BLING
(Blockchain in Government)
Use-case

https://northsearegion.eu/bling/
Project End: 31.06.2022
Prostitutes Protection Act

Prof. Dr.-Ing. habil. Jorge Marx Gómez

Ali Amin Rezaei

Problems Statement

- Prostitute´s health certificate can be **faked**
  - Cannot make sure about the **source and integrity** of the certificate

- Saving the **privacy** of prostitutes is challenging
  - Having full control over who can access his/her identity

- Prostitutes are changing their places from time to time
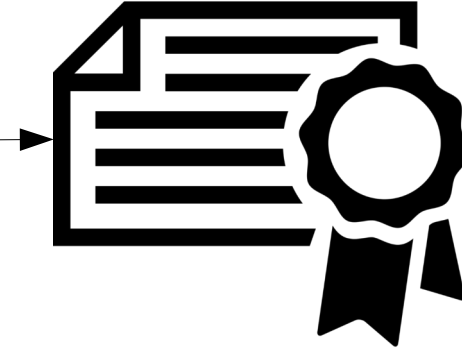 - **Expand-ability** should be taken into account
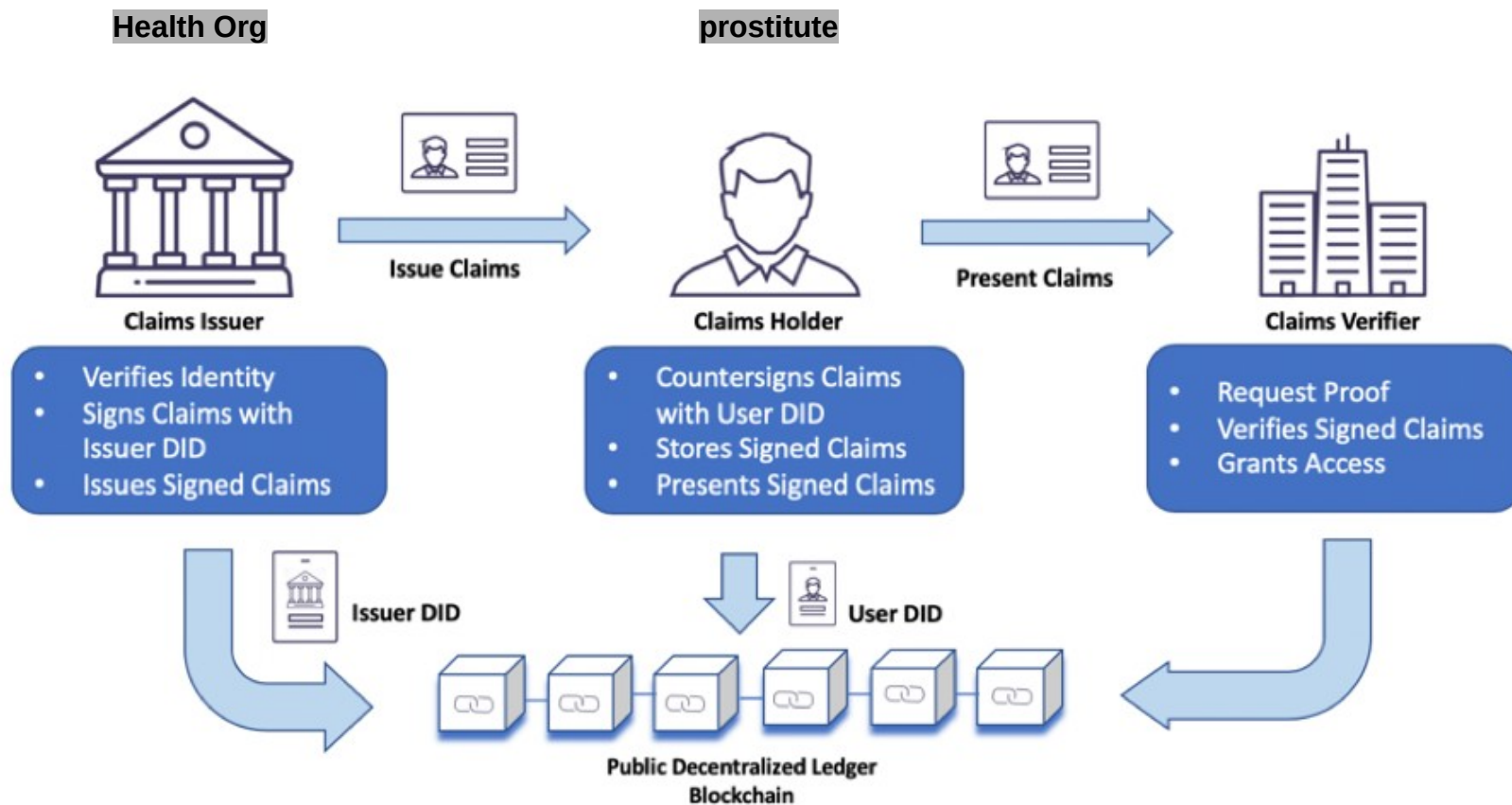
Solution?

