Towards Secure, Decentralized, and Automatic Audits with Blockchain

Rafael Belchior

rafael.belchior
@tecnico.ulisboa.pt

André Vasconcelos

andre.vasconcelos
@tecnico.ulisboa.pt

Miguel Correia

miguel.p.correia
@tecnico.ulisboa.pt

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

inesc id lisboa

QualiChain

Outline

Context

- Audits & Motivation
- Objectives
- JusticeChain

Solution, Evaluation

- JusticeChain v2.0
- Evaluation

Conclusion

- Future Work
- Conclusions

Context

Audits

- Audits are expensive and necessary to businesses, including in public administration.

- Auditing processes utilise audit files and address validation, attribution and evidence.

- Access control systems record actions from subjects and stored, and create logs which can be used in audits - audit logs.

Problems with audit logs

- ❑ Audit logs are typically saved on centralized databases - single point of failure
- ❑ They are vulnerable to attacks where adversaries can tamper data
- ❑ The analysis of logs are made *post festum*, sometimes taking a long time for organizations to realize so
- ❑ There can be distinct stakeholders with different roles and different levels of trust with different access rights to data

Objective

- Conduct semi-automatic audits, distributing trust amongst the stakeholders.

Previous Work: JusticeChain

- ❑ Citius manages judicial courts' processes

- ❑ Important to the well functioning of justice

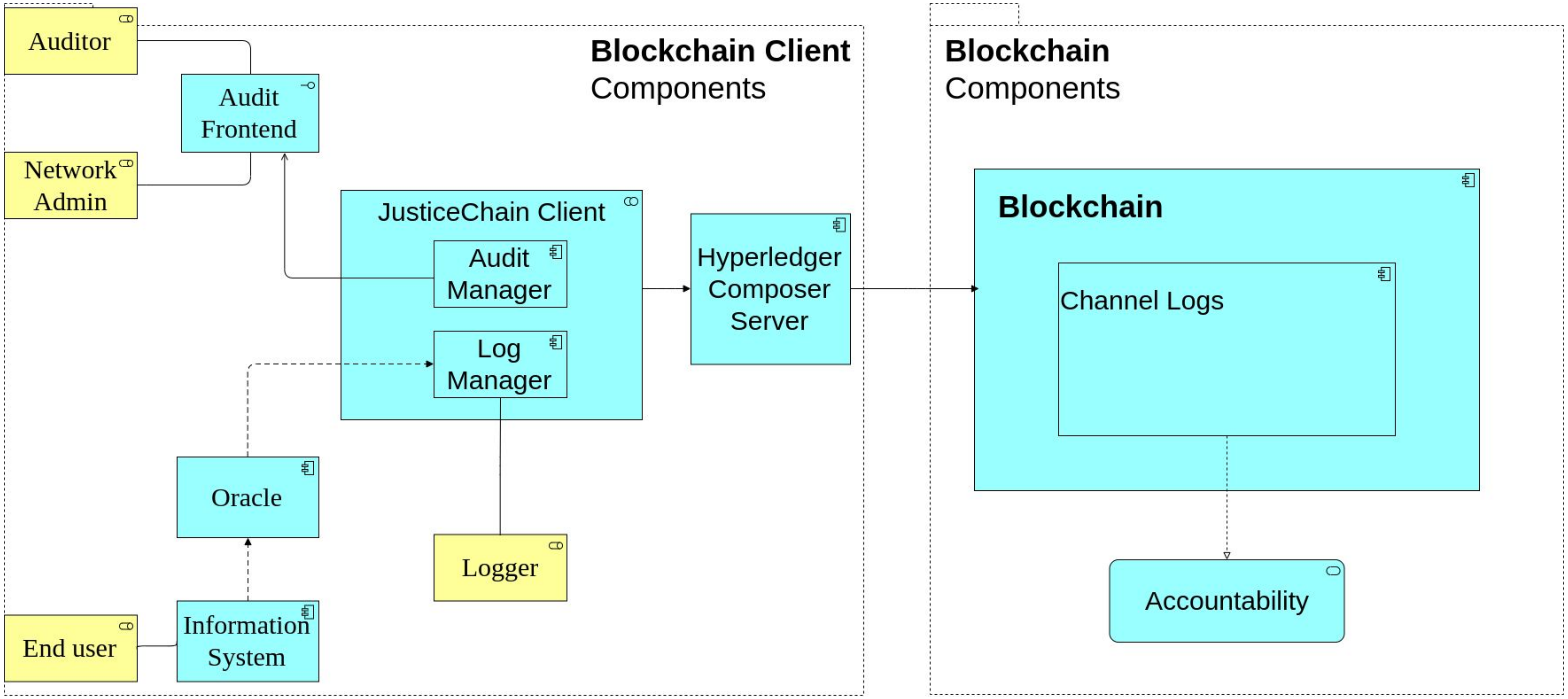
Citius

IGFEJ
INSTITUTO DE GESTÃO
FINANCEIRA E EQUIPAMENTOS
DA JUSTIÇA I.P.

