

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/342735438>

# JusticeChain: Using Blockchain To Protect Justice Data

Thesis · December 2019

CITATION  
1

1 author:



Rafael Belchior  
Instituto Superior Técnico

44 PUBLICATIONS 474 CITATIONS

SEE PROFILE

READS  
743

# JusticeChain: Using Blockchain to Protect Justice Data

## Advisors

André Vasconcelos  
Miguel Correia

Rafael Belchior

rafael.belchior@tecnico.ulisboa.pt

December 2019

- ❑ Citius manages judicial courts' processes
- ❑ Important to the well functioning of justice

**Citius** 



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



Página temporariamente indisponível

Vimos por este meio informar que por motivos de realização de intervenções técnicas imprescindíveis, a plataforma CITIUS, estará indisponível até às 23h59m do dia 31 agosto 2014 (domingo).

Agradecemos a vossa compreensão e pedimos desculpa por possíveis incómodos causados.

34 | DESPORTO

**PAULO GONÇALVES**  
**INTERVÊM EM NEGÓCIOS DO BENFICA**  
**PROFUTE** Ex-assessor jurídico das águias abriu uma empresa de agenciamento de jogadores em janeiro e, entre outras intervenções, esteve envolvido na renovação de Salvio e na contratação do avançado Cádiz

**SOBE KIM CLIJSTERS**  
TENISTA  
A belga, de 36 anos, vai voltar aos 'courts' em 2020. A ex-nº1 mundial é mãe de 3 filhos e já conquistou 4 títulos do Grand Slam.

**GRE POF TREN**

**MÁRIO FIGUEIREDO**

**P**aulo Gonçalves esteve envolvido em pelo menos cinco negócios efetuados pelo Benfica, quatro contratações e uma renovação de contrato (Salvio, em janeiro), apurou o **Correio da Manhã**.

O advogado, antigo assessor jurídico do Benfica - deixou a Luz em setembro de 2018 - e arquiado no processo E-Toupeira (**ver caixa**) participou nas transferências de Bernardo Martins e Pedro Henriques do Leixões para o Benfica a troca de 1,6 milhões de euros. São ambos representados pelo agente António Teixeira. O médio ofensivo, de 21 anos, nem aqueceu o lugar na equipa B dos encarnados e foi cedido ao P. Ferreira. Já o avançado, de 22 anos, participou em quatro jogos dos bés.

Paulo Gonçalves interveio também na contratação do avançado brasileiro João Borges, de 19 anos, que saltou do Berço Sport Clube (Guimarães) para a equipa de sub-23 das águias. E igualmente terá tido um papel ativo na contratação do colombiano Cádiz ao V. Setúbal por um valor a rondar os três milhões de euros. Mais um juras de amor aos encarnados acabou por sair do clube seis meses depois para o Boca Juniors, num processo conturbado que rendeu oito milhões de euros às águias.

O Benfica não confirmou ao **CM** a intervenção de Paulo Gonçalves em nenhum destes negócios, mas admitiu que o advogado possa ter participado nas negociações a pedido dos referidos jogadores ou dos seus empresários.

A experiência Gonçalves também poderá ter sido requerida por 'Toto' Salvio aquando do processo de renovação de contrato com o Benfica.

Em janeiro, Paulo Gonçalves abriu uma empresa de agenciamento de futebolistas. A Profute Consultoria Unipessoal LDA diz que fornece serviços de consultoria e assessoria. Tem escritório em Lisboa e parcerias com profissionais sediados no Porto, Londres, Bruxelas, Split, Buenos Aires, Rio de Janeiro, Montevideo e Dubai. ●

**EX-DIRIGENTE RESPONDE POR 50 CRIMES**

**E**x-assessor jurídico do Benfica Paulo Gonçalves vai responder em tribunal por 50 crimes no processo E-Toupeira: um crime de corrupção ativa, seis de violação de segredo de Justiça, 21 de violação de segredo de Justiça por funcionário, 11 por acesso indevido e outros 11 por violação do dever de sigilo.

Além de Paulo Gonçalves vão ser ainda julgados Júlio Loureiro e José Augusto Silva, ambos funcionários judiciais, que responderem, respetivamente, por 47 e 75 crimes.

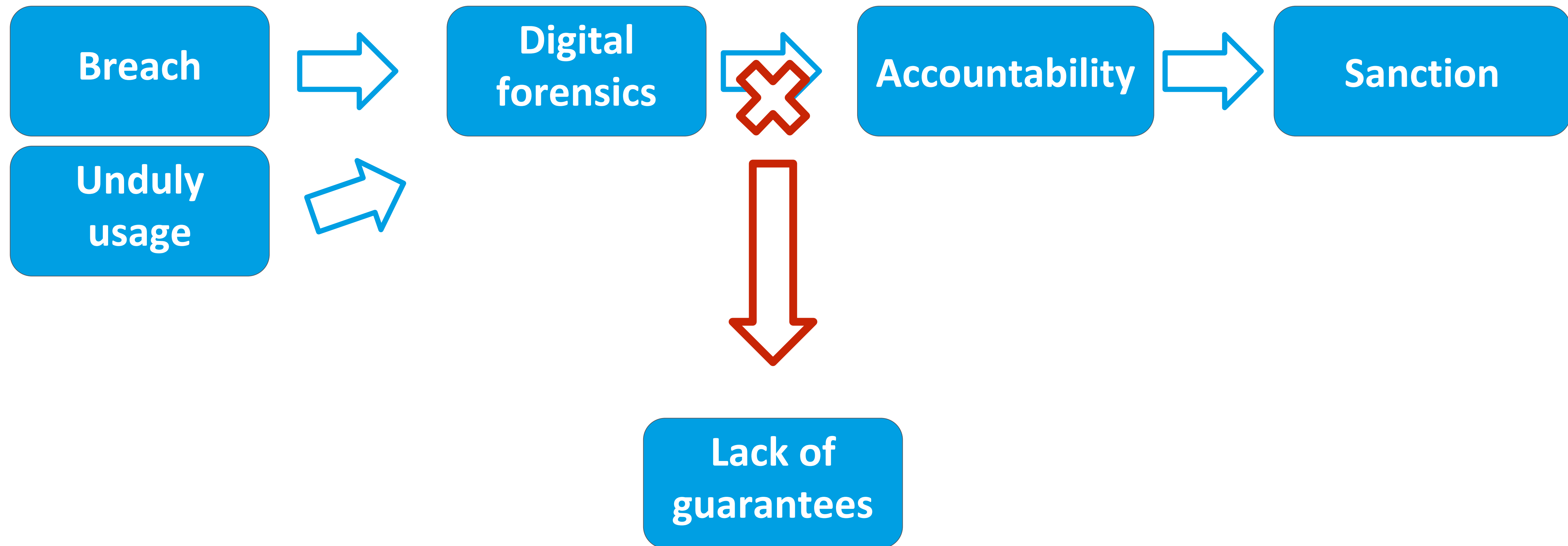
Já a Benfica SAD, que chegou a ser acusada por 30 crimes, não vai a julgamento. ●

**gravidade dos crimes imputados aos arguidos num recurso interposto por um funcionário judicial. ●**

**Bastava mudar as passwords**  
**E** O acesso ao sistema informático Citius era simples. Bastava José Silva 'errar' três vezes na password de um magistrado que não acesse ao sistema. O computador pedia nova senha, o que o próprio criava. A partir daí, entrava nos processos e acedia à informação. ●

**Ofendidos por...**





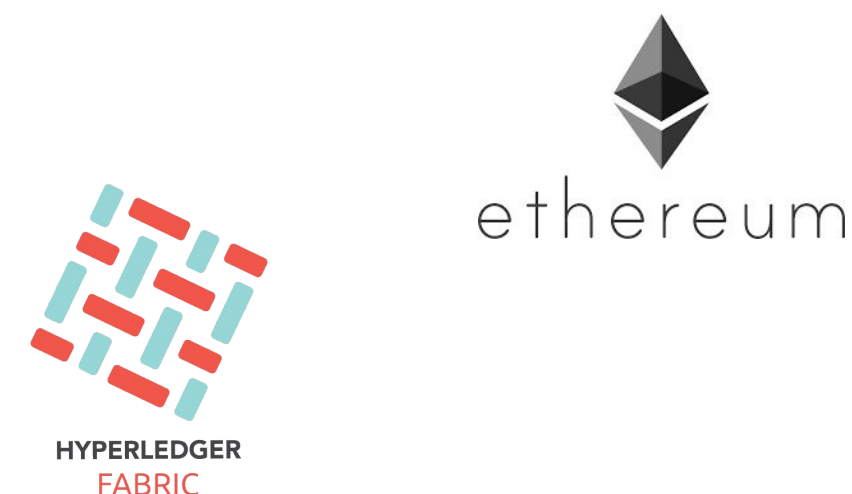
❏ Ultimately, attackers can get away

- ❏ How to increase the resiliency of audit logs at the Portuguese justice?

- ❑ Guarantee audit logs' integrity (and availability)
- ❑ Control access to audit logs