1. Integrity

Cryptography algorithm

2. Source **?**

3. Privacy **?**

Self Sovereign Identity Model

**Addressing privacy and source
=
DID (Decentralized ID)**

Health Org

prostitute

Claims Issuer
- Verifies Identity
- Signs Claims with Issuer DID
- Issues Signed Claims

Issue Claims

Claims Holder
- Countersigns Claims with User DID
- Stores Signed Claims
- Presents Signed Claims

Present Claims

Claims Verifier
- Request Proof
- Verifies Signed Claims
- Grants Access

Issuer DID

User DID

Public Decentralized Ledger Blockchain

Public vs Private Blockchain

	Public		Private	
Access	Unlimited	✅	Limited	
Authority	Decentralized	✅	Partially Centralized	
Transaction Speed	Slow		Fast	✅
Transaction-fee	Yes		No	✅

Public blockchain VS IOTA

- Transactions on public blockchain are **slow** and **costs** fee
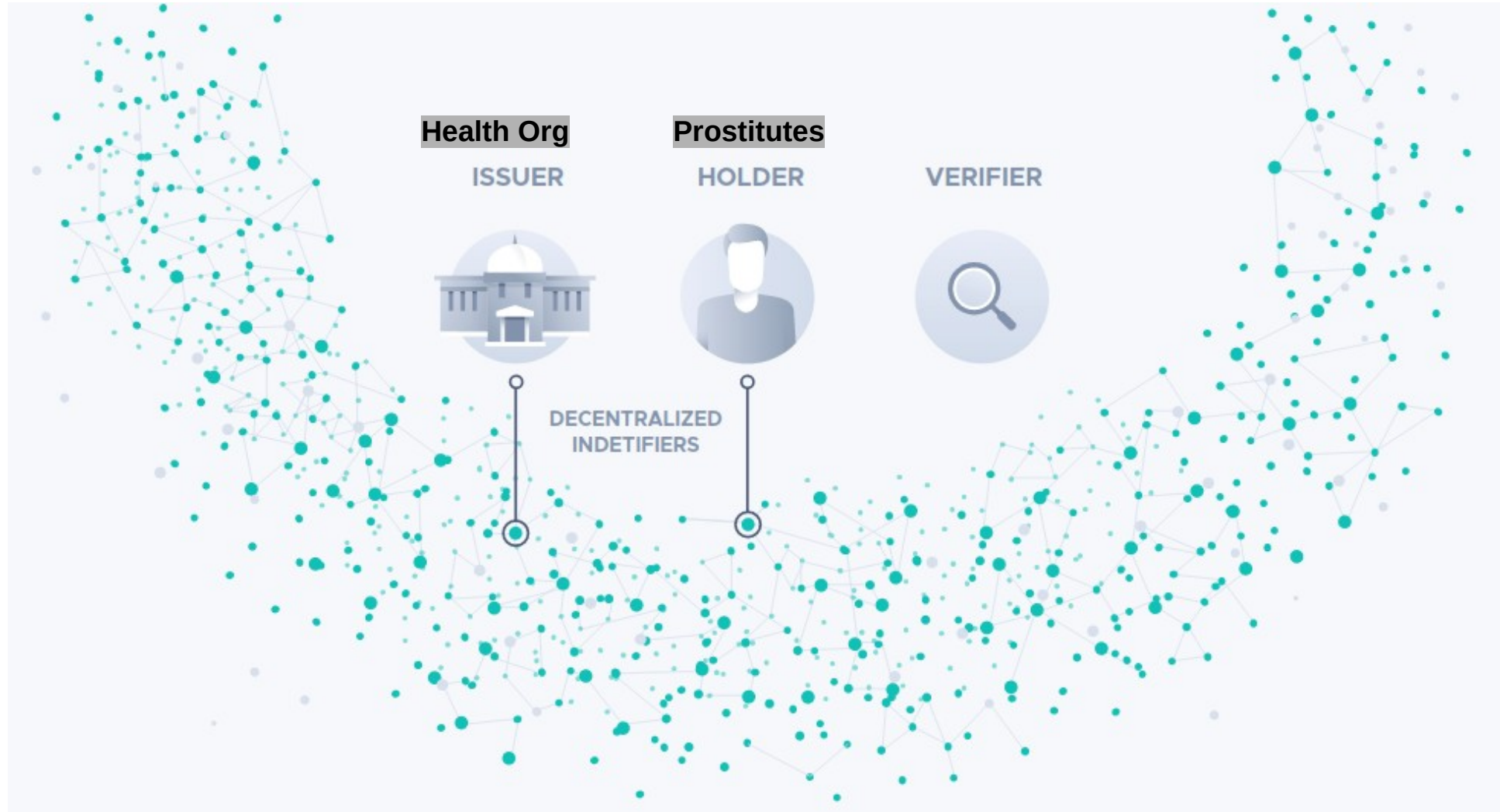
THE BLOCKCHAIN BOTTLENECK