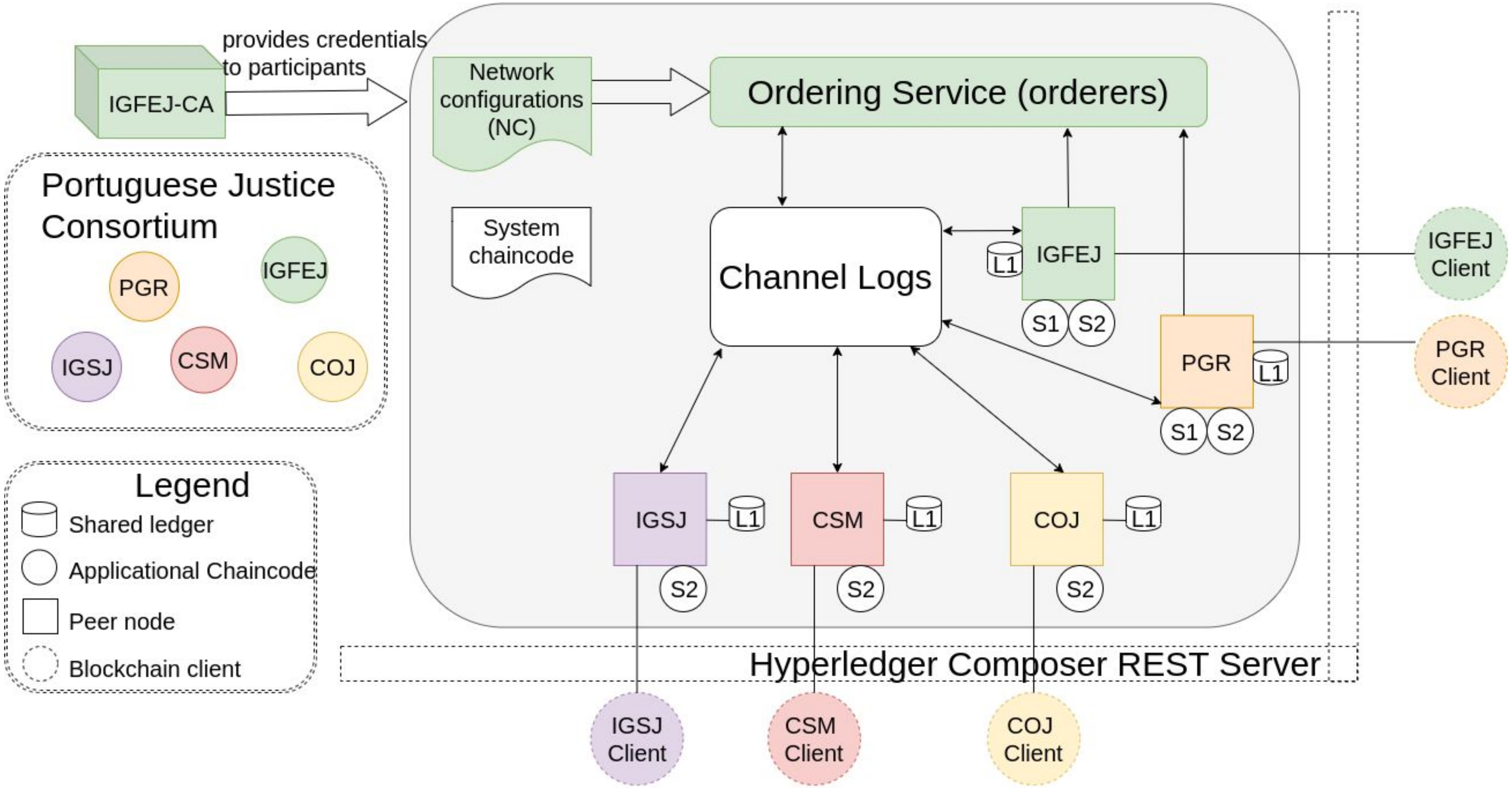
JusticeChain

- JusticeChain, a blockchain-based system for protecting and managing accesses to logs
- Blockchain Component: Permissioned, private blockchain
- Blockchain Client Components
- Implemented with Hyperledger Composer

