Hyperledger Global Forum 2021

Virtual 2 / ● Business

Trust Data Sharing and Utilization Infrastructure for Sensitive Data using Hyperledger Avalon

June 10th, 2021

Hitachi, Ltd., Research and Development Group

Koshi Ikegawa, and Nao Nishijima

HITACHI
Inspire the Next

Contents

1. Introduction
2. Design and Approach
3. Work in Progress
4. Summary

HITACHI
Inspire the Next

Contents

1. **Introduction**
2. Design and Approach
3. Work in Progress
4. Summary

Market

Increasing demand for trust data sharing & utilization

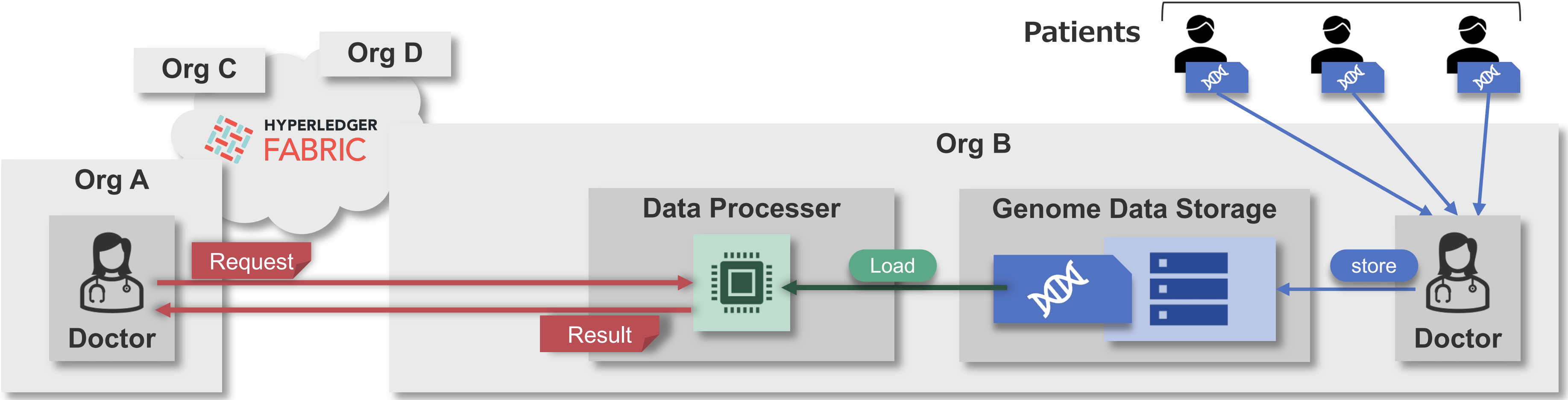
Data Free Flow with Trust (DFFT) is advocated by the World Economic Forum (2019)

- Focus on cross border data flows
  - Blockchain is needed
- There are many types of data to share
  - Open data: map, news, disaster info, etc...
  - **Sensitive data: healthcare, government, personal, etc...**

Background

In our use case, we created an infrastructure to manage and utilize genome data in multiple organizations and has confirmed PoC [1]

- Multiple organizations are participating in a blockchain network for genome data sharing
- Raw genome data must not be passed on to other organizations because the data is sensitive data
- Analyze the data on the processor of the data owner org and pass only the results to other orgs