More Activity
=
Same Validation
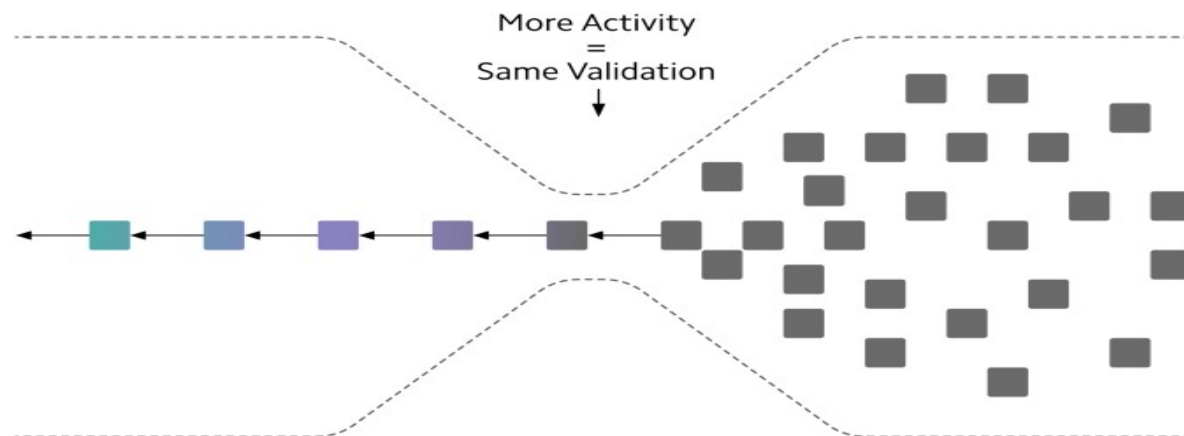
- Transactions on IOTA are much **faster** and **fee-less**

- Quantum-proof security

THE IOTA TANGLE SCALES!

