautify

none form-data x-www-form-urlencoded **raw** binary GraphQL JSON

```
1 {
2   "flowId": "1234",
3   "routeId": "4321",
4   "timestamp": "5678",
5   "lightMultSig": "8765"
6 }
```

Body Cookies Headers (4) Test Results (1/1) 201 CREATED · 57 ms · 221 B Save Response

Pretty Raw Preview Visualize JSON

```
1 "0x0dc0ec30f9c98528b599bb77485826efce1a0c584dc2c8c5588290efc7fe0952"
```



API Rest - Smart Contract

- GET getFlowCompliance
- Obtendo os resultados contabilizados

HTTP AuditPath / getFlowCompliance

GET http://localhost:5000/getFlowCompliance/1234

Params Authorization Headers (6) Body Scripts Settings Cookies

Query Params

Key	Value	Description	Bulk Edit
Key	Value	Description	

Body Cookies Headers (4) Test Results (1/1) 200 OK · 47 ms · 215 B Save Response

Pretty Raw Preview Visualize JSON

```
1 [
2   {
3     "fail": 0,
4     "nil": 0,
5     "success": 2
6   },
7   201
8 ]
```





Obrigado



MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