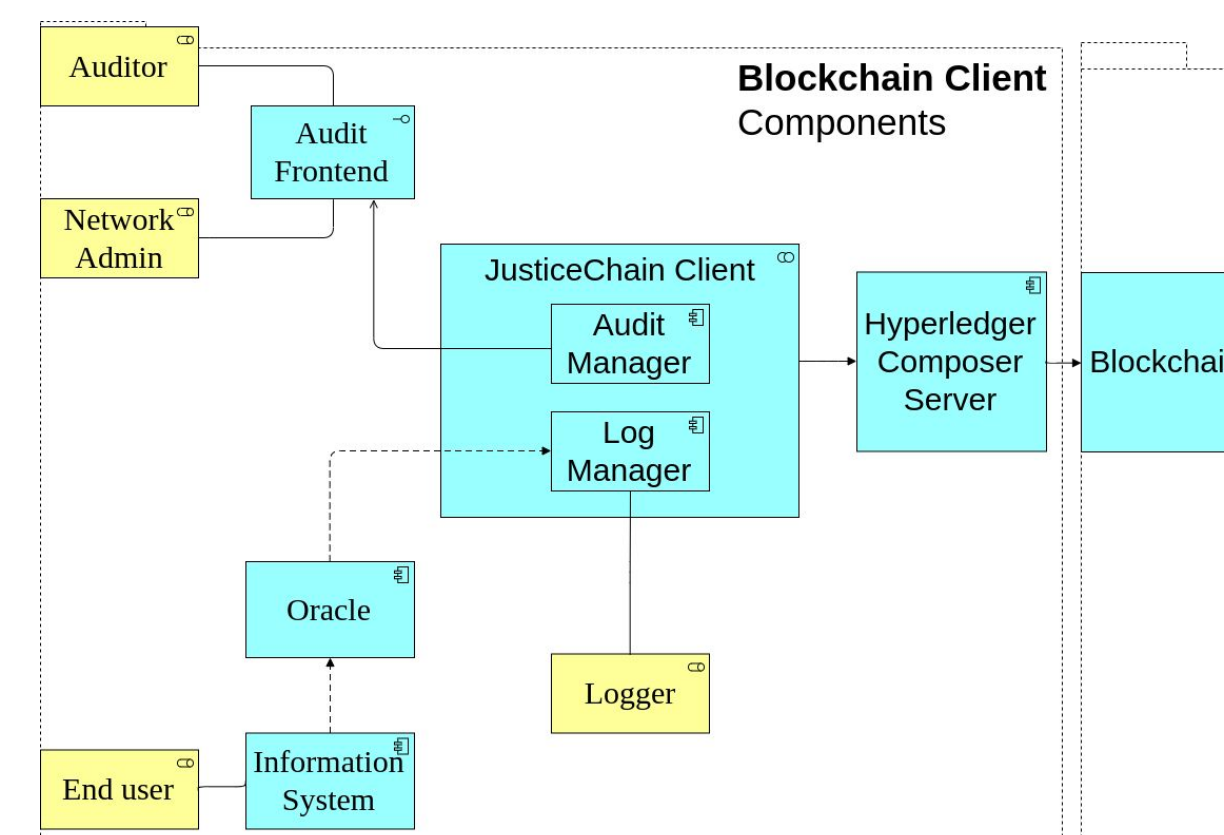
## Related Work

- Blockchain
- Hyperledger Fabric
- Audit Logs
- Access Control



## Solution, Evaluation

- JusticeChain
- JusticeChain v2

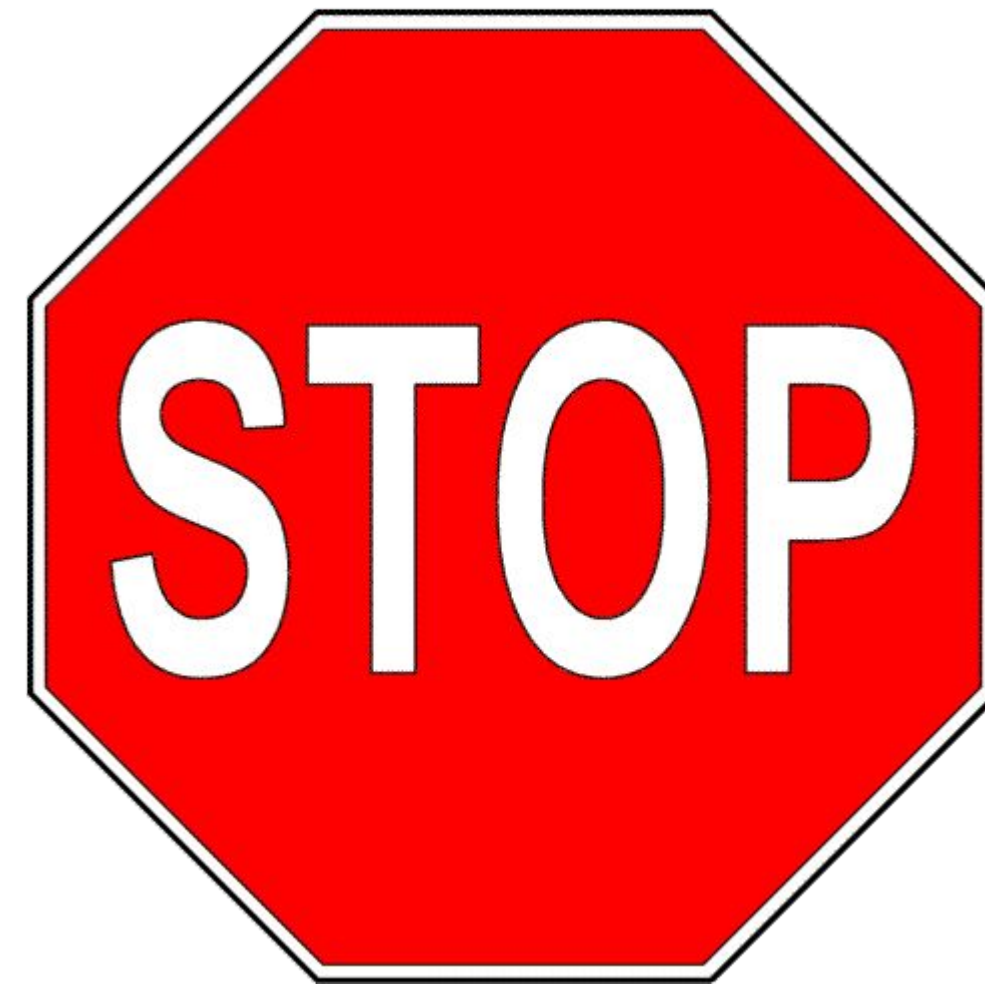


## Conclusion

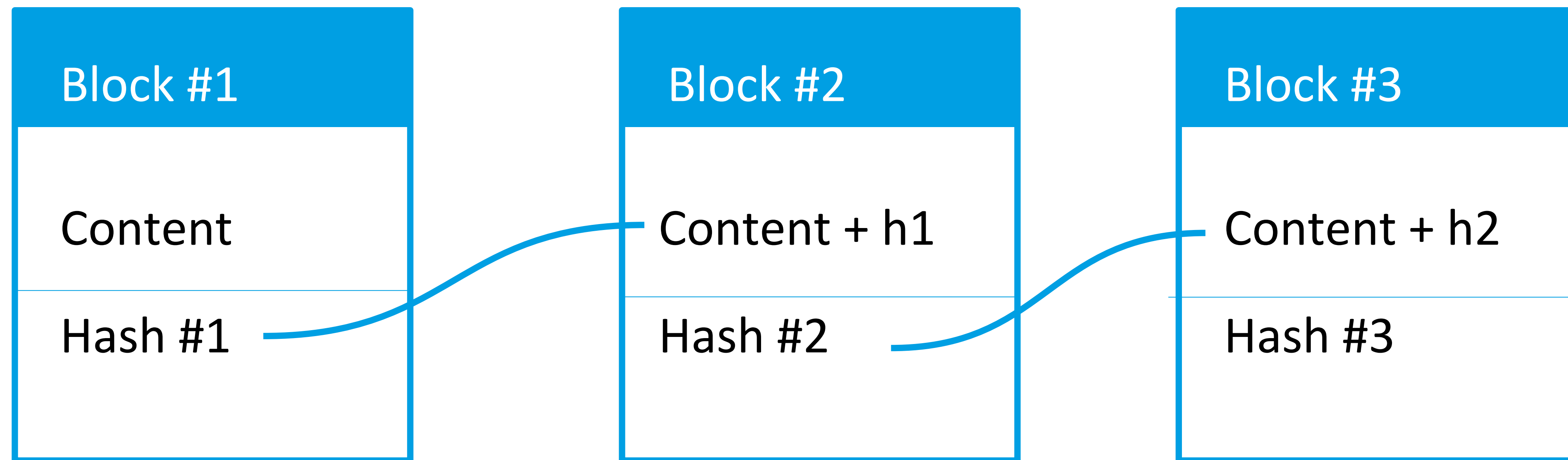
- Conclusions
- Contributions
- Future Work







- ❑ Legislative power vs judicial power
- ❑ Conflict of interests, leading to lack of trust
- ❑ Blockchain distributes trust, giving guarantees to the government and judges



- Global ledger maintained by consensus



- ❑ Not based on the computational power of the network. Based on the amount of coins held, i.e., the stake on the network
- ❑ Introduction of smart contracts



Brings other problems:

- ❑ Nothing at stake: based on double-spending problems on forks
- ❑ In order-execute paradigm all nodes execute transactions sequentially (expensive)





2009, Blockchain v1.0



ethereum

2014, Blockchain v2.0

- ❑ Computationally expensive
- ❑ Performance (6-7 tps)
- ❑ Sequential execution - performance
- ❑ Confidentiality/privacy issues
- ❑ Static consensus algorithm



HYPERLEDGER  
FABRIC



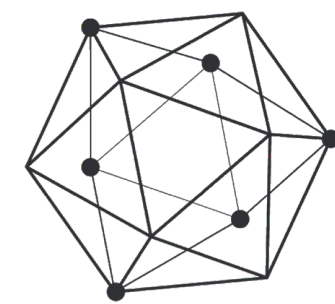
MultiChain



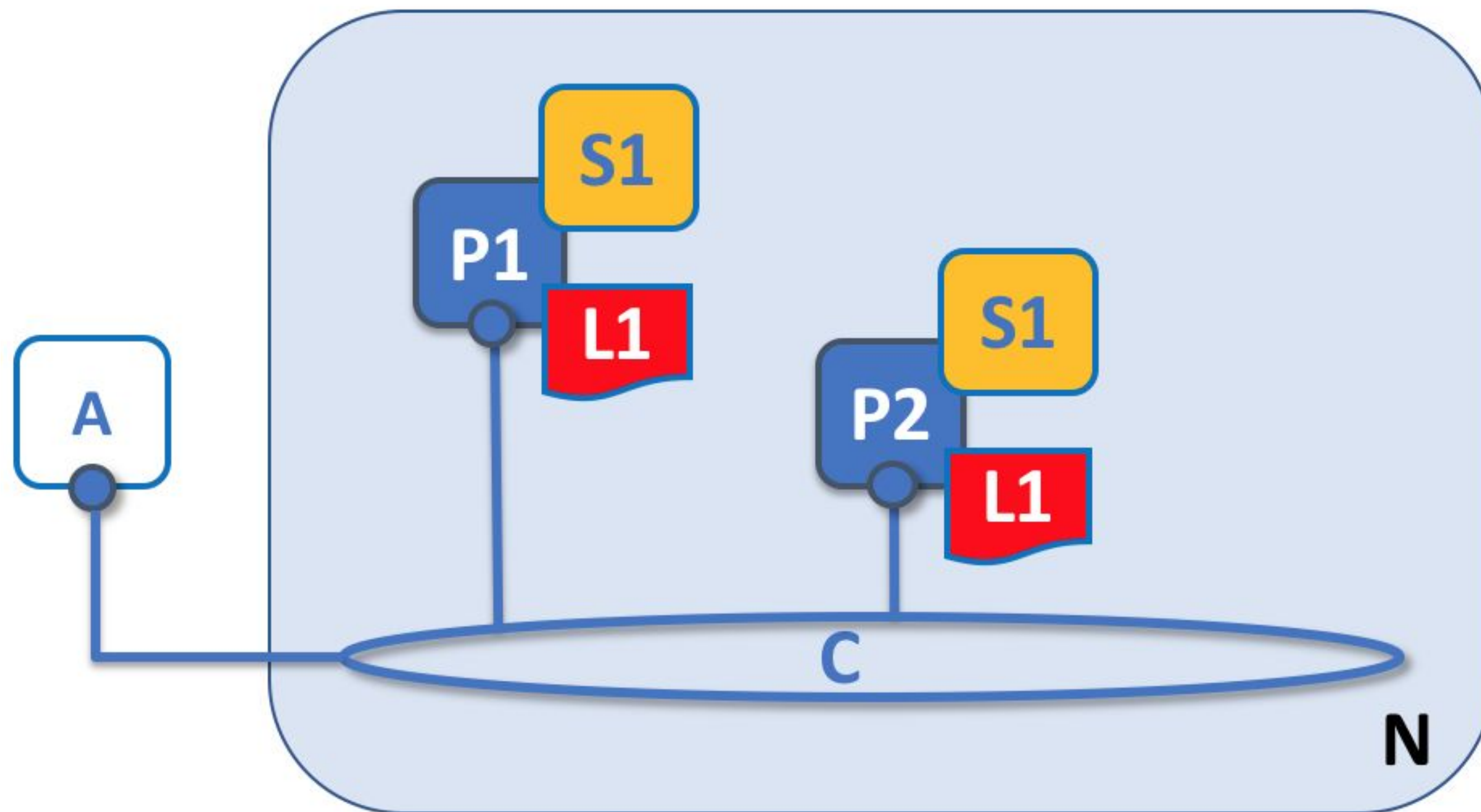
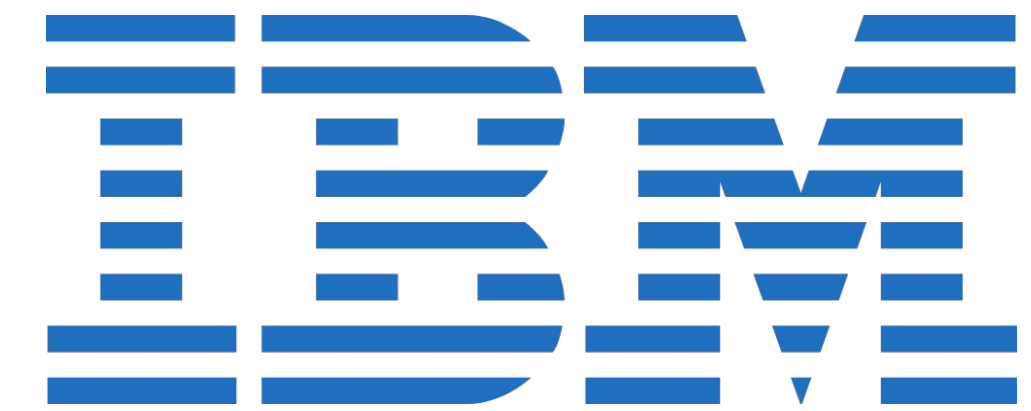
Quorum