More Activity
=
More Validation
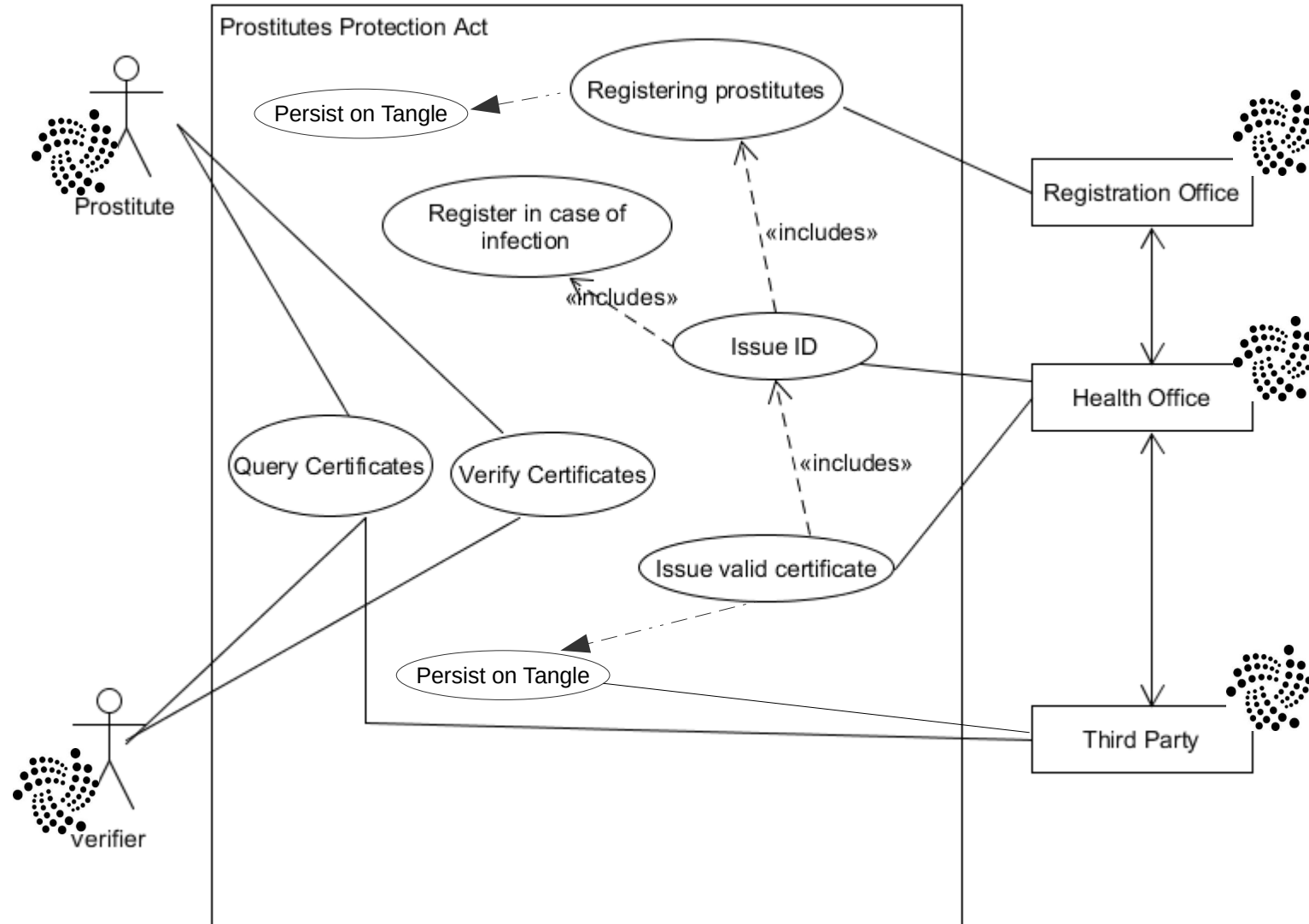