JusticeChain Overview



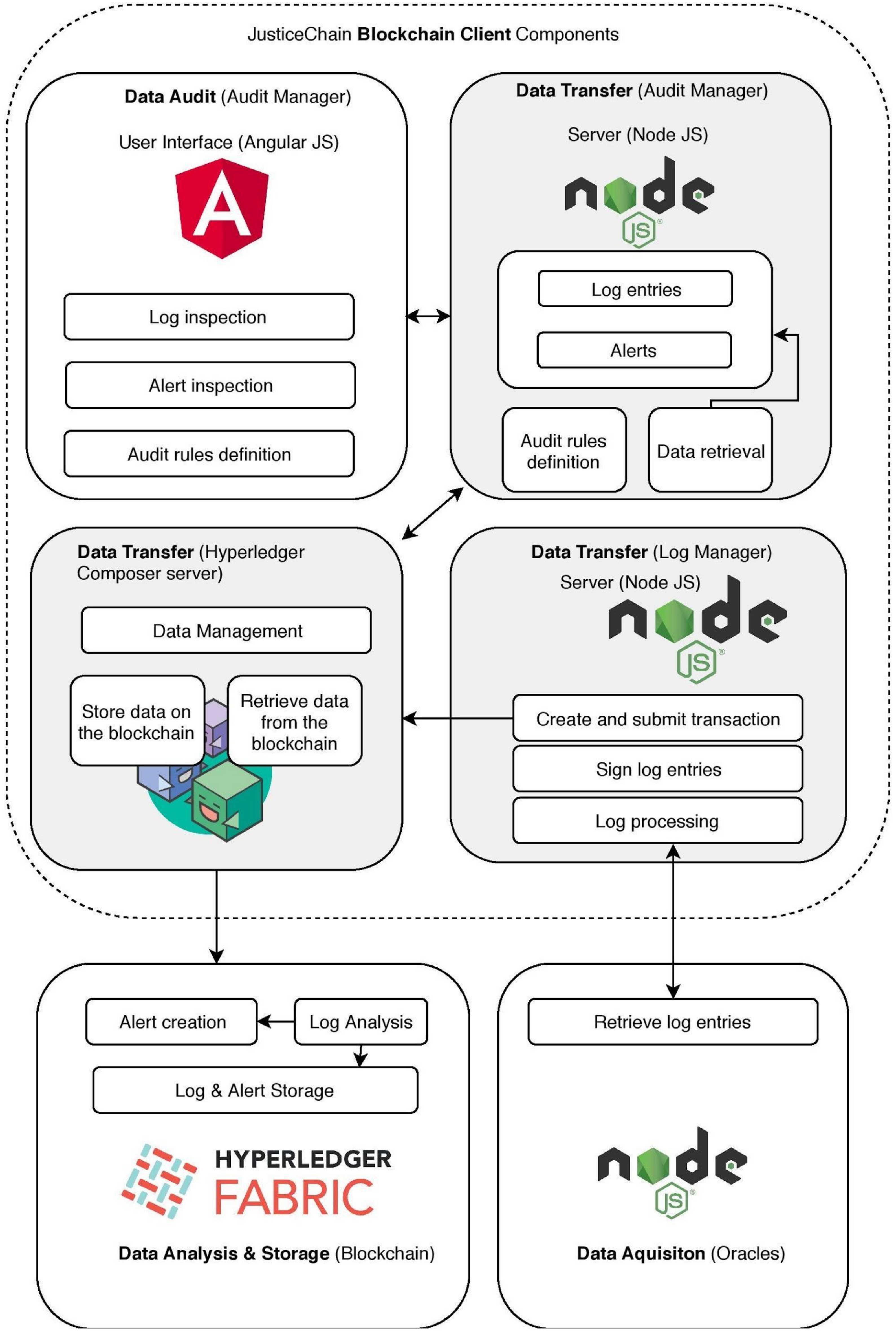
JusticeChain: Blockchain Components



Solution

Solution: JusticeChain v2.0

- Log preprocessing (compaction and minimization)
- Automatic analysis (distributed smart contract execution)
- Event emission: new log, new alert, audit started, audit stopped, permission changes
- Four-layered approach