Tendermint

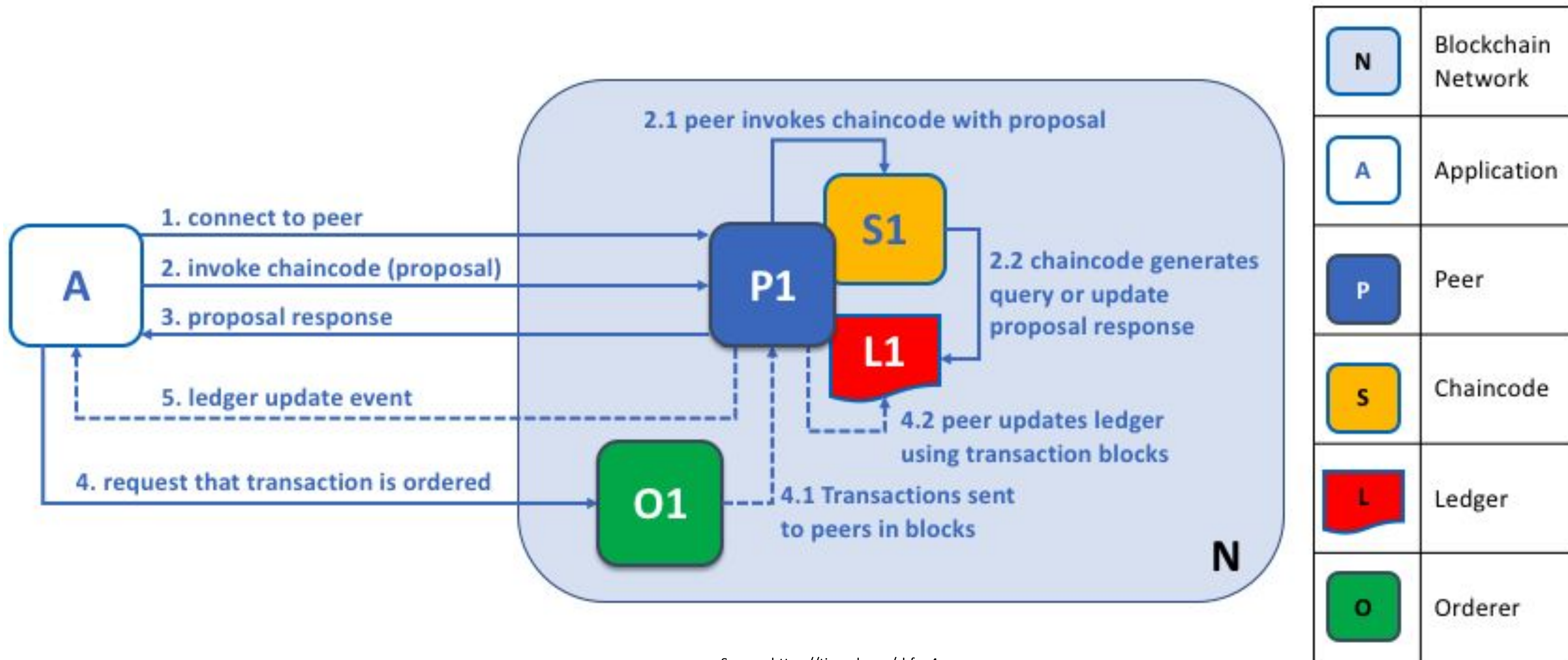


# HYPERLEDGER



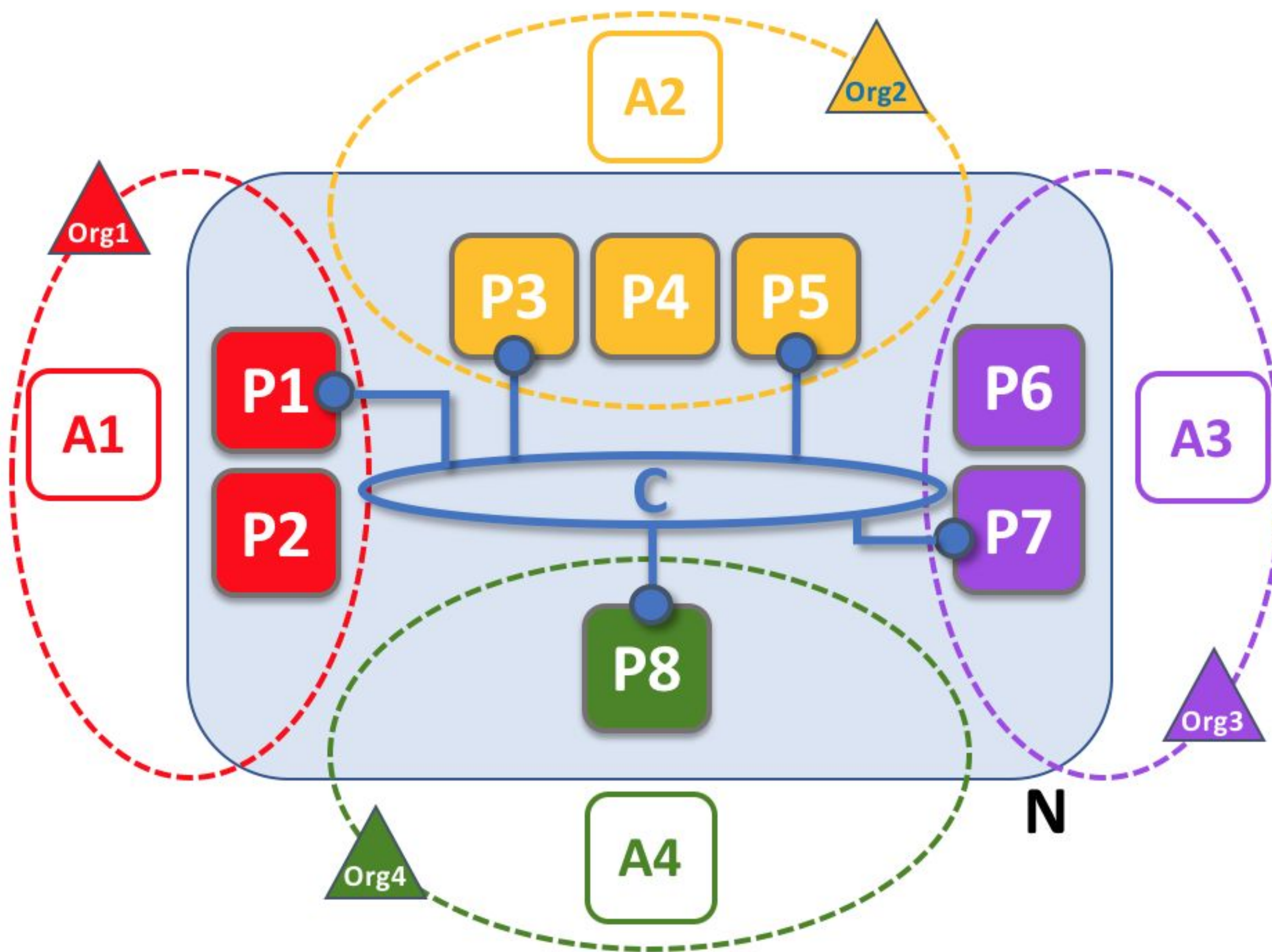
	Blockchain Network		Ledger
	Channel		Application
	Peer		Principal PA (e.g. A, P1) communicates via channel C.
	Chaincode		









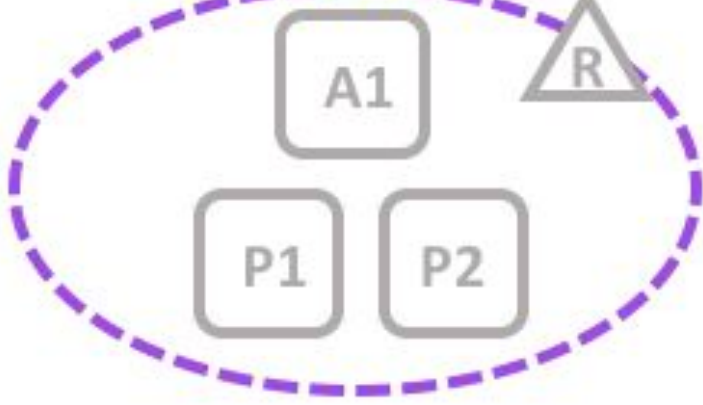




Source: <https://tinyurl.com/rhfep4g>





	Blockchain Network		Ledger
	Channel		Application
	Peer	 	Principal PA (e.g. A1, P5) communicates via channel C.
			Organization
		Organization R owns application A1 and peers P1, P2.	

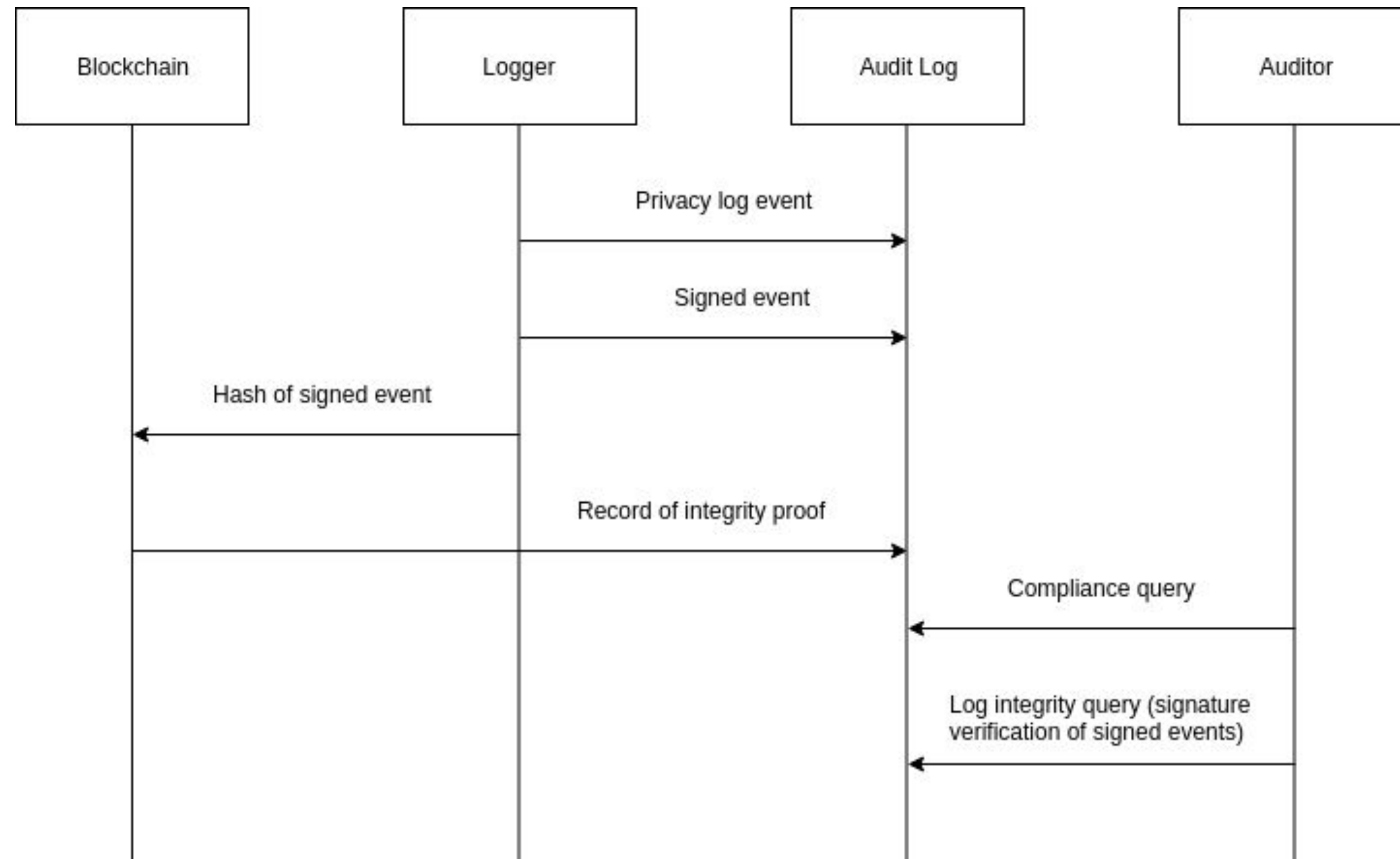


Author	IC	IA	SPF	D	DP	FGP
Cohen, 1987 [17]	✓	x	✓	x	-	-
Bellare et al., 1997 [6]	✓	x	✓	x	-	-
Schneier et al., 1998 [64]	✓	✓	✓	x	-	-
Snodgrass et al., 2004 [66]	✓	✓	✓	x	-	-
Ma and Tsudik, 2009 [44]	✓	✓	✓	x	-	-
Ray et al., 2013 [60]	✓	✓	x	x	-	-
Bharathi and Rajashree, 2014 [7]	✓	✓	x	✓	-	-
Cucurull and Puiggal, 2016 [20]	✓	✓	x	✓	x	x
Sutton and Samavi, 2017 [67]	✓	✓	x	✓	x	x
Pourmajidi and Miranskyy, 2018 [58]	✓	✓	x	✓	x	x
Anderson and Smith, 2018 [2]	✓	✓	x	✓	✓	x
Ahmad & Saad & Mohaisen, 2019 [1]	✓	✓	x	✓	✓	x

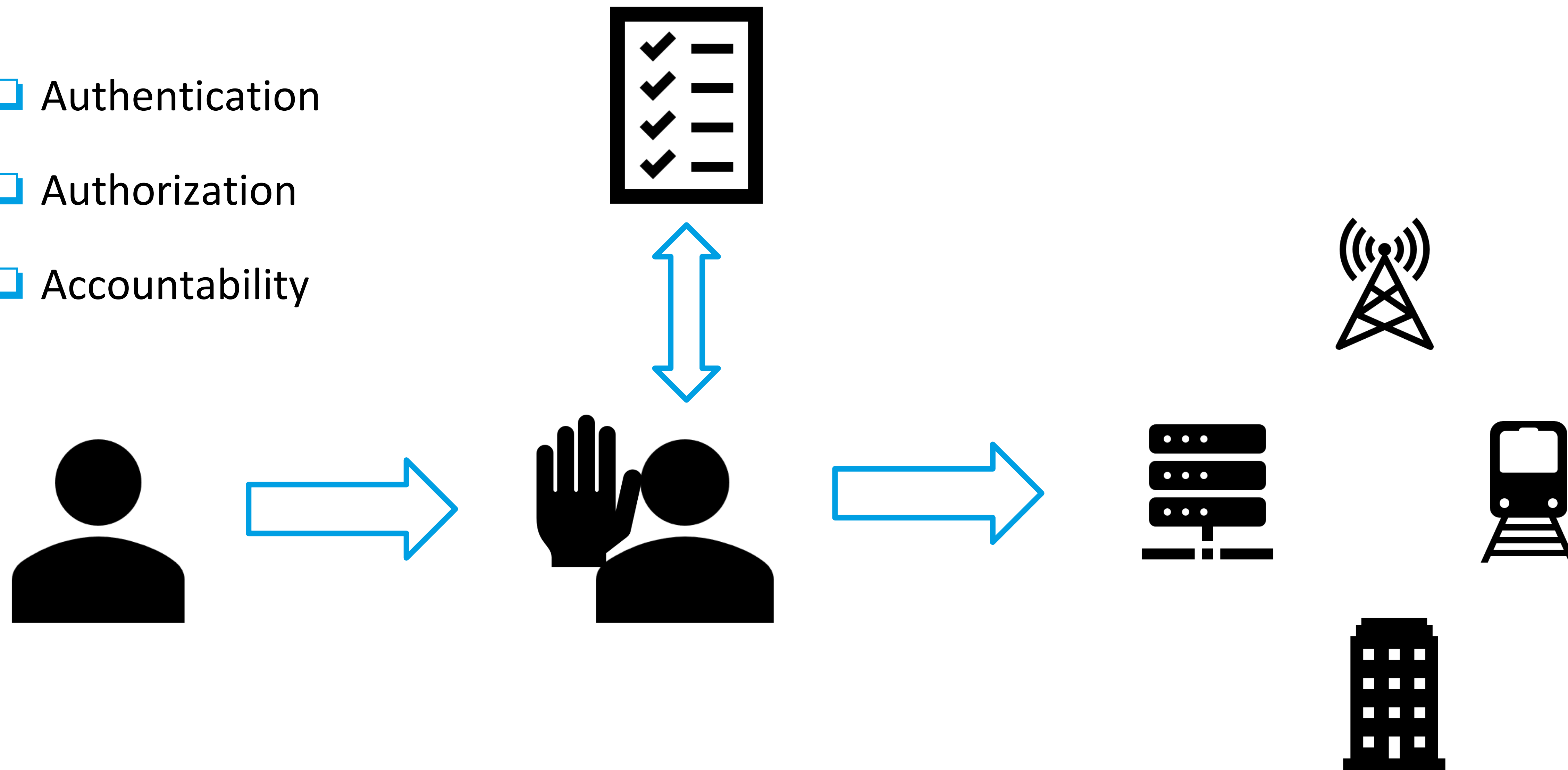
Table 2.2: Features from contributions to audit logs.