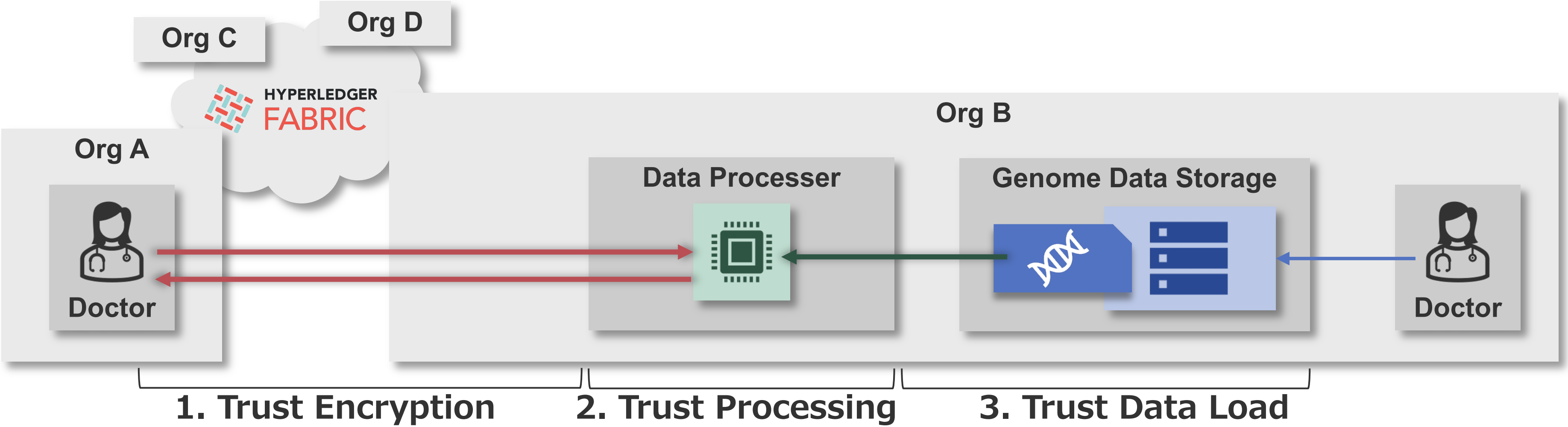


[1] Koshi Ikegawa, Nao Nishijima, Yoji Ozawa, Katsuhiro Fukunaka, Hironori Emaru, Masaru Hisada, Akihito Kaneko, Eiichi Araki, Ai Okada and Yuichi Shiraishi. Secure and Traceable System for Genomic Data Sharing Using Hyperledger Fabric Blockchain (in Japanese). IIBMP2020, September 2020.

Motivation

Realize Trust Data Sharing and Utilization Infrastructure for Sensitive Data

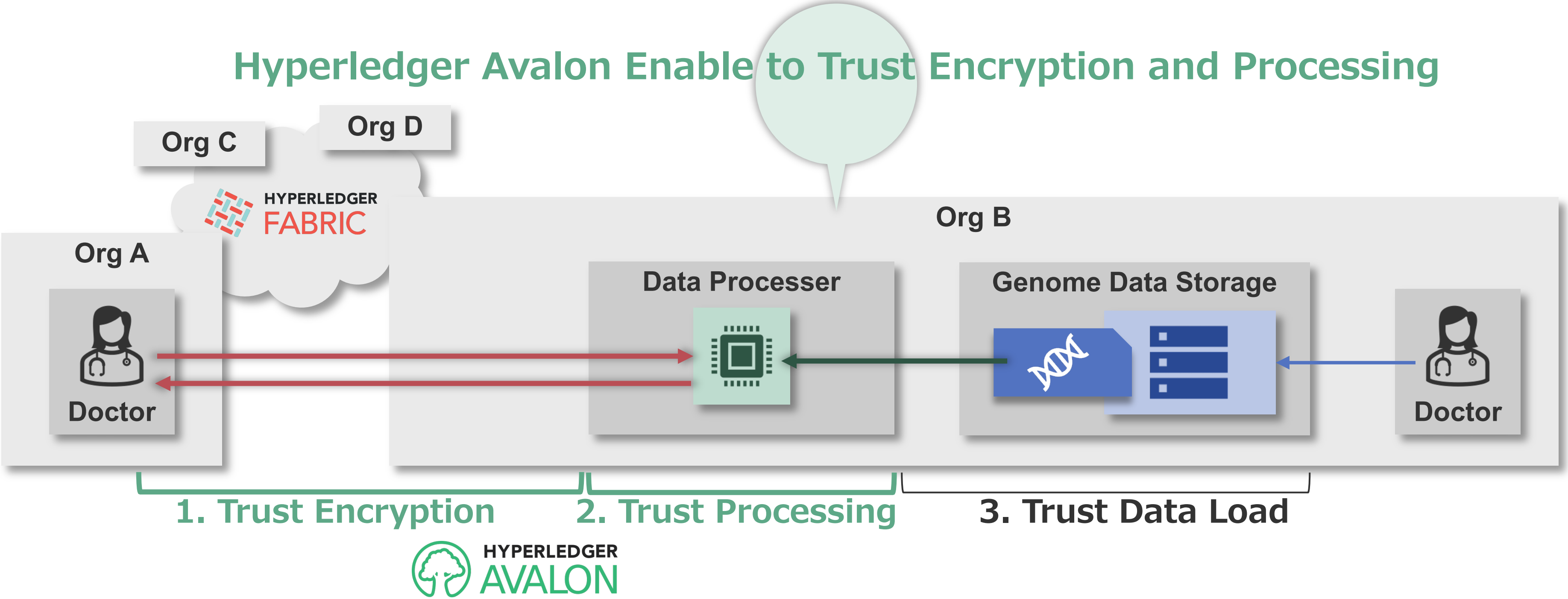
- Personal data, such as genome data needs to be handled with particular care in accordance with the law
- Focus on the following three to realize the infrastructure