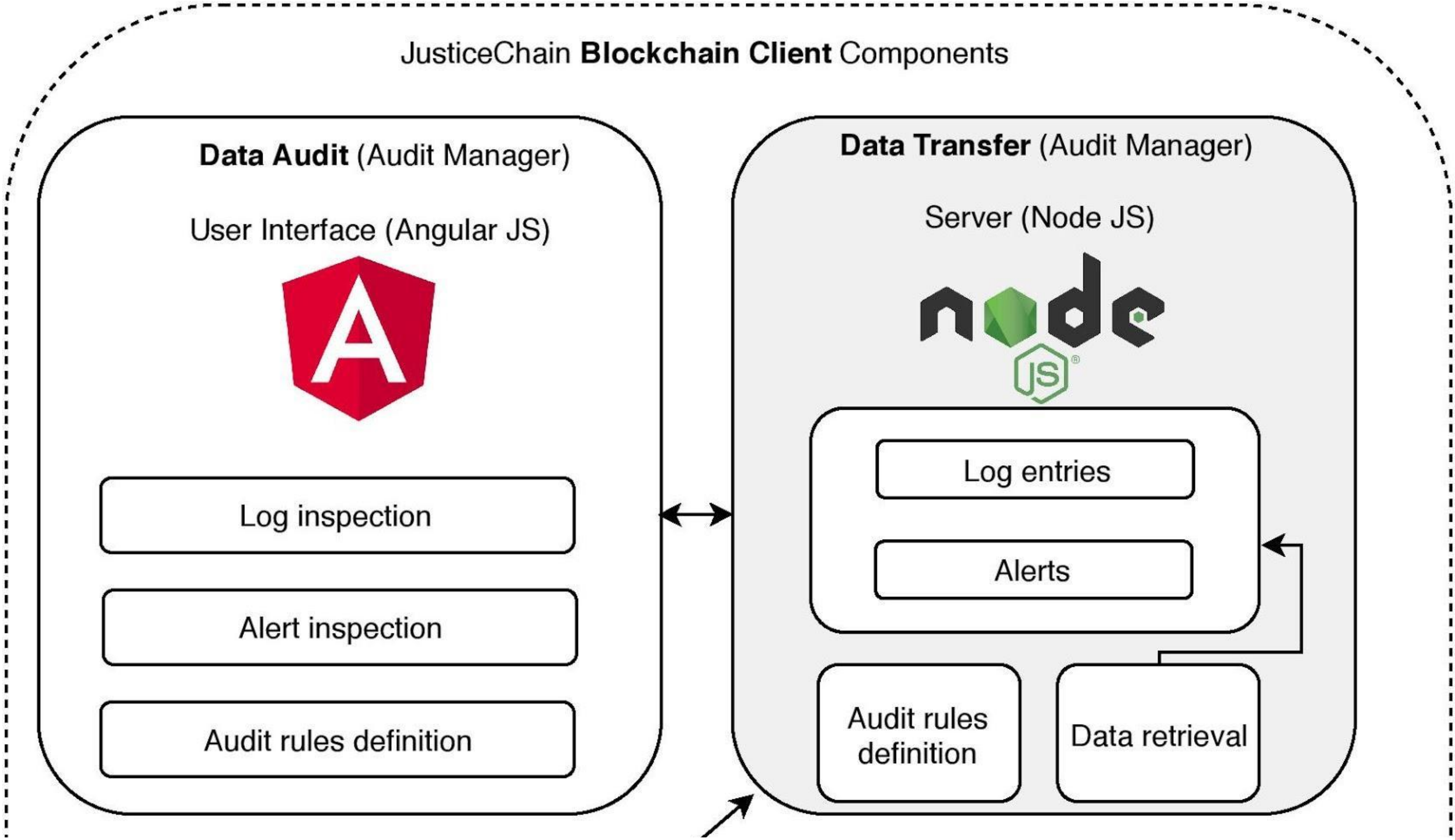

JusticeChain Blockchain Client Components
Data Audit (Audit Manager)
User Interface (Angular JS)
Log inspection
Alert inspection
Audit rules definition
Data Transfer (Audit Manager)
Server (Node JS)
Log entries
Alerts
Audit rules definition
Data retrieval
Data Transfer (Hyperledger Composer server)
Data Management
Store data on the blockchain
Retrieve data from the blockchain
Data Transfer (Log Manager)
Server (Node JS)
Create and submit transaction
Sign log entries
Log processing
Alert creation
Log Analysis
Log & Alert Storage
HYPERLEDGER FABRIC
Data Analysis & Storage (Blockchain)
Retrieve log entries
Data Aquisiton (Oracles)

Solution

- Audit access control done via a Allow Audit transaction

- An auditor can access logs when has a certain threshold of authorizations

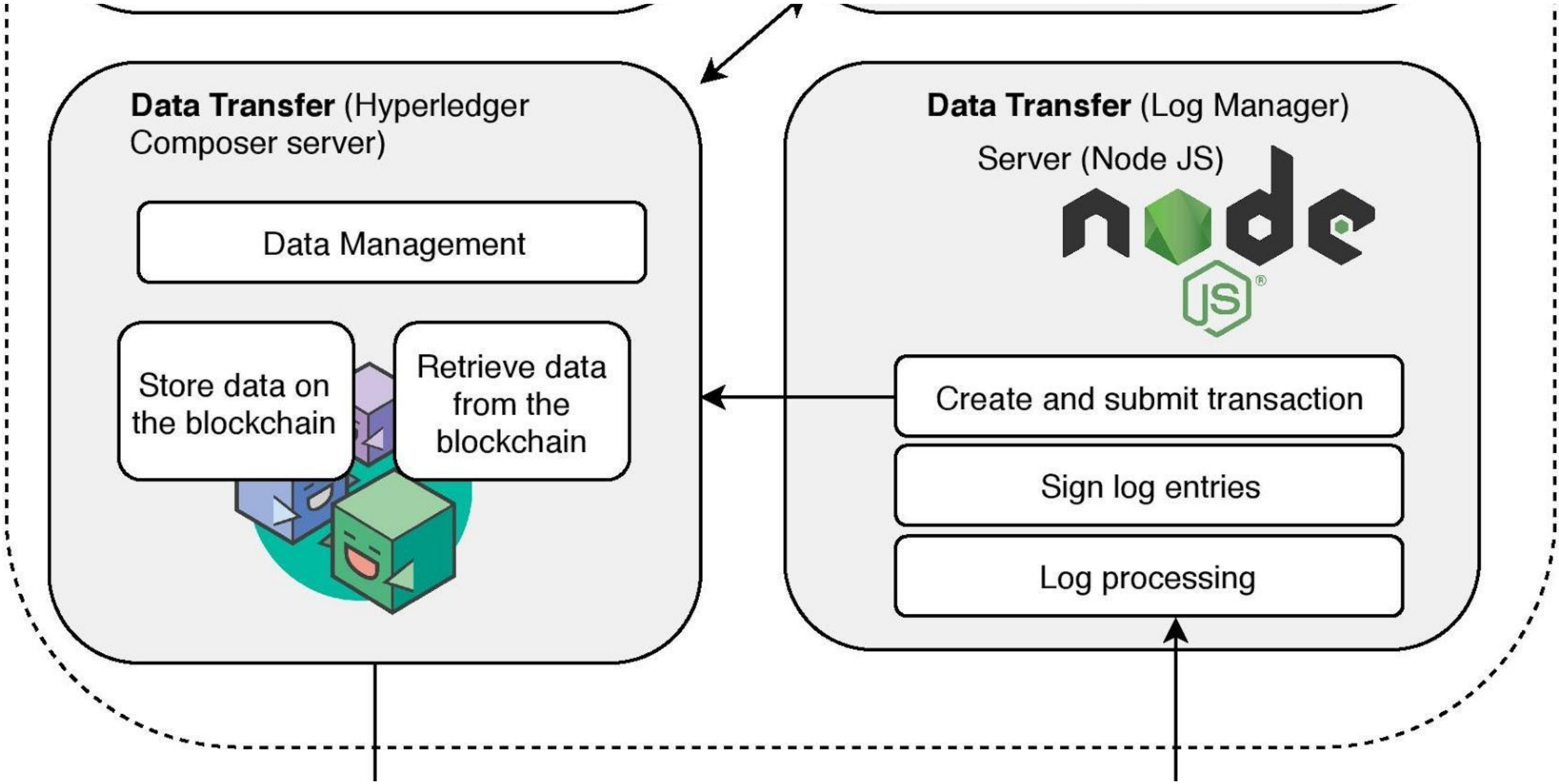
- Upon log retrieval, permissions are reset; logs are marked as visited