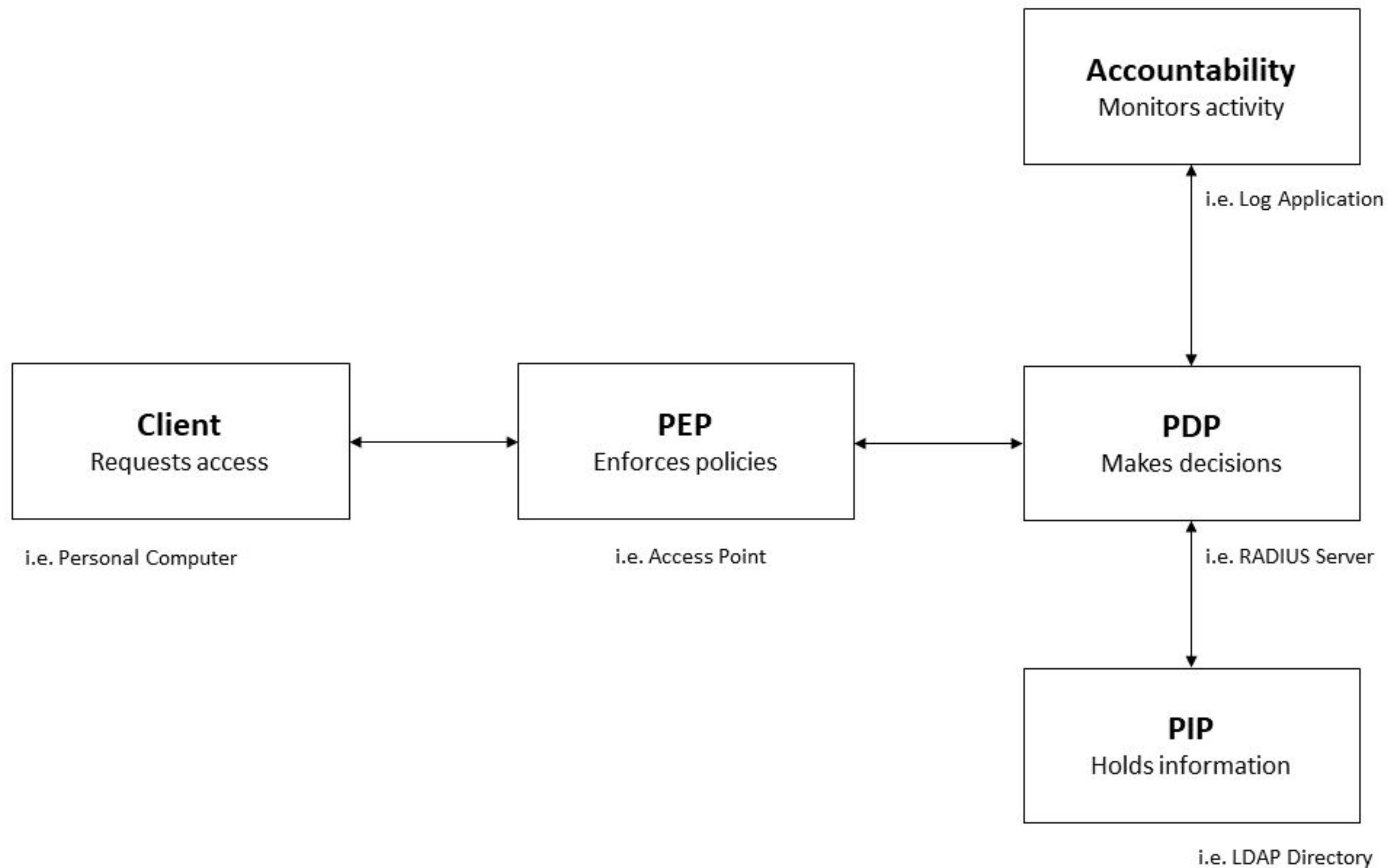


■ Sutton and Samavi, [2017]



- ❑ Authentication
- ❑ Authorization
- ❑ Accountability



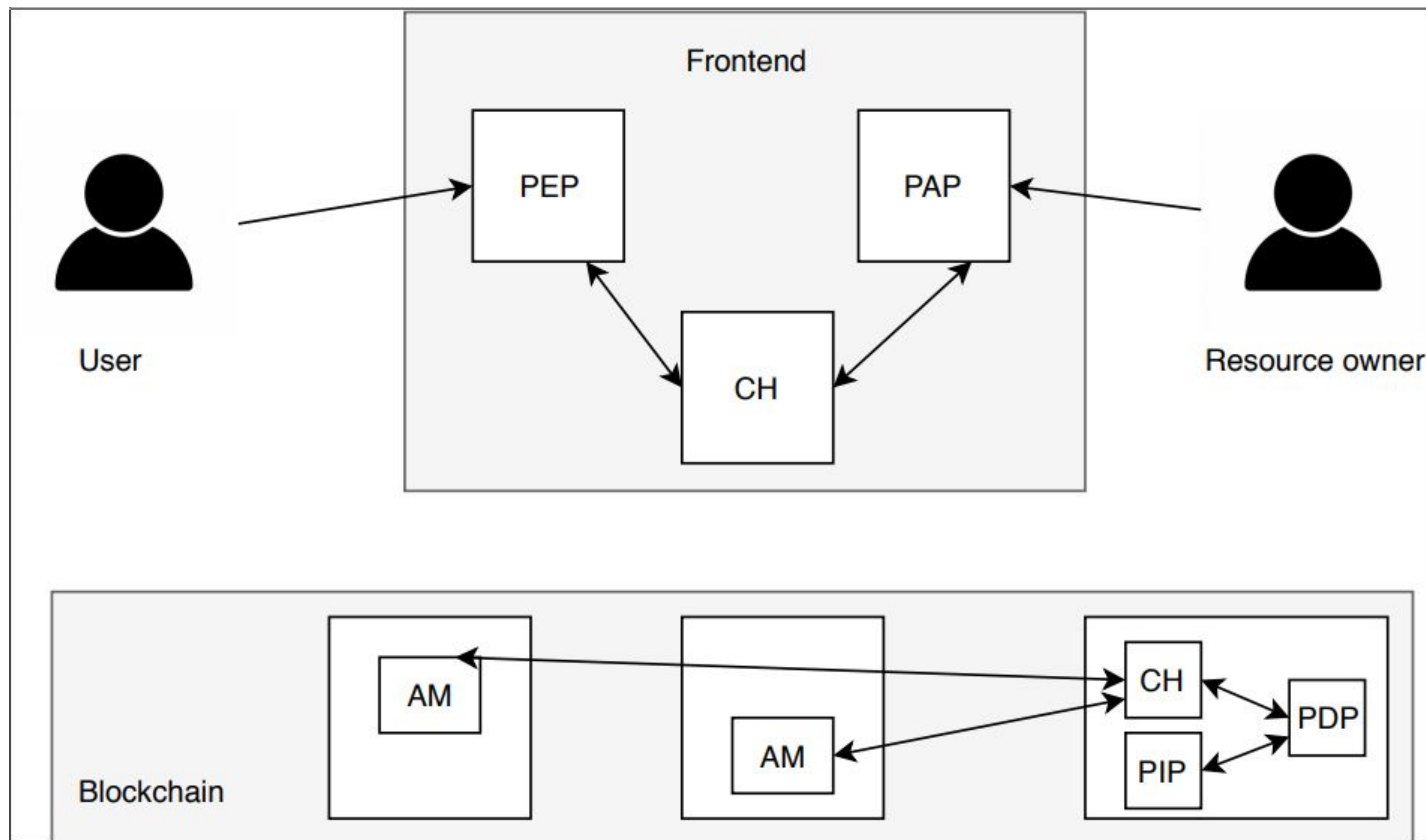




Author	D	FGP	S	PB	MS
Zyskind et al., 2015 [86]	✓	✓	x	x	x
Laurent et al., 2018 [50]	✓	✓	x	x	x
Zhang et al., 2019 [83]	✓	✓	x	x	x
Uchibeke et al., 2018 [73]	✓	✓	x	✓	x
Maesa et al., 2019 [48]	✓	✓	✓	x	x

Table 2.3: Features from contributions to blockchain access control.

Maesa et al.  
[2019]



☐ JusticeChain

☐ Evaluation

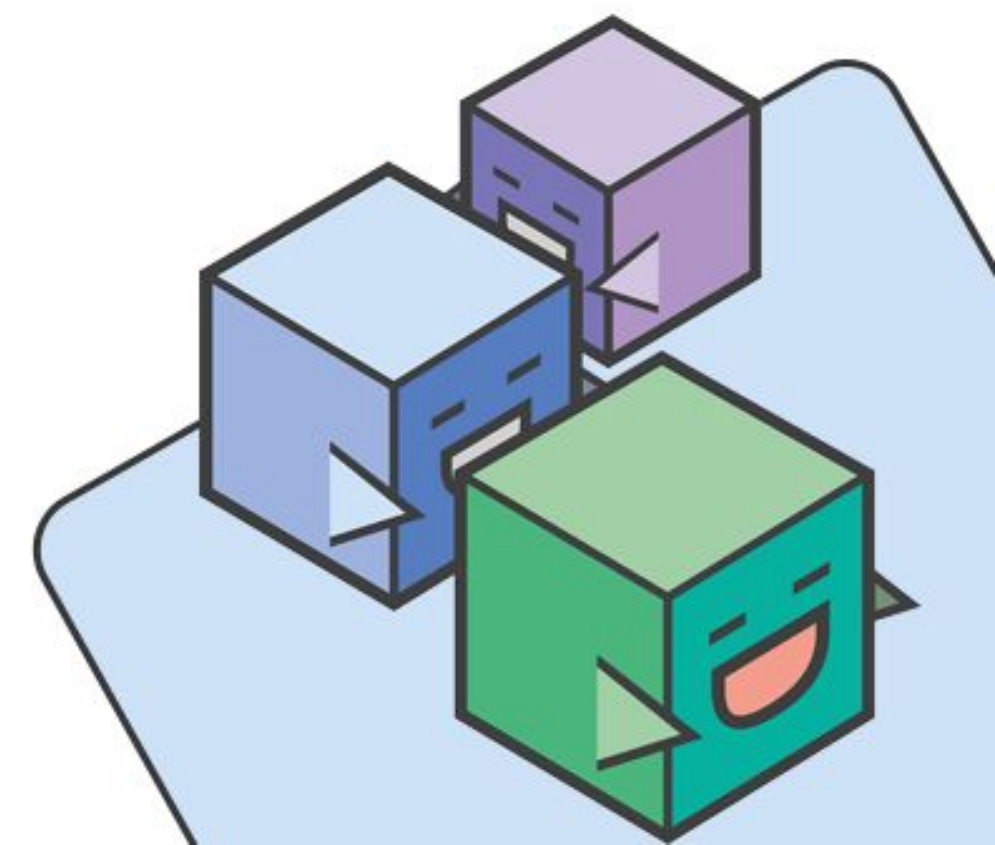
☐ JusticeChain v2

☐ Evaluation

☐ JusticeChain vs JusticeChain v2



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



Assets:

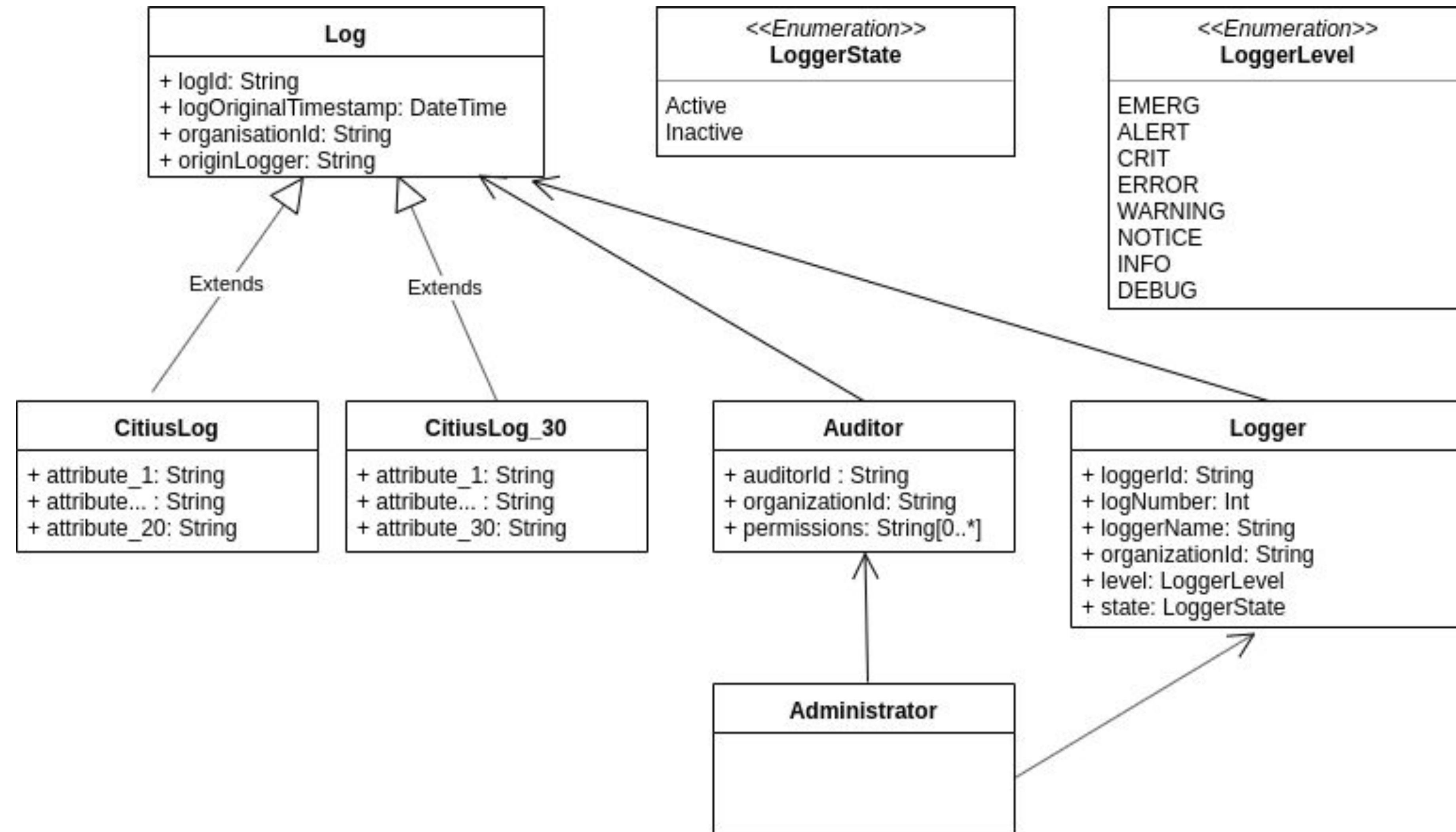
■ Audit Logs

3 participants:

■ Logger

■ Auditor

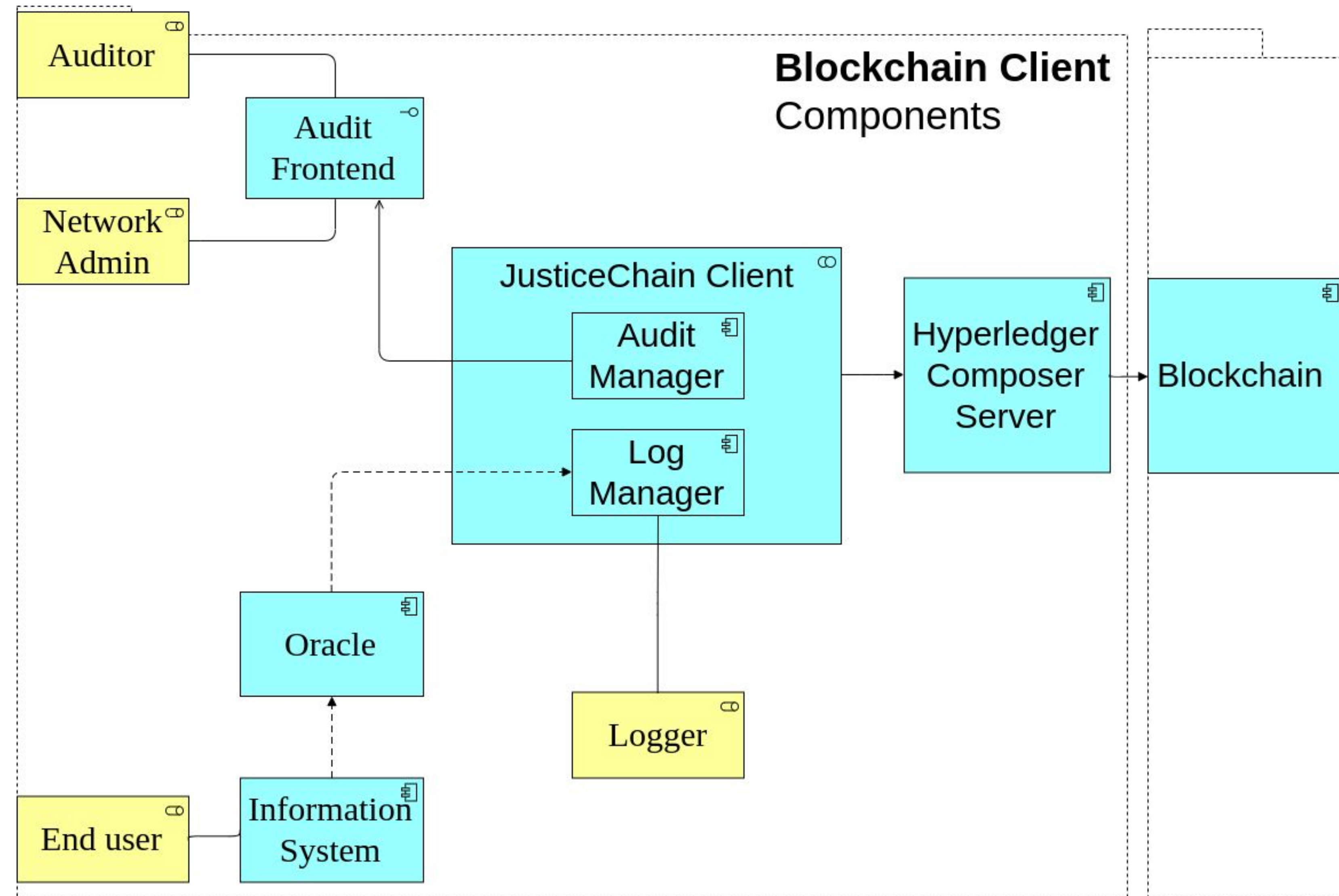
■ Network Admin



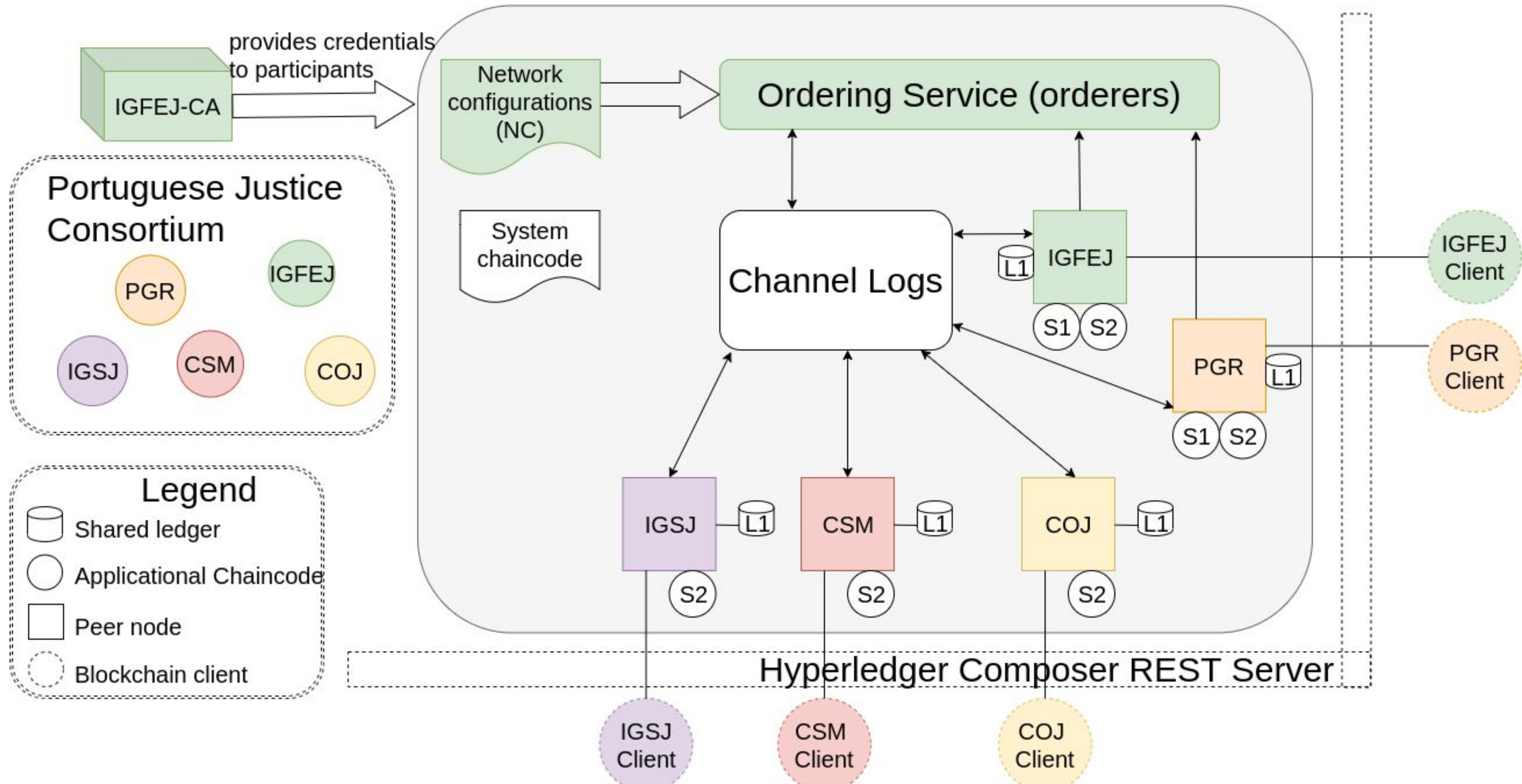


## JusticeChain Client:

- ❑ Retrieves logs
- ❑ Preprocesses logs
- ❑ Issues transactions to the blockchain
  