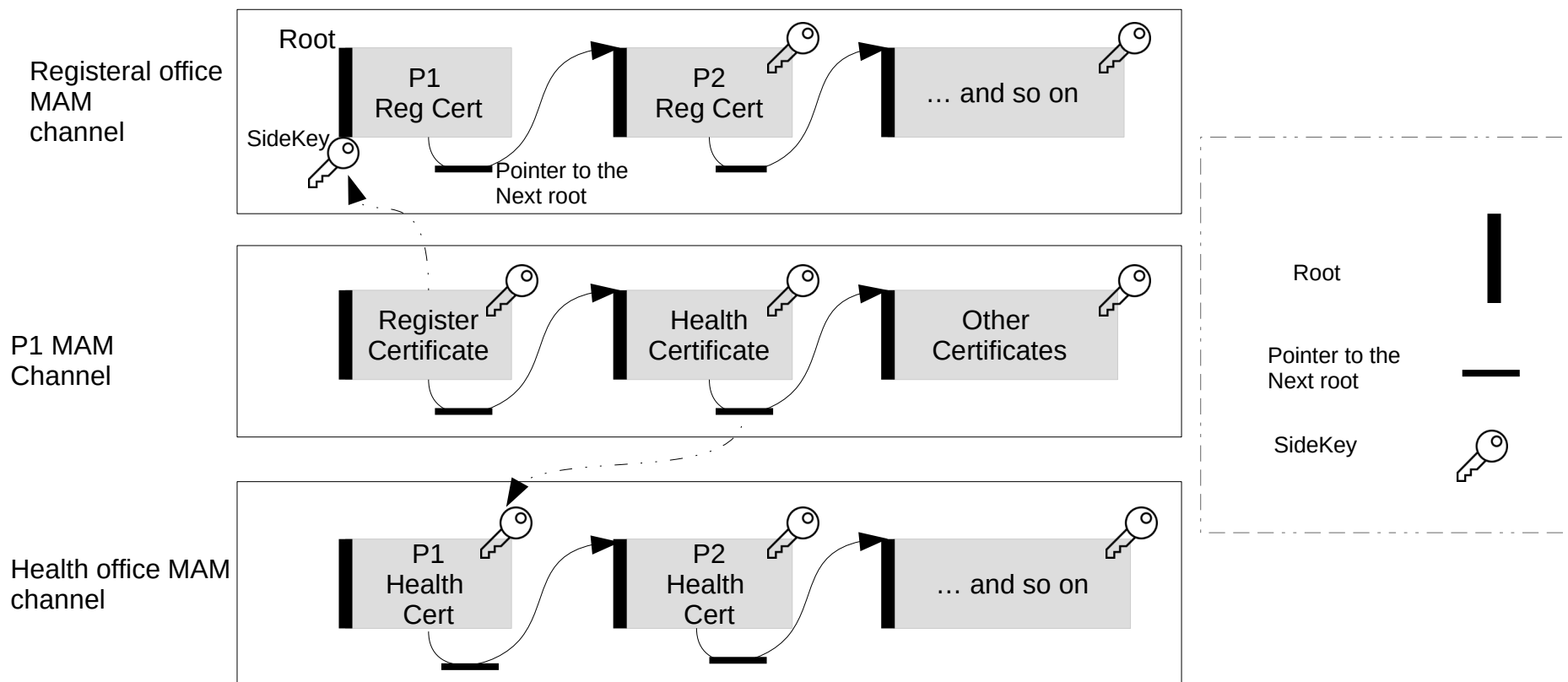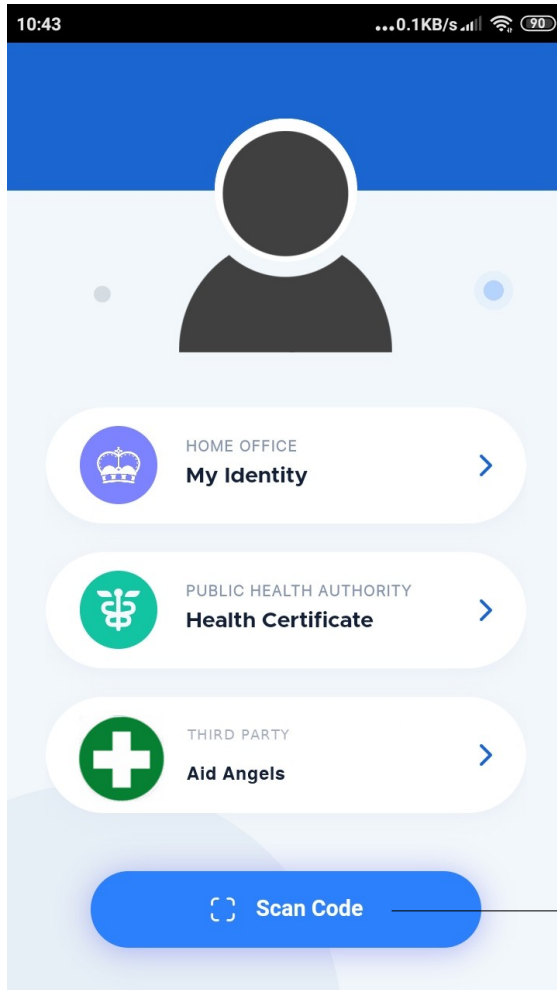
IOTA network