JusticeChain **Blockchain Client** Components
Data Audit (Audit Manager)
User Interface (Angular JS)
Log inspection
Alert inspection
Audit rules definition
Data Transfer (Audit Manager)
Server (Node JS)
node JS
Log entries
Alerts
Audit rules definition
Data retrieval

Solution

- Data transfer layer redirects data after processing

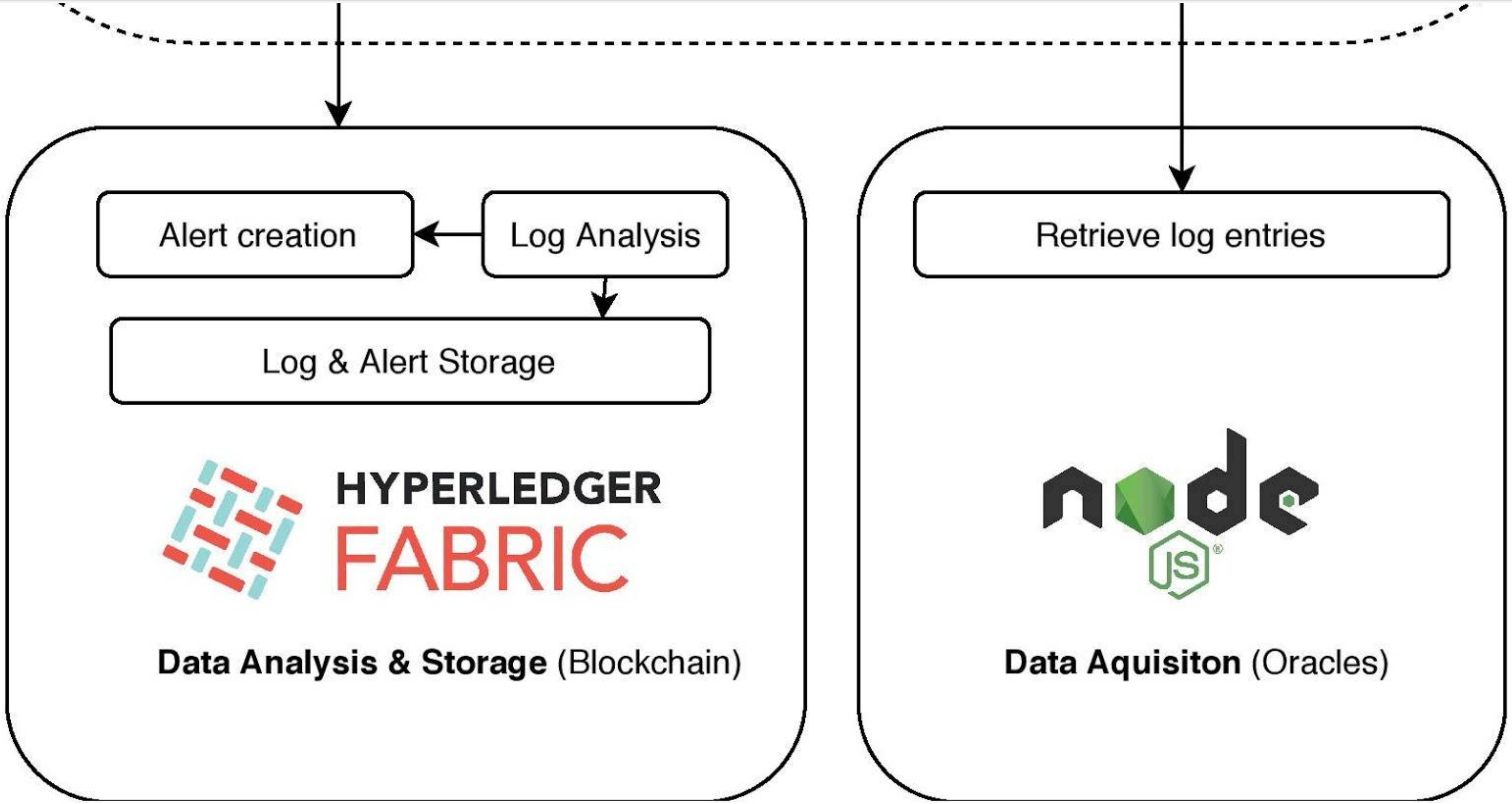
- Data processing is signed by the processor (i.e., Logger)