- ❑ For more decentralization, there can be multiple JusticeChain clients

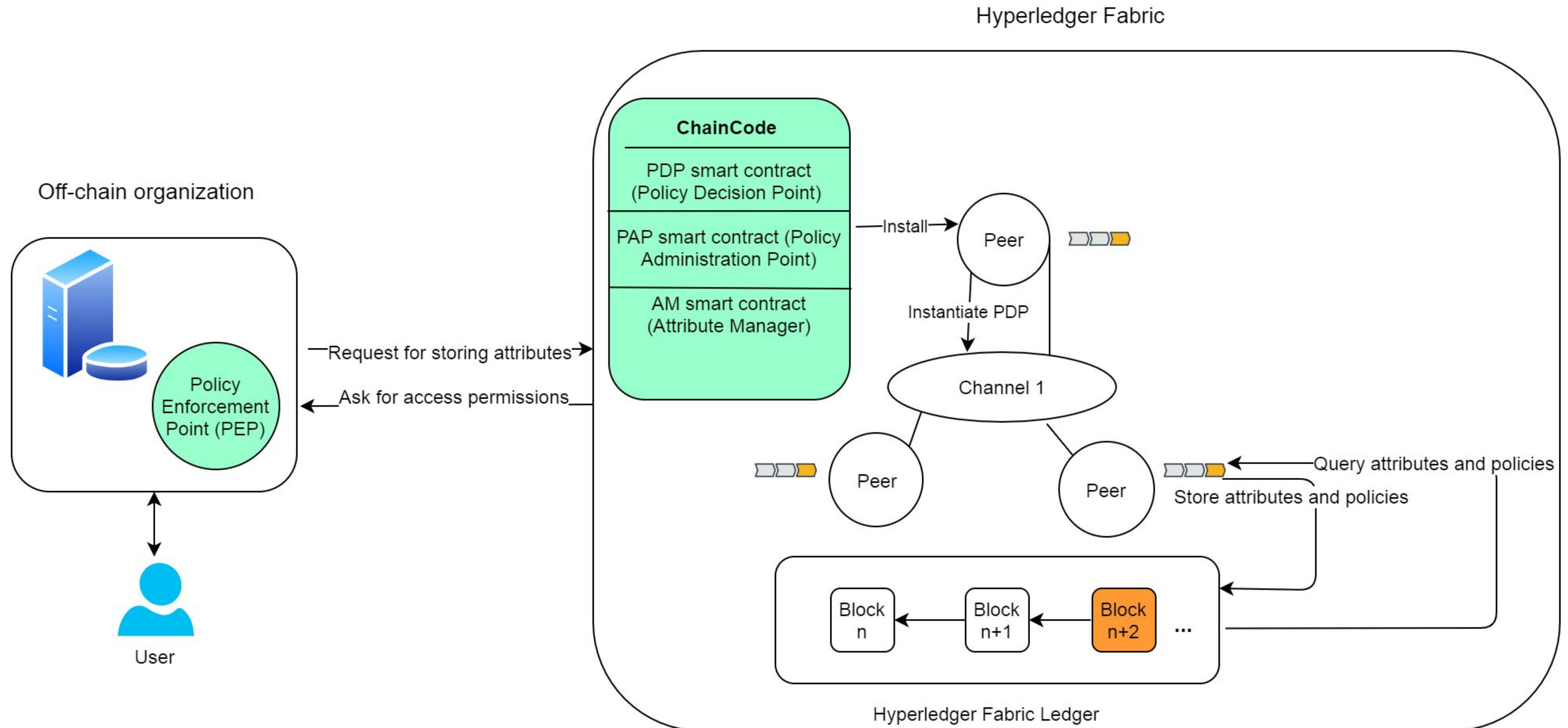


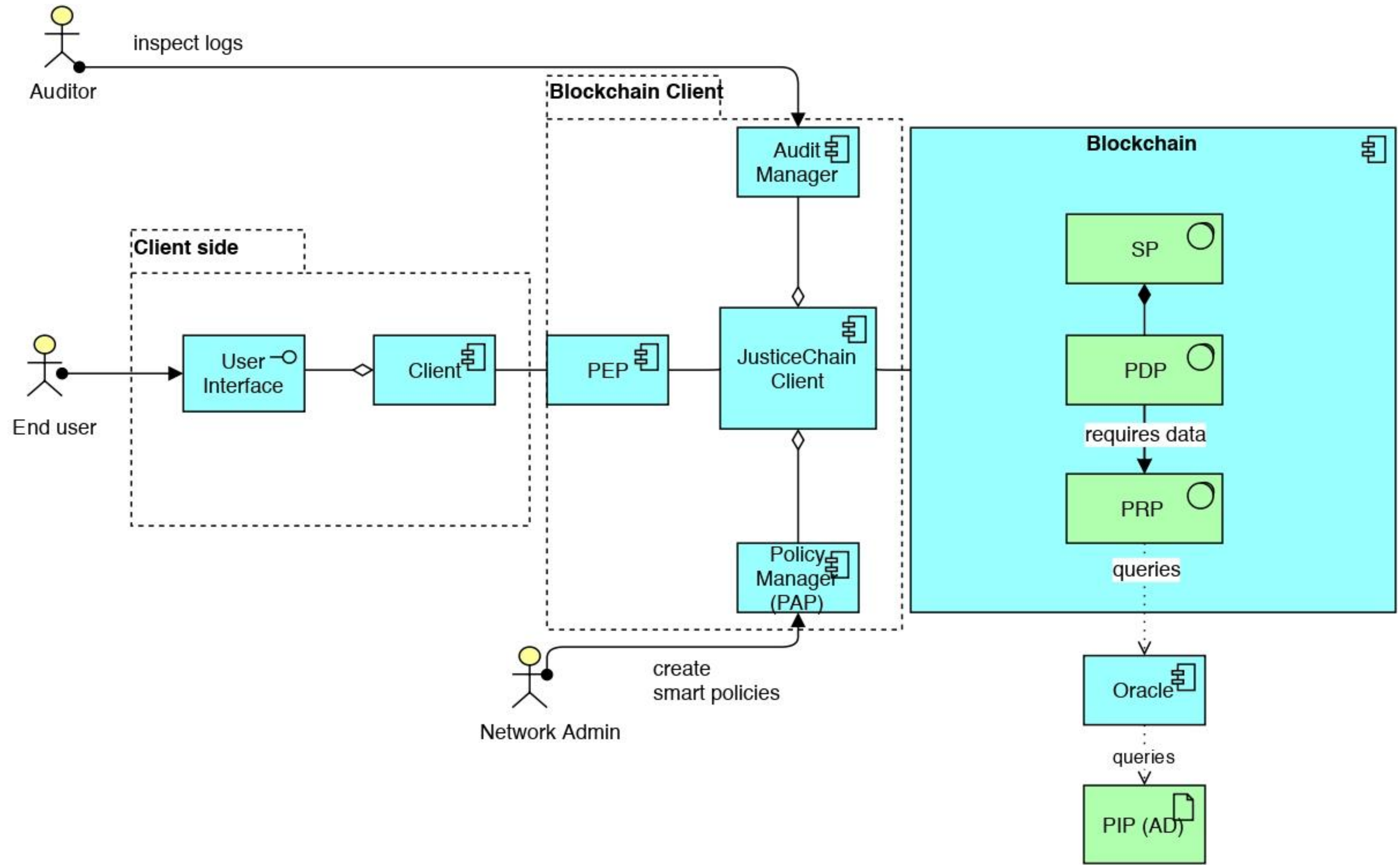






- ❑ Performance: Hyperledger Composer and Hyperledger Caliper
- ❑ JusticeChain does not necessarily capture the whole access control flow:
  - ❑ Some information may not be recorded (accesses)





- ❑ Privacy: access control policies can be seen by all participants
- ❑ Evaluation comprised simple access control policies and rules



- ❑ Evaluation Methodology
- ❑ Setup
- ❑ Throughput and latency
- ❑ Storage



**HYPERLEDGER**  
CALIPER

- ❑ What is the throughput rate JusticeChain can achieve?
- ❑ What is the latency of JusticeChain, i.e., what is the time window needed for logs to be secured?
- ❑ What is the cost, in terms of storage, of protecting logs, i.e., what is the scalability of JusticeChain?