Motivation

Realize Trust Data Sharing and Utilization Infrastructure for Sensitive Data

- Personal data, such as genomic information needs to be handled with particular care in accordance with the law
- Focus on the following three to realize the infrastructure

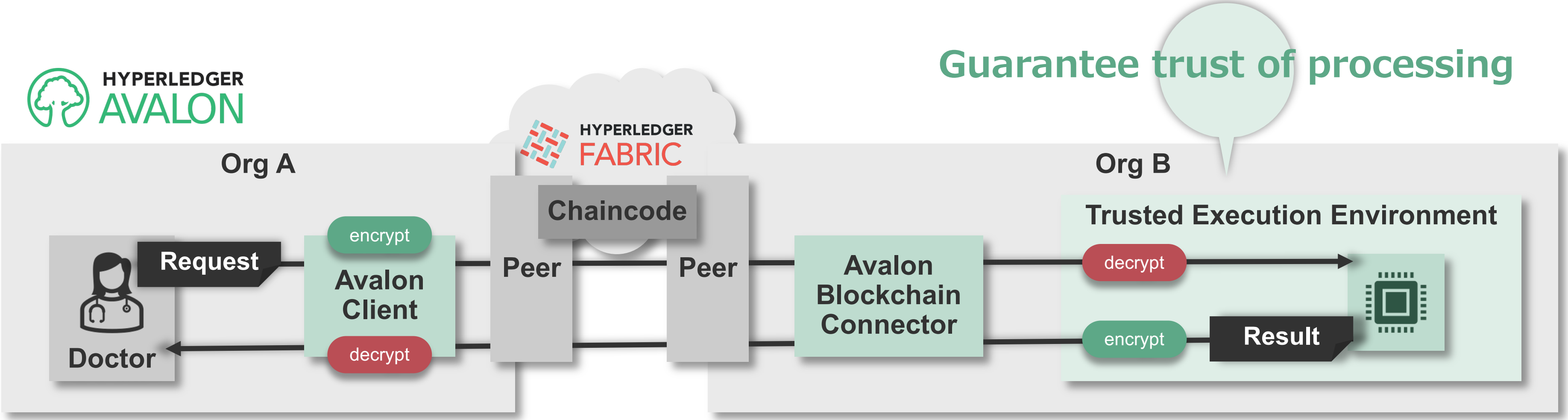

Hyperledger Avalon Enable to Trust Encryption and Processing

1. Trust Encryption
2. Trust Processing
3. Trust Data Load

What is Hyperledger Avalon

Avalon is a Hyperledger project to realize Off-chain Trusted Computing

- Avalon is the **first and only implementation** of EEA's[1] Off-Chain Trusted Compute Specification
- **Avalon guarantees a trust execution of a program in the protected area** by CPU native secure function (Trusted Execution Environment)



Simplified Hyperledger Avalon Architectural Diagram

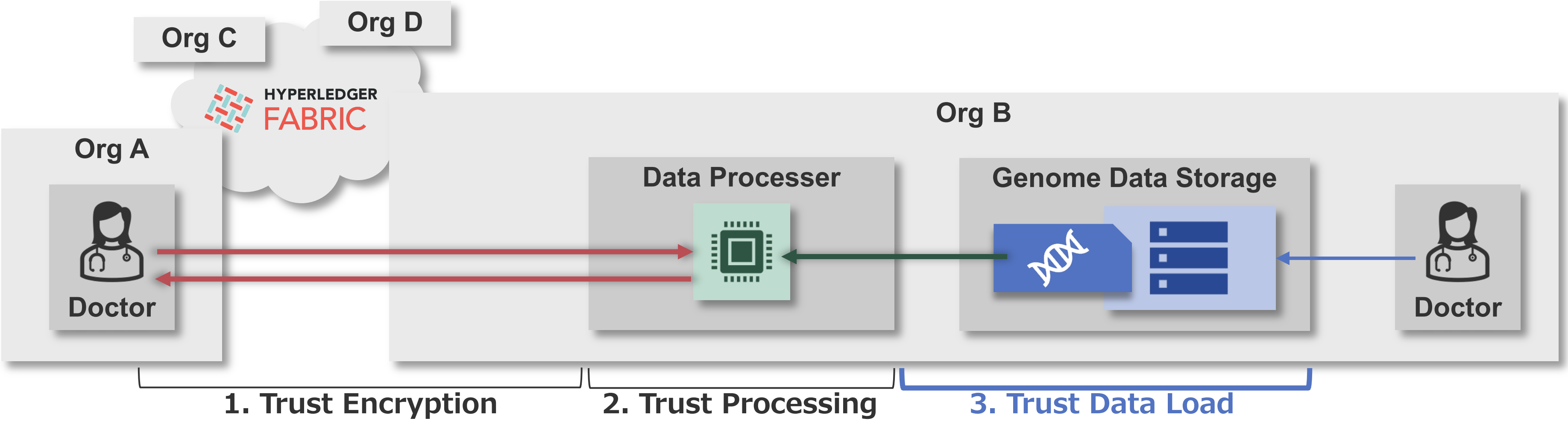
What is Trusted Execution Environment (TEE)

Trusted Execution Environment is CPU Security Technology

- TEE is a CPU security function that generates a protected area called enclave in memory and loads programs and data into the area, enabling programs to be executed while protecting sensitive data
  - Provided by CPU vendors such as **Intel Software Guard Extensions (SGX)**, ARM TrustZone, AMD Secure Encrypted Virtualization (SEV), etc.
- In Hyperledger Avalon, Intel SGX is being used for implementation.
  - In Intel SGX, the encrypted area in memory is called Enclave.

Focus Point in This Session

Enable to Trust Data Load



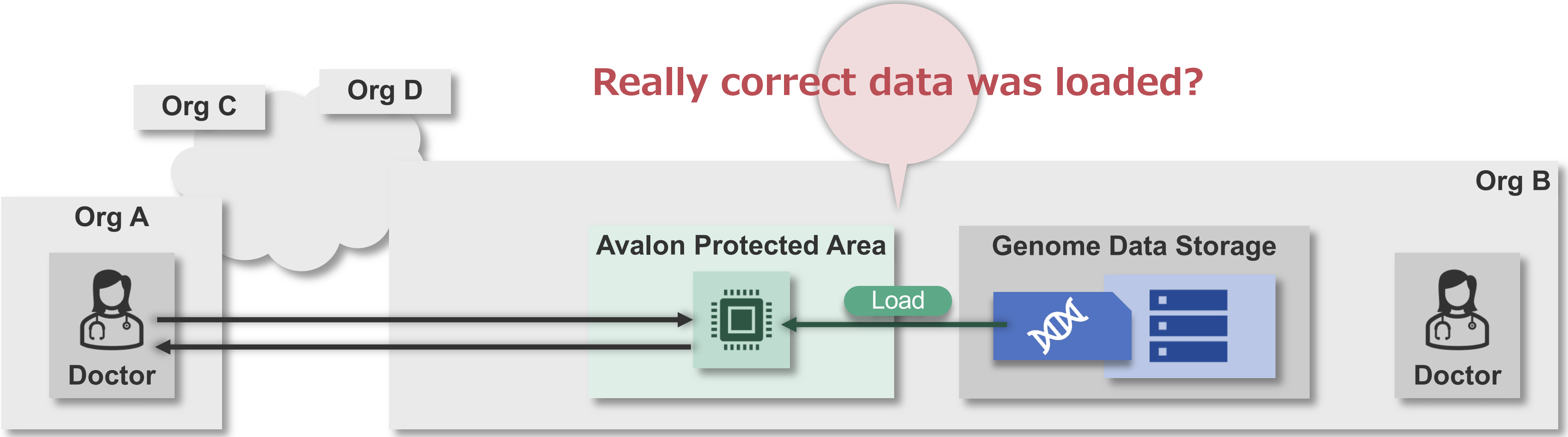
HITACHI
Inspire the Next

Contents

1. Introduction
2. **Design and Approach**
3. Work in Progress
4. Summary

Issue

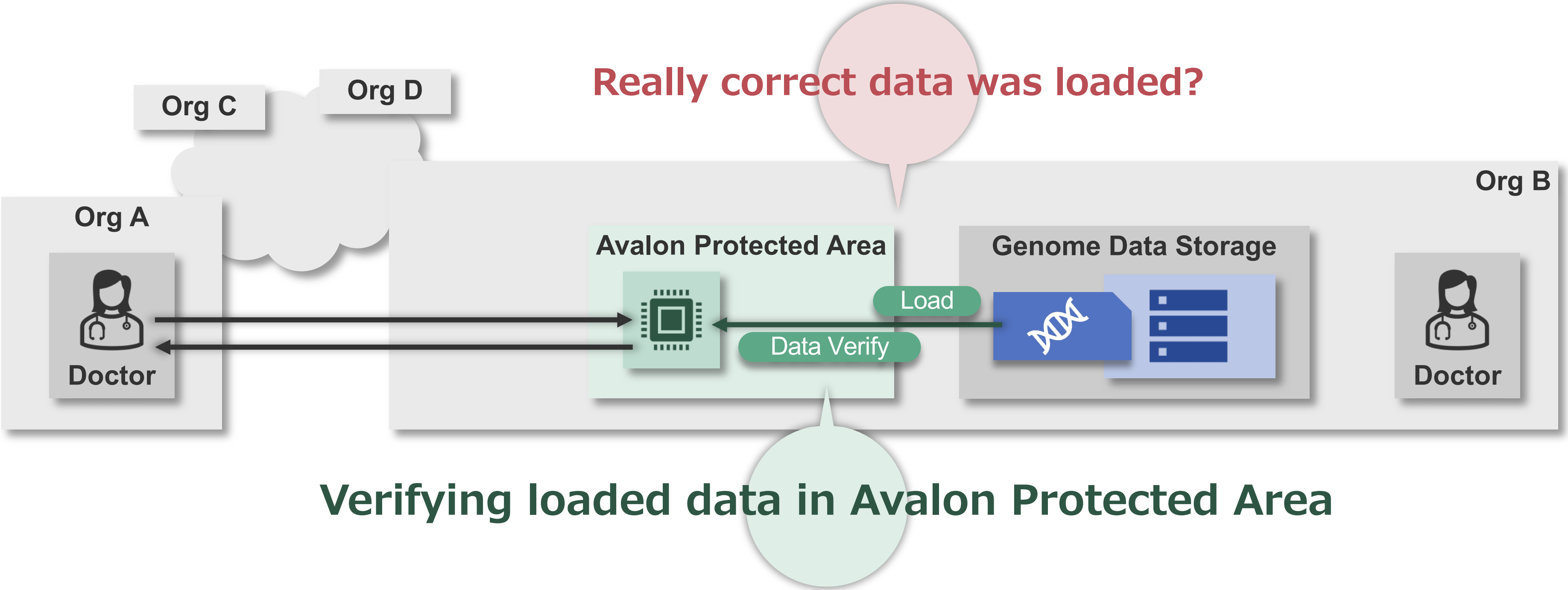
Unable to verify the correctness of data on private storage



Really correct data was loaded?

Design Idea

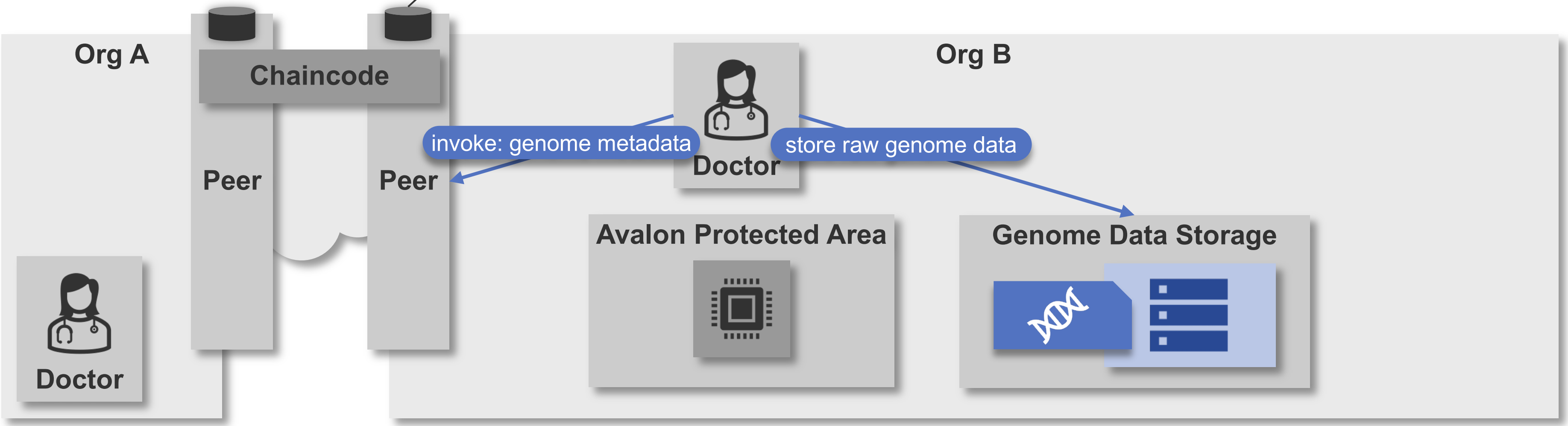
Unable to verify the correctness of data on private storage



Approach | Step 1: store raw genome data & metadata

State DB: Metadata Management

Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...



Approach | Step 2: Access control

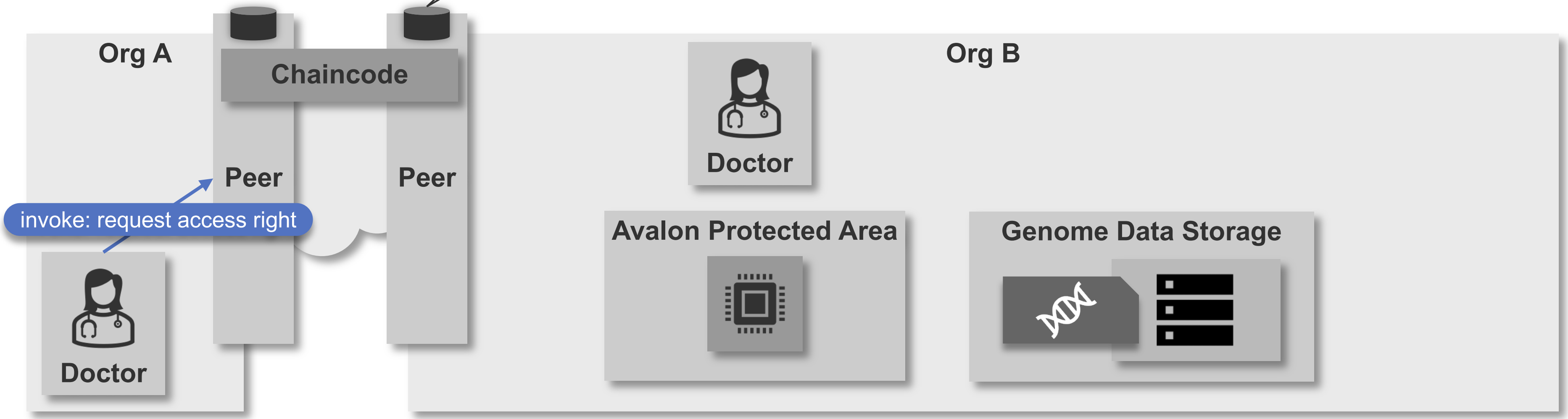
HITACHI
Inspire the Next

State DB: Metadata Management

Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	



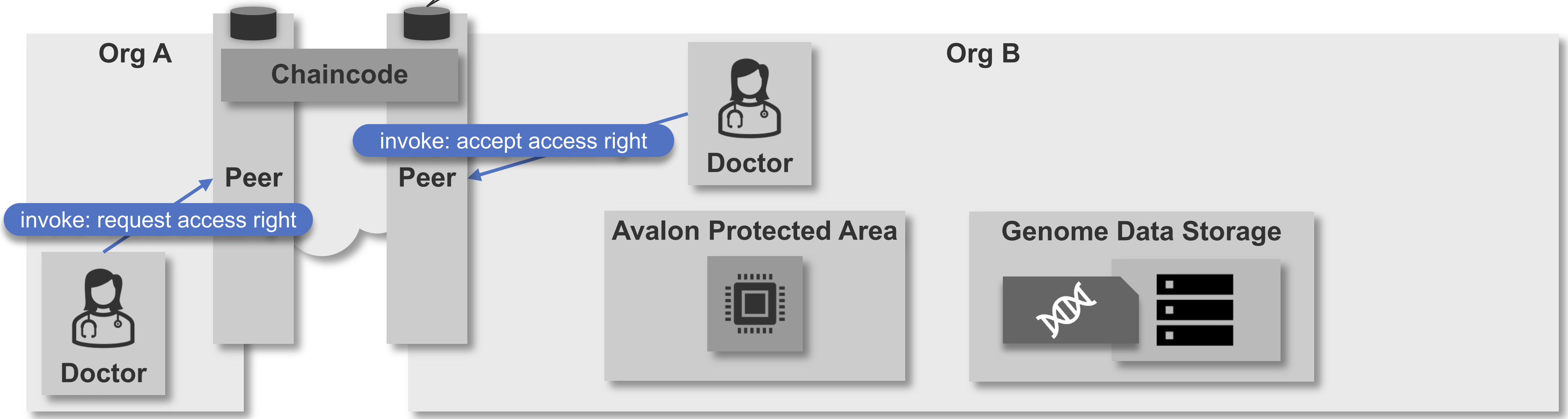
Approach | Step 2: Access control

State DB: Metadata Management