Data Transfer (Hyperledger Composer server)
Data Management
Store data on the blockchain
Retrieve data from the blockchain
Data Transfer (Log Manager)
Server (Node JS)
node JS
Create and submit transaction
Sign log entries
Log processing

Solution

- ❑ Data on-chain vs off-chain
- ❑ Smart contract execution creates alerts upon certain patterns detected



Evaluation

Solution Evaluation

- Evaluation Methodology
- Setup
- Throughput and latency
- Storage

HYPERLEDGER CALIPER

Methodology

- What is the throughput rate JusticeChain can achieve, i.e., how many audit logs can it save per second?

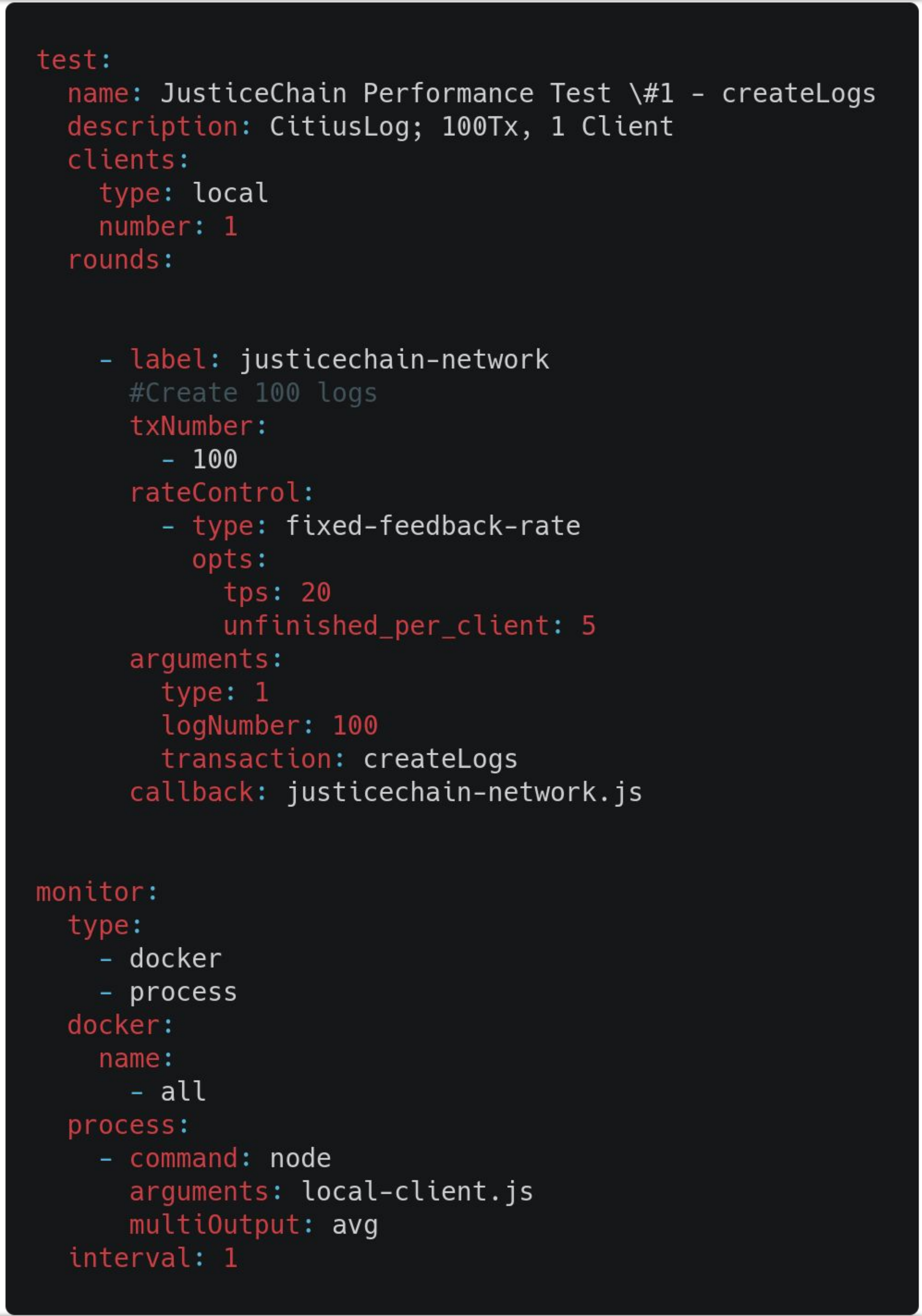
- What is the latency of JusticeChain, i.e., what is the time window needed for logs to be secured, and analysed?