- ❏ 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
```



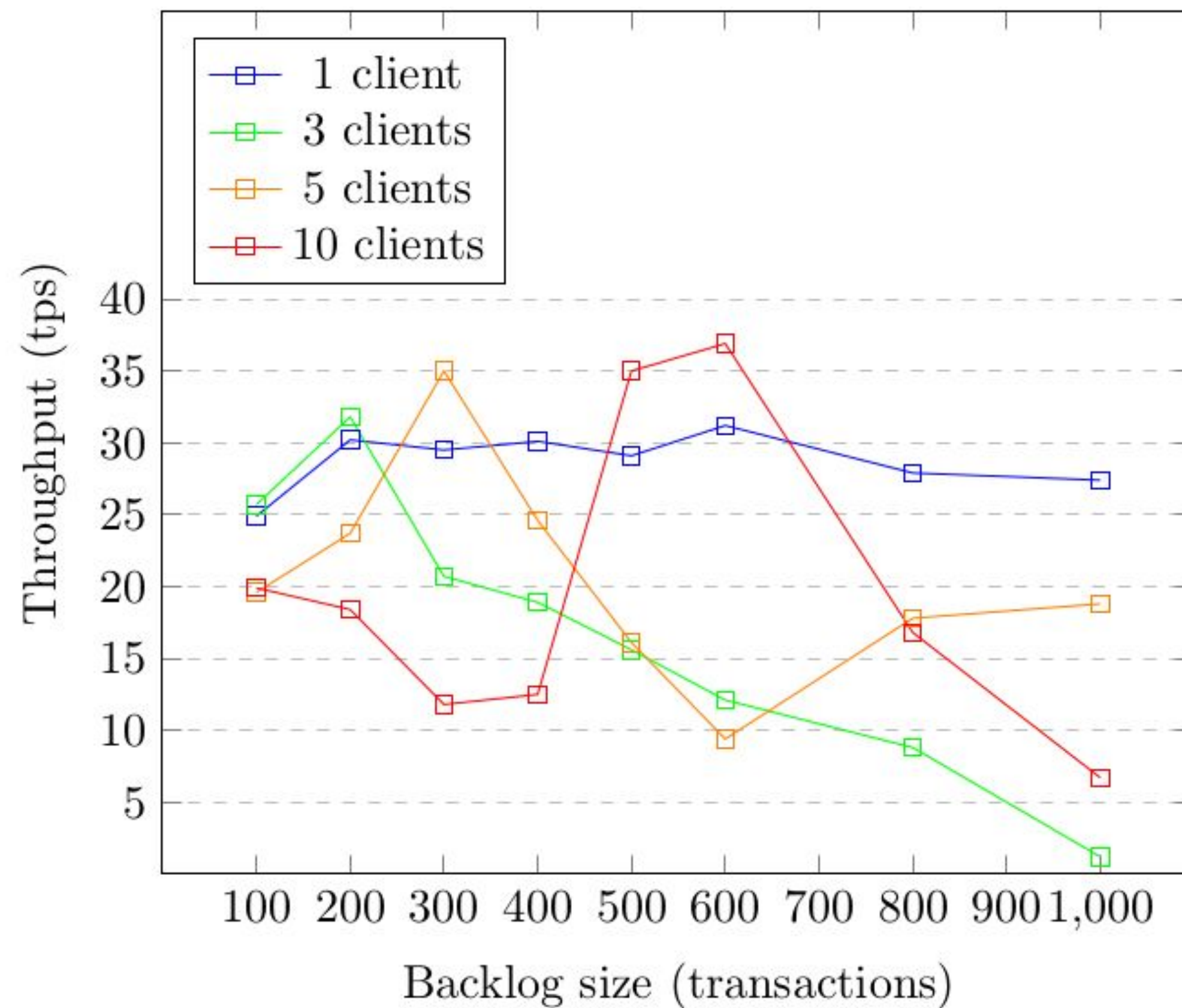


Figure 4.4: Variation of the throughput with the size of the backlog

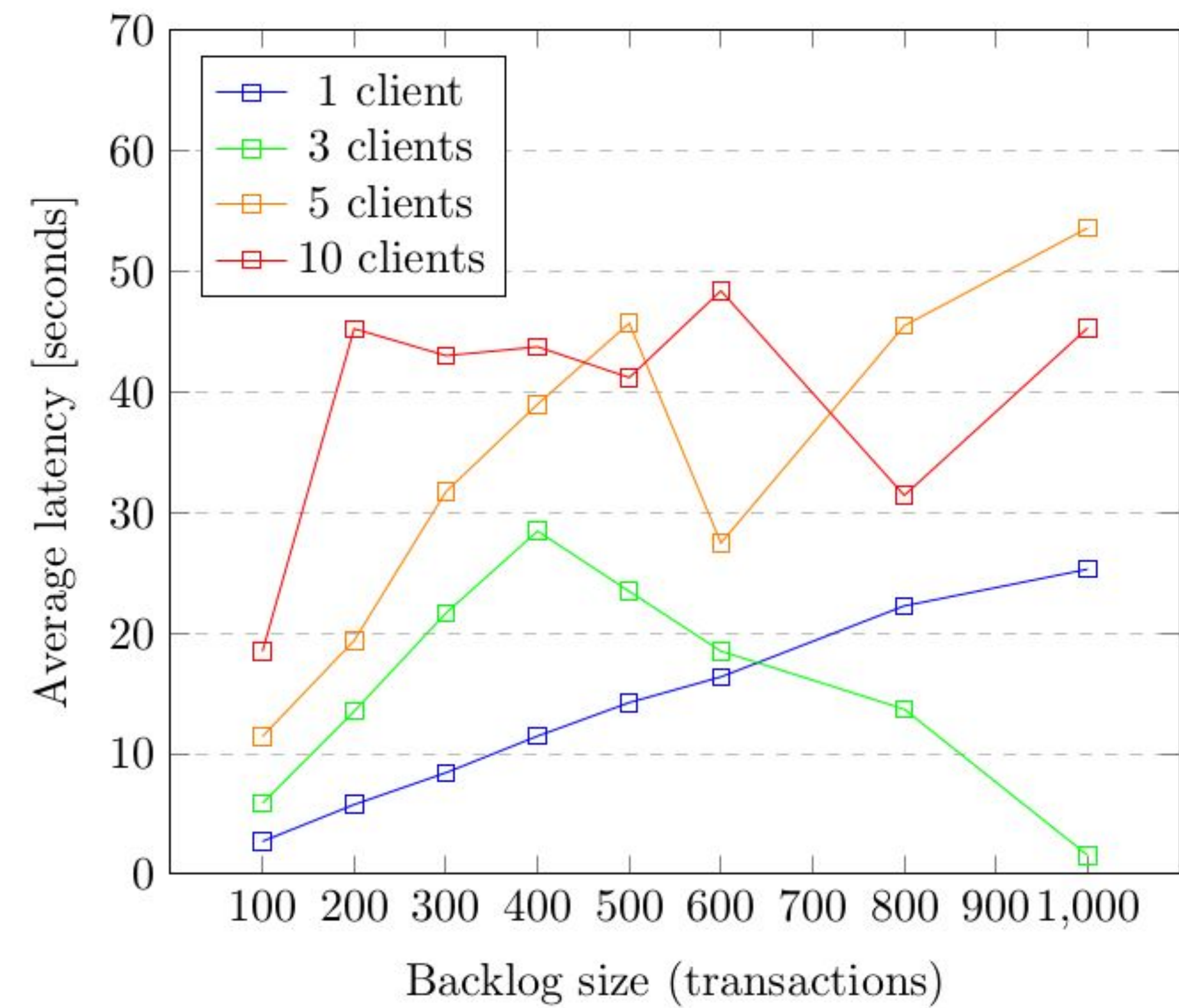
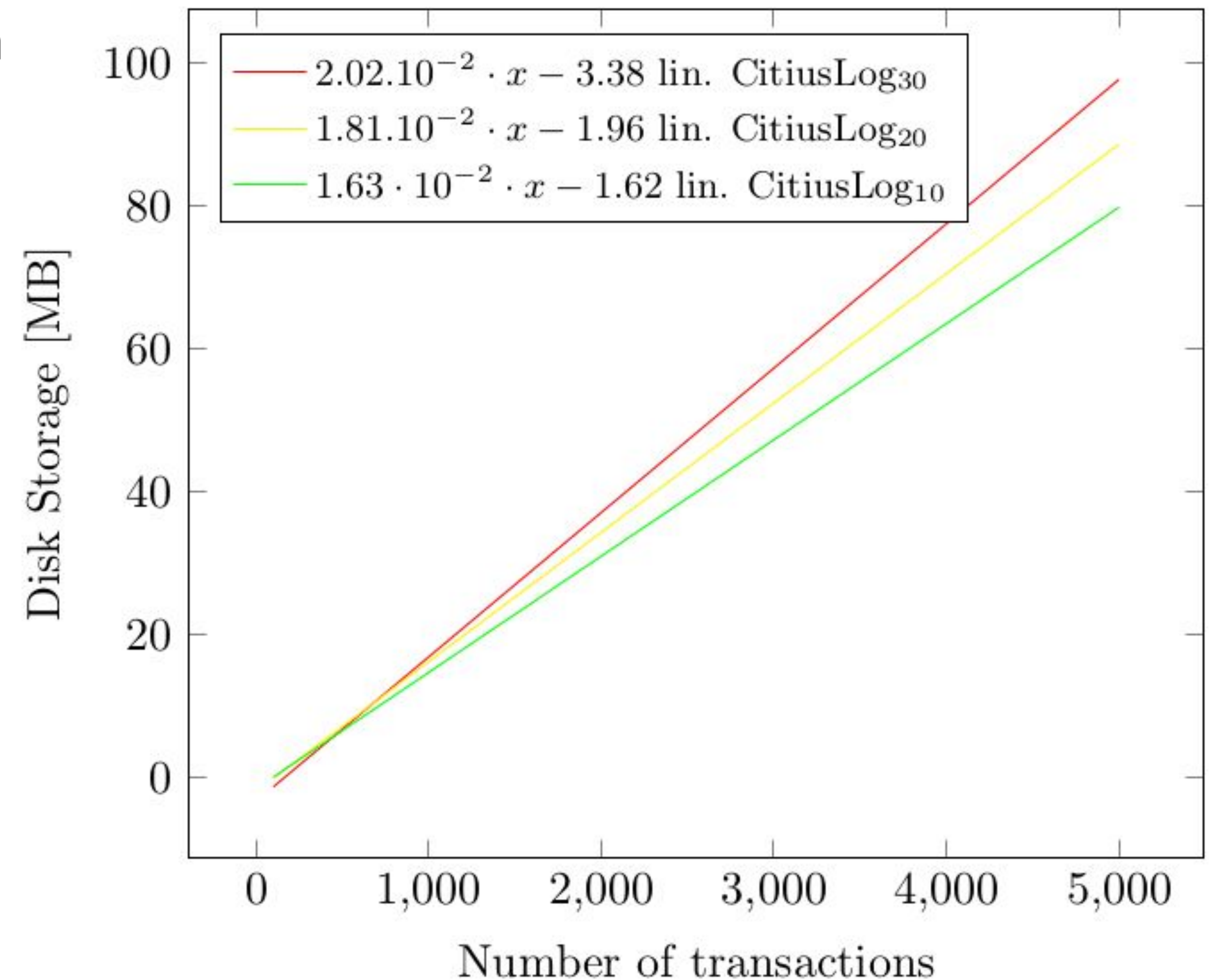
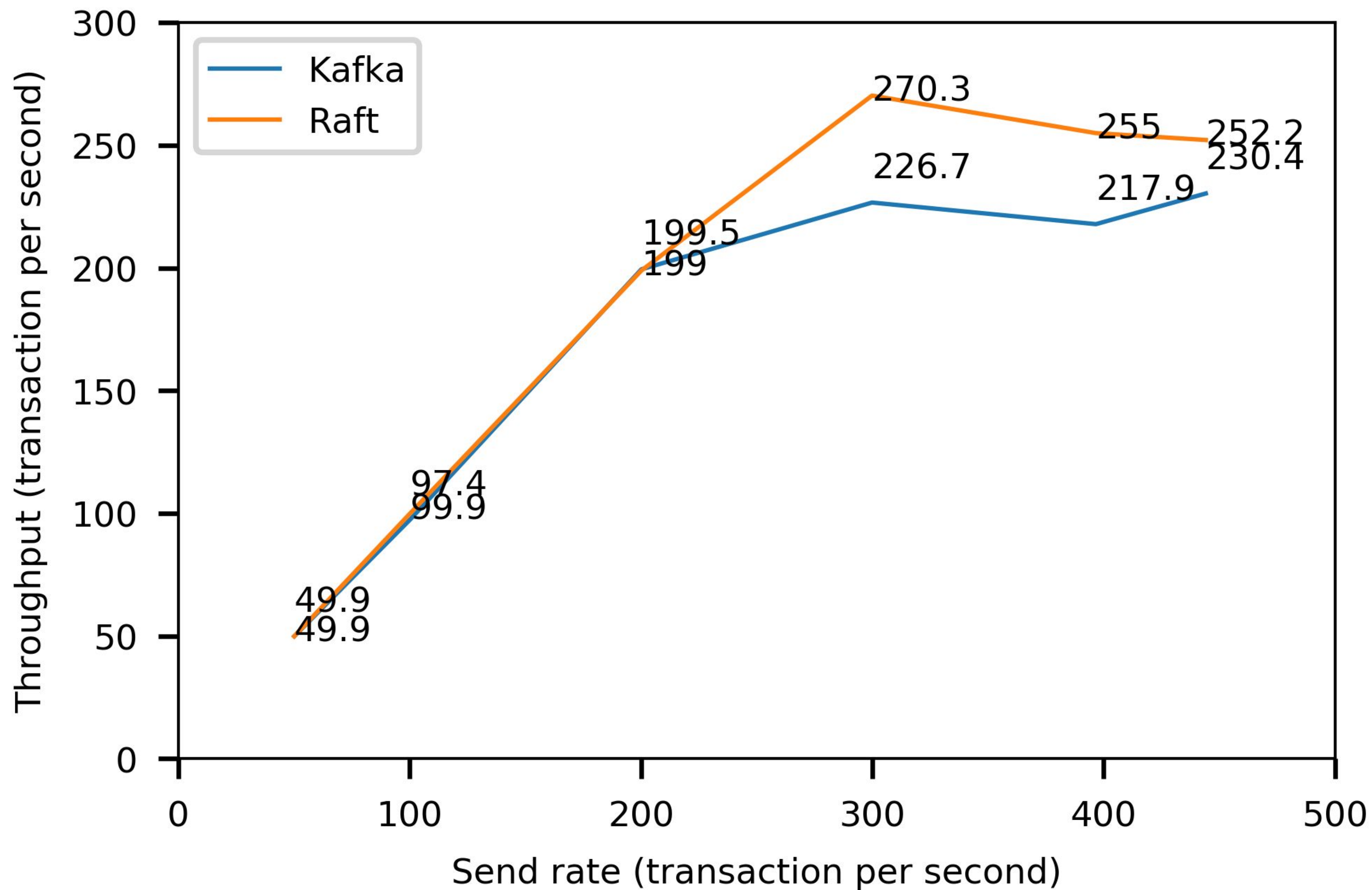


Figure 4.5: Variation of the latency with the size of the backlog

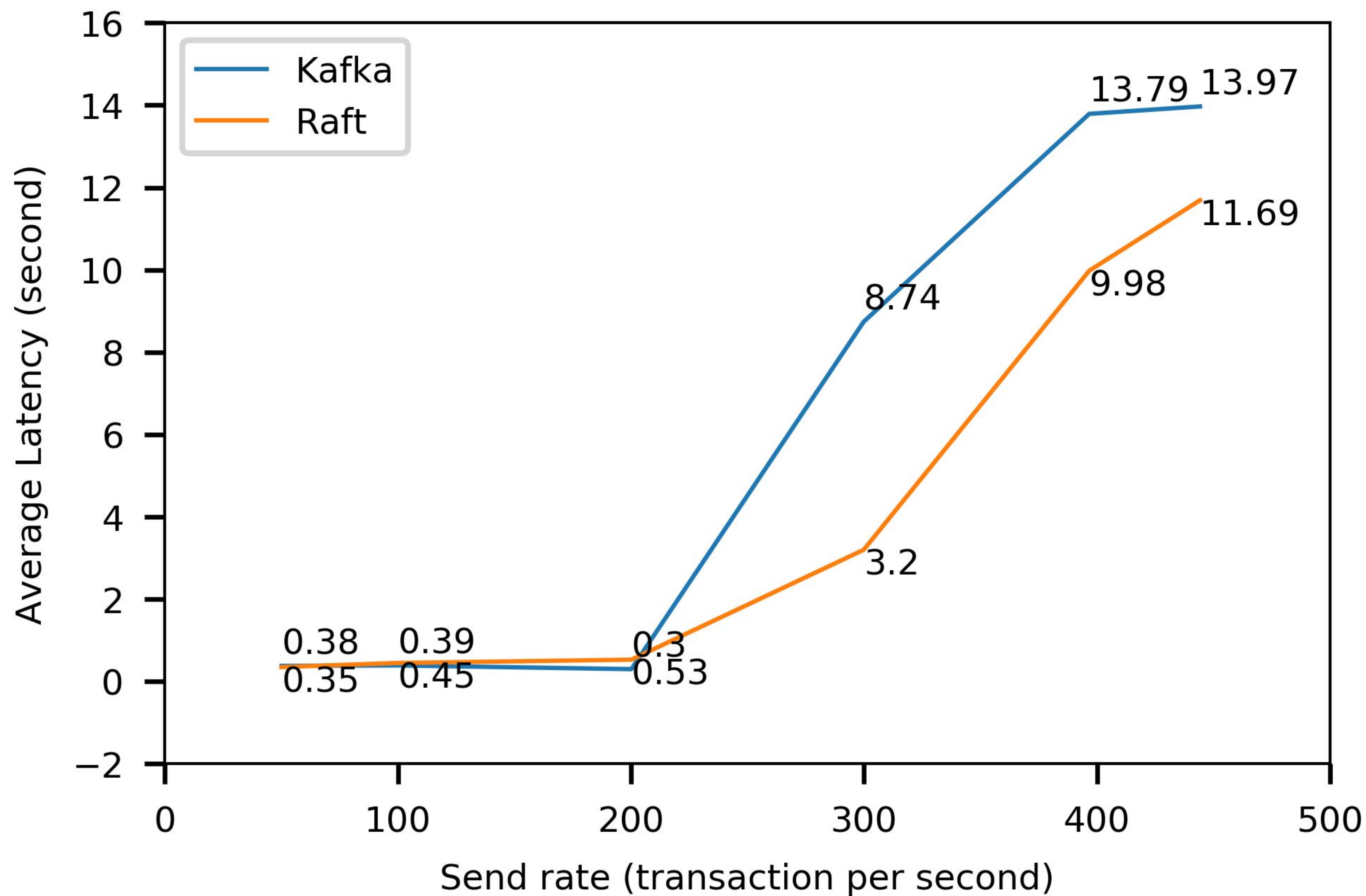
- What is the storage required for each committing peer, for a year?
- For a log entry with 10 attributes:  
5.67 TB
- Required storage evolves linearly

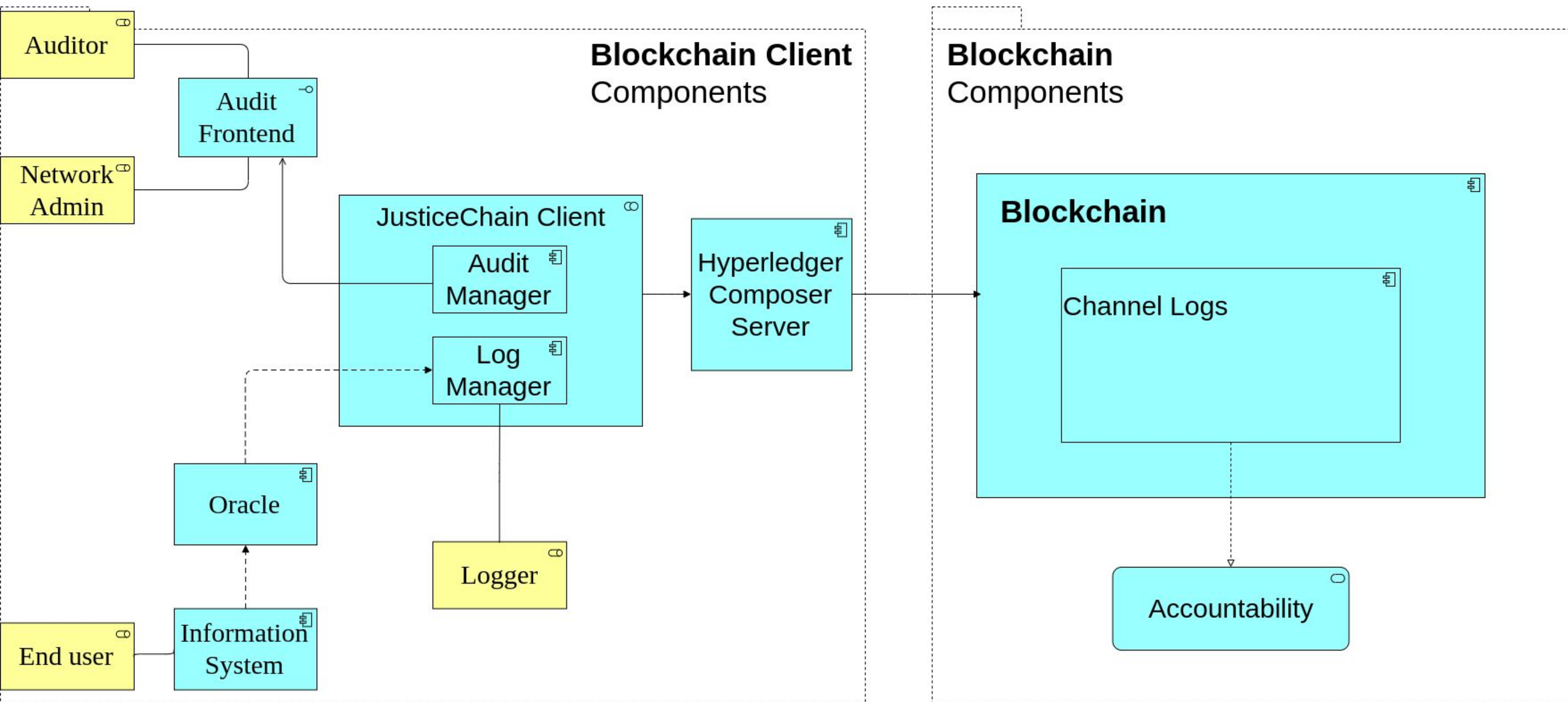




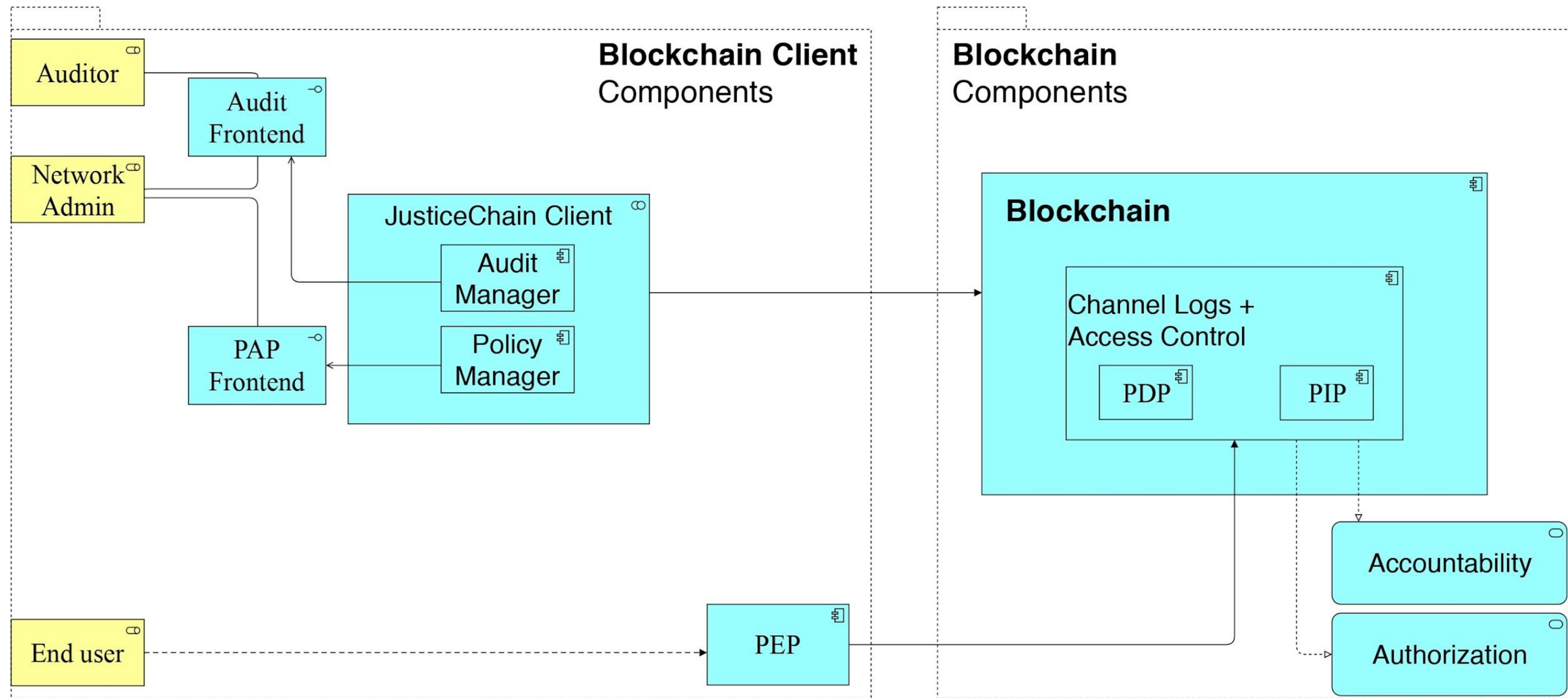














- ❑ We tackle the three main challenges at IGFEJ:
  - ❑ Increase integrity
  - ❑ Distribute trust
  - ❑ Control access to logs
- ❑ Limitations: expensive solution (throughput, storage)
- ✅ JusticeChain can address those challenges
- ✅ JusticeChain proof of concept, to be implemented at the Portuguese justice

- ❏ How to provide a secure, decentralized access control system that:
  - ❏ Captures all access control requests
  - ❏ Increases trust distribution
- ❏ Regarding trust: stakeholders can now know if resources are being denied to them unduly
- ❏ Extensible to other domains
- ❏ Limitations: expensive solution (throughput, storage).
- ❏ JusticeChain v2 encompasses JusticeChain's features and distributes trust regarding authorization.

- ❑ R. Belchior, M. Correia & A. Vasconcelos (2019). JusticeChain: Using Blockchain to Protect Justice Logs, OTM Confederated International Conferences" On the Move to Meaningful Internet Systems, Greece, Oct 21-25. Berlin, Germany: Springer Verlag **(Rank A)**
  
- ❑ R. Belchior, M. Correia & A. Vasconcelos (2019). Towards Secure, Distributed, and Automatic Audits with Blockchain, submitted at The European Conference on Information Systems **(Rank A)**



- ❑ Blockchain-based access control system proof of concept, available as an open-source project at **Hyperledger Labs**, validated by the Hyperledger Foundation.
- ❑ S. Rouhani, R. Belchior, R. Cruz & R. Deters (2019). Hyperledger Fabric Attribute-Based Access Control System: A Step Towards Distributed Access Control Using Blockchain, submitted to IEEE Access (**Q1**)