Health Org   **Prostitutes**

ISSUER   HOLDER   VERIFIER

DECENTRALIZED
INDETIFIERS
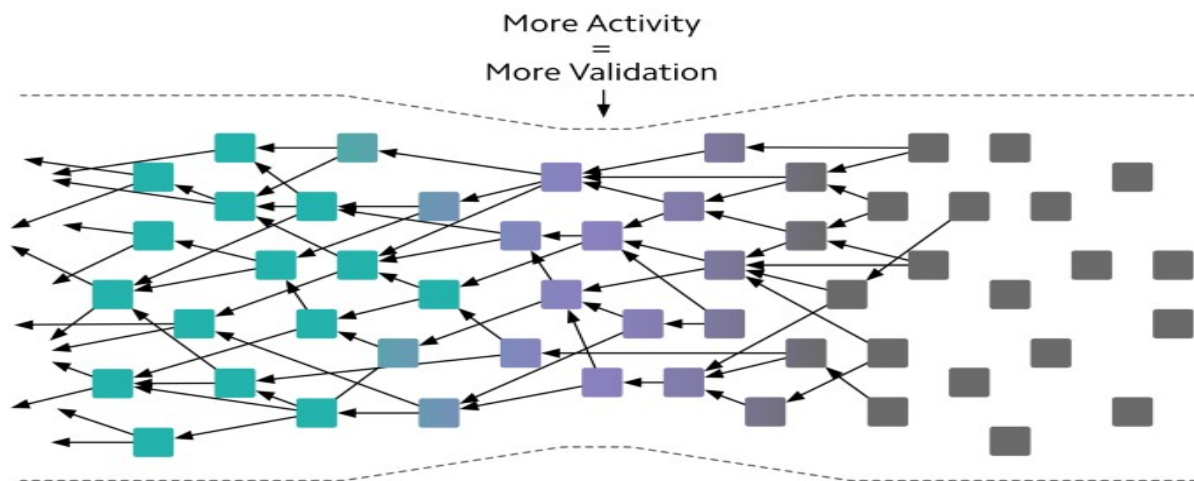
Use-Case Diagram

Architecture (Based on MAM channel)

Digital wallet

Prostitute

Issuer
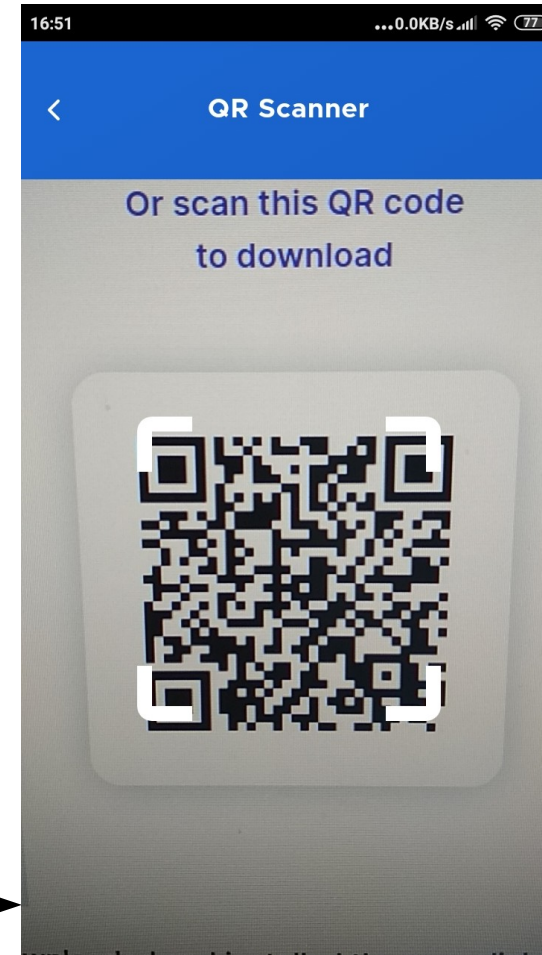
Providing Certificate to Third-parties

Prostitute

**Verifier**

Extention-call12: Ambulant Covid Surveillance

- The pandemic can bring medical system to the limit

- Sensors can facilitate the monitoring process from remote

- However storing sensor data on the cloud might cause security and privacy issues

- A distributed ledger system can address the issues
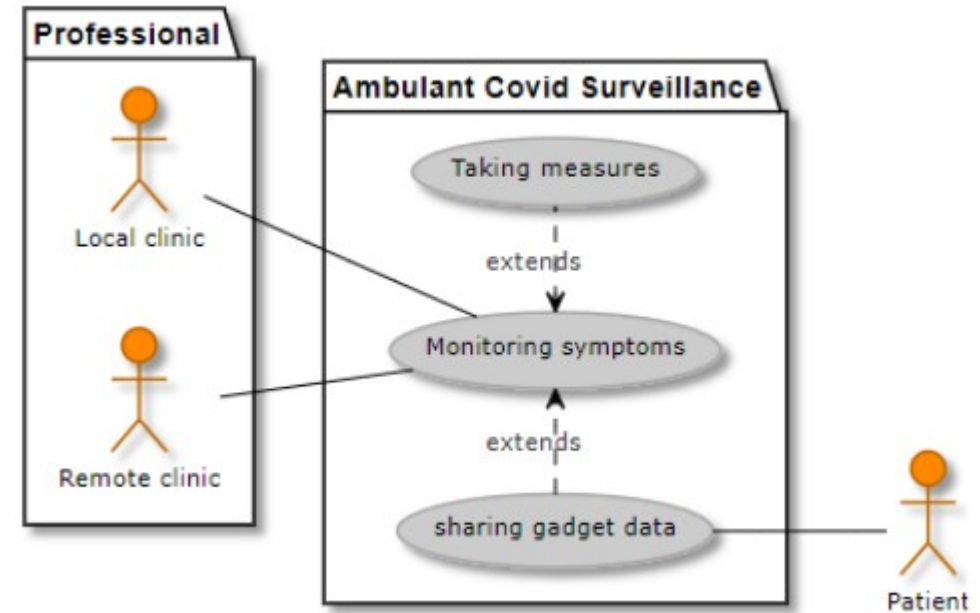
Extention-call12: Ambulant Covid Surveillance

Proposed Architecture based on IOTA multi branch Stream
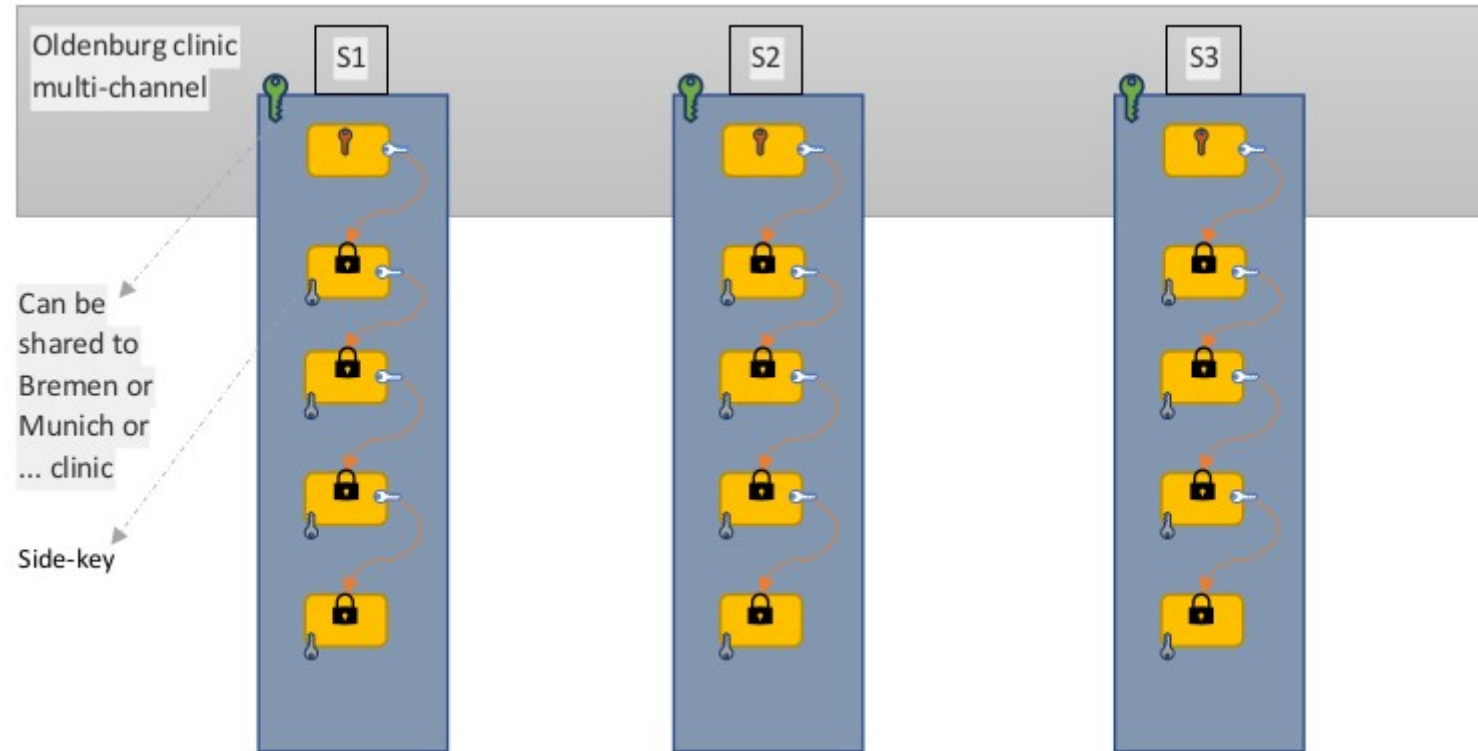
Thank you for your kind attention.

Are there any questions?

Get in touch

jorge.marx.gomez@uol.de

ali.amin.rezaei@uol.de

Using Blockchain?

Generic approach

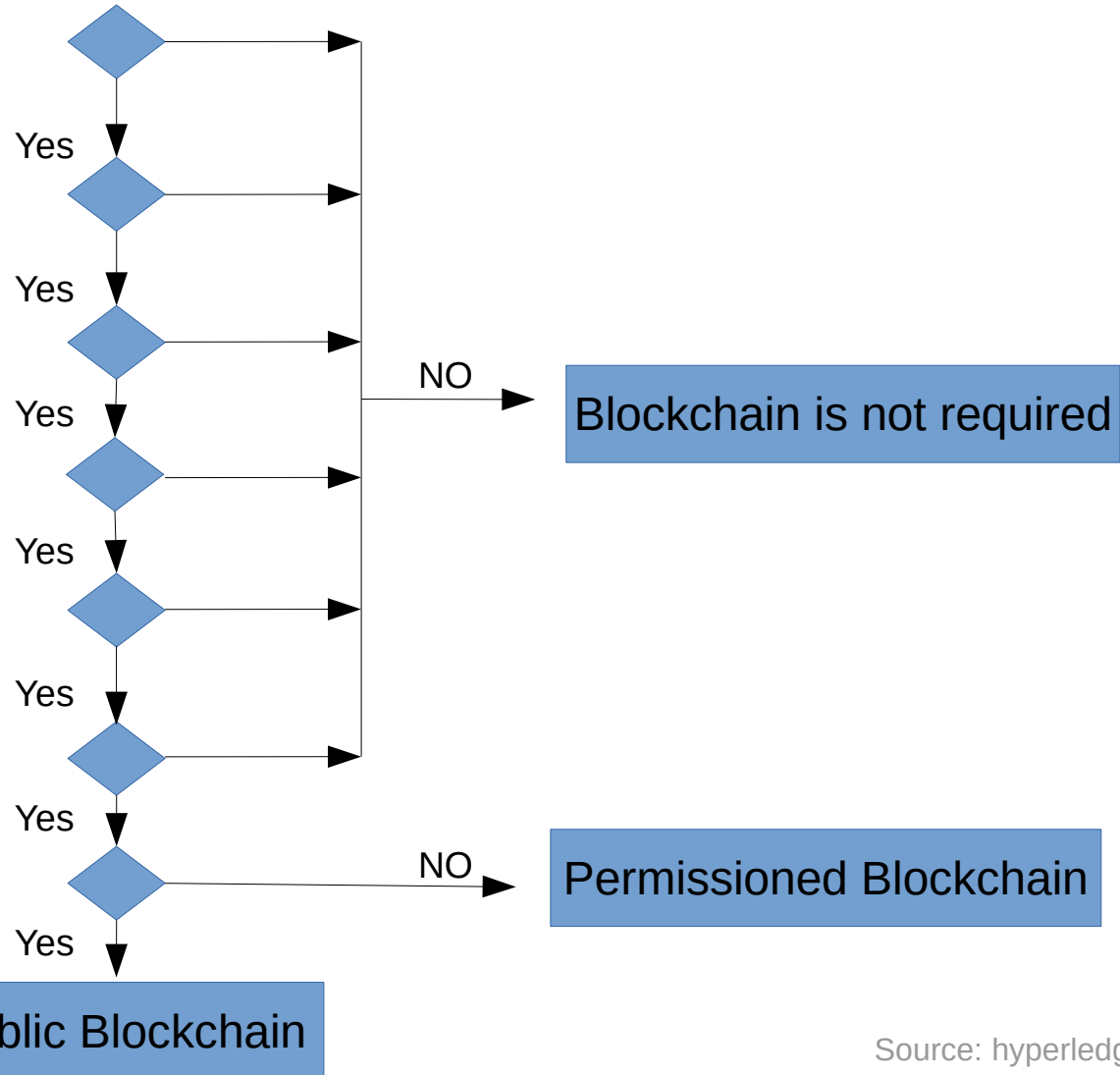Need for a shared common database?

Multiple parties involved?

Parties involved are **not trusted**?

Rules governing participants are uniform?

Need for an objective immutable log?

Rules of transaction do not change frequently?

Are transactions public?

Yes

Yes

Yes

Yes

Yes

Yes

Yes

NO → Blockchain is not required

NO → Permissioned Blockchain

Public Blockchain

Private Blockchain – Class Diagram