- What is the cost, in terms of storage, of protecting logs, i.e., what is the scalability of JusticeChain? (see paper)

Setup

- ❑ 2 orgs, 2 peers
- ❑ 1 channel
- ❑ Solo orderer
- ❑ Variable number of clients/Loggers
- ❑ Backlog rate controller

- ❑ Google Cloud: London,UK with 16vCPU and 60GB of memory, and a 50GB SSD



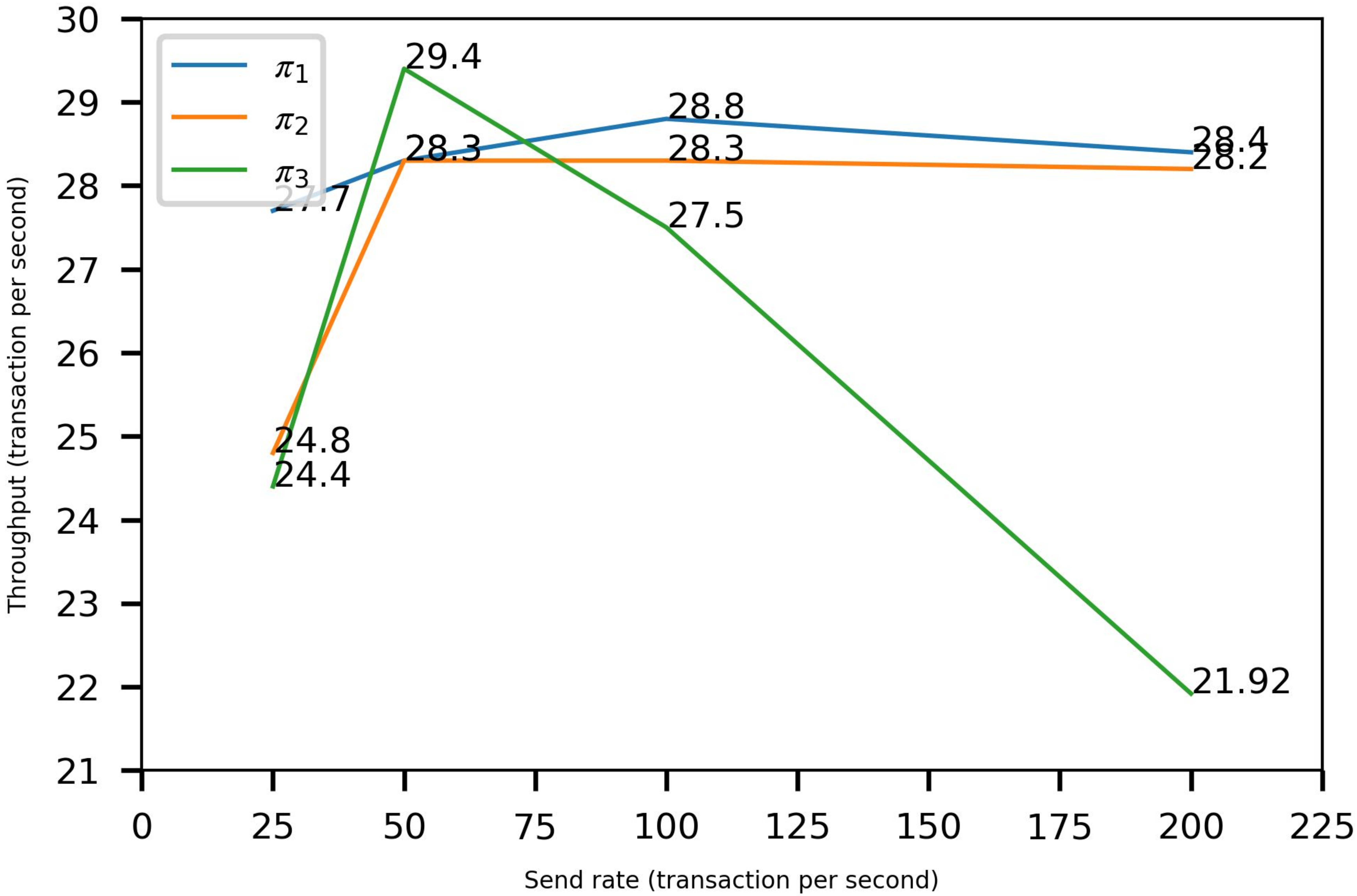
```
test:
  name: JusticeChain Performance Test \#1 - createLogs
  description: CitiusLog; 100Tx, 1 Client
  clients:
    type: local
    number: 1
  rounds:


    - label: justicechain-network
      #Create 100 logs
      txNumber:
        - 100
      rateControl:
        - type: fixed-feedback-rate
          opts:
            tps: 20
            unfinished_per_client: 5
      arguments:
        type: 1
        logNumber: 100
        transaction: createLogs
      callback: justicechain-network.js


monitor:
  type:
    - docker
    - process
  docker:
    name:
      - all
  process:
    - command: node
      arguments: local-client.js
      multiOutput: avg
  interval: 1
```

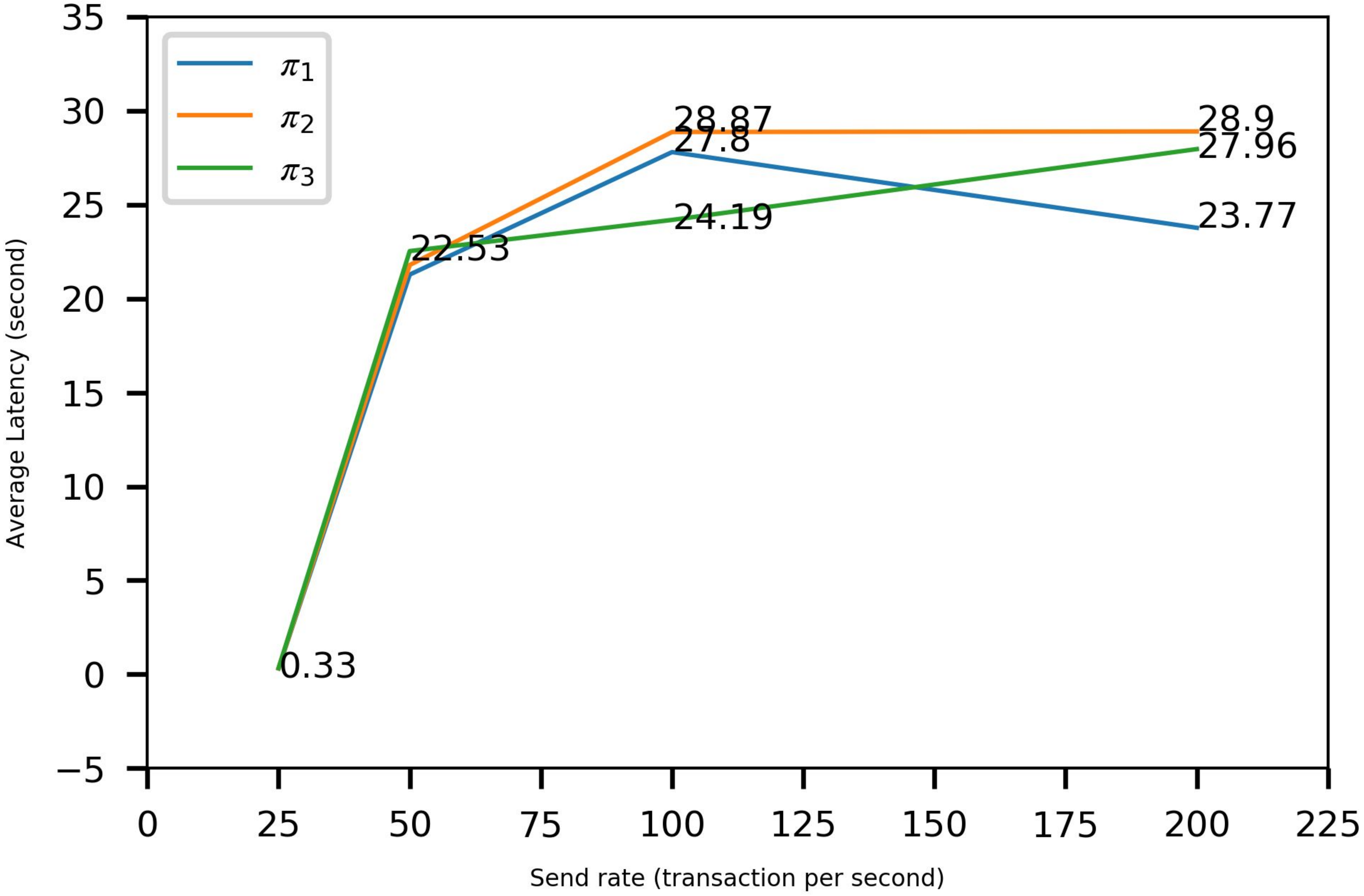
JusticeChain: **Throughput** and Latency

- Dummy audit rule policies, that perform a certain number of operations on 20 available attributes.
- π1 = 1
- π2 =20
- π3 =100



JusticeChain: Throughput and **Latency**

- π1 =1
- π2 =20
- π3 =100



Conclusions

Limitations

- ❑ We meaningful audit rules

- ❑ Low performance limited by Composer might not be suitable for production

Wrap up

- ❑ An audit is an expensive, time-consuming process that can benefit from automation, given that trust in that process is distributed by the stakeholders.
- ❑ We provide a blockchain-based solution that promotes the automation of audit log analysis and accountability, allowing to reduce the cost of audits and increase synergies between stakeholders.
- ❑ Upon performance improvement, this solution is suitable for production.

Future Work

- ❏ Dynamic adjusting of audit rules via a trusted oracle
- ❏ Study general data protection regulation implications
- ❏ Dynamic consortium adjustment via an on-chain policy administration point

TÉCNICO LISBOA

inesc id lisboa

Towards Secure, Decentralized, and Automatic Audits with Blockchain

Rafael Belchior

rafael.belchior
@tecnico.ulisboa.pt

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

inesc id lisboa

QualiChain