- ❑ On JusticeChain v2 legit authentication is assumed. Extend to authentication
- ❑ Explore different options to overcome the performance limitations (e.g., using another blockchain).
- ❑ Explore the usage of several blockchains to increase the dependability of an blockchain-based access control

Hyperledger Composer

+

← → ↺ 🏠

localhost:8080/test

⋮ 🛡️ ☆

📄 📖 👤 ☰

PARTICIPANTS

Auditor

Logger

ASSETS

CitiusLog

CitiusLog\_10

CitiusLog\_30

TRANSACTIONS

All Transactions

Submit Transaction

8

"auditUtilName": "Commodo trure.",

9

"auditUtilName": "Commodo.",

10

"auditHostName": "Id cupidatat velit velit.",

11

"auditHostIP": "Tempor ut ipsum eu aliquip.",

12

"processo": "Eiusmod nostrud nisi ipsum.",

13

"tribunal": "Ullamco aute cupidatat.",

14

"unidadeOrganica": "Laborum.",

15

"clientAuditID": "Tempor occaecat ut deserunt amet.",

16

"idTribRef": "Ullamco incididunt ipsum minim.",

17

"idUnOrgRef": "Eiusmod Lorem.",

18

"auditUtilID": "Non.",

19

"CuditMccCdress": "Nisi.",

20

"logId": "3939",

21

"logOriginalTimestamp": "2019-11-21T00:10:08.280Z",

22

"organizationId": "1"

23

}

☐ Optional Properties

Cancel

⌂

+ Create New Asset

✎ 🗑️

Legal

GitHub

Playground v0.20.9

Tutorial

Docs

Community

🔗

Parece que não inicia o Firefox há algum tempo. Pretende limpá-lo para uma nova experiência? E, já agora, seja bem-vindo(a) de volta!

Restaurar o Firefox...

✕



localhost:3000/
+
localhost:3000

## Record Subjects attributes

Subject key
juiz\_a

Subject attributes
{ "user": { "active": "true", "dob": "1989-06-06", "infracoes": 0, "group": 12, "department": "computer" } }

Submit

## Record Resources attributes

Resource key
processo\_benfica

Resource attributes
{ "group":{ "id":12 }, "id":"4203" }

Submit

## IGFEJ

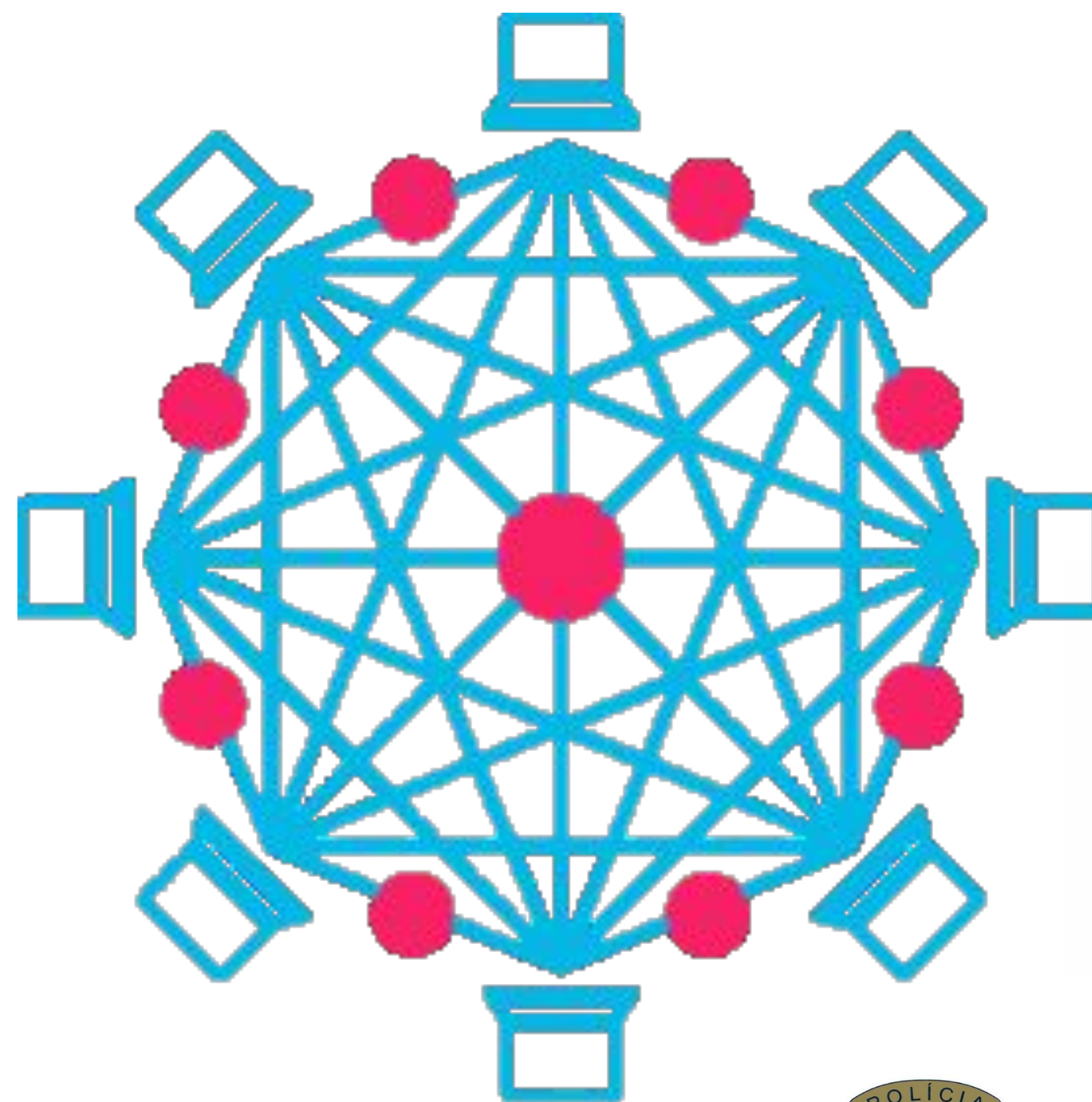
INSTITUTO DE GESTÃO  
FINANCEIRA E EQUIPAMENTOS  
DA JUSTIÇA I.P.



PROCURADORIA GERAL  
DA REPÚBLICA



INSPEÇÃO-GERAL DE FINANÇAS



Conselho Superior da Magistratura

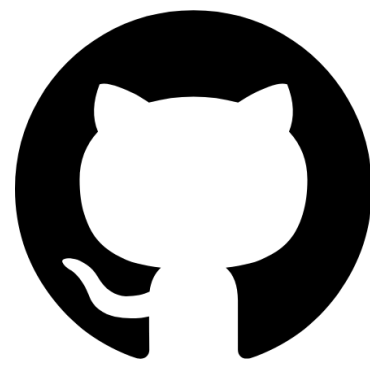
IGSJ

Inspeção-Geral dos  
Serviços de Justiça





# Thank you!



JusticeChain is available at:  
<https://github.com/RafaelAPB/JusticeChain>

[Rafael Belchior](#)

rafael.belchior@tecnico.ulisboa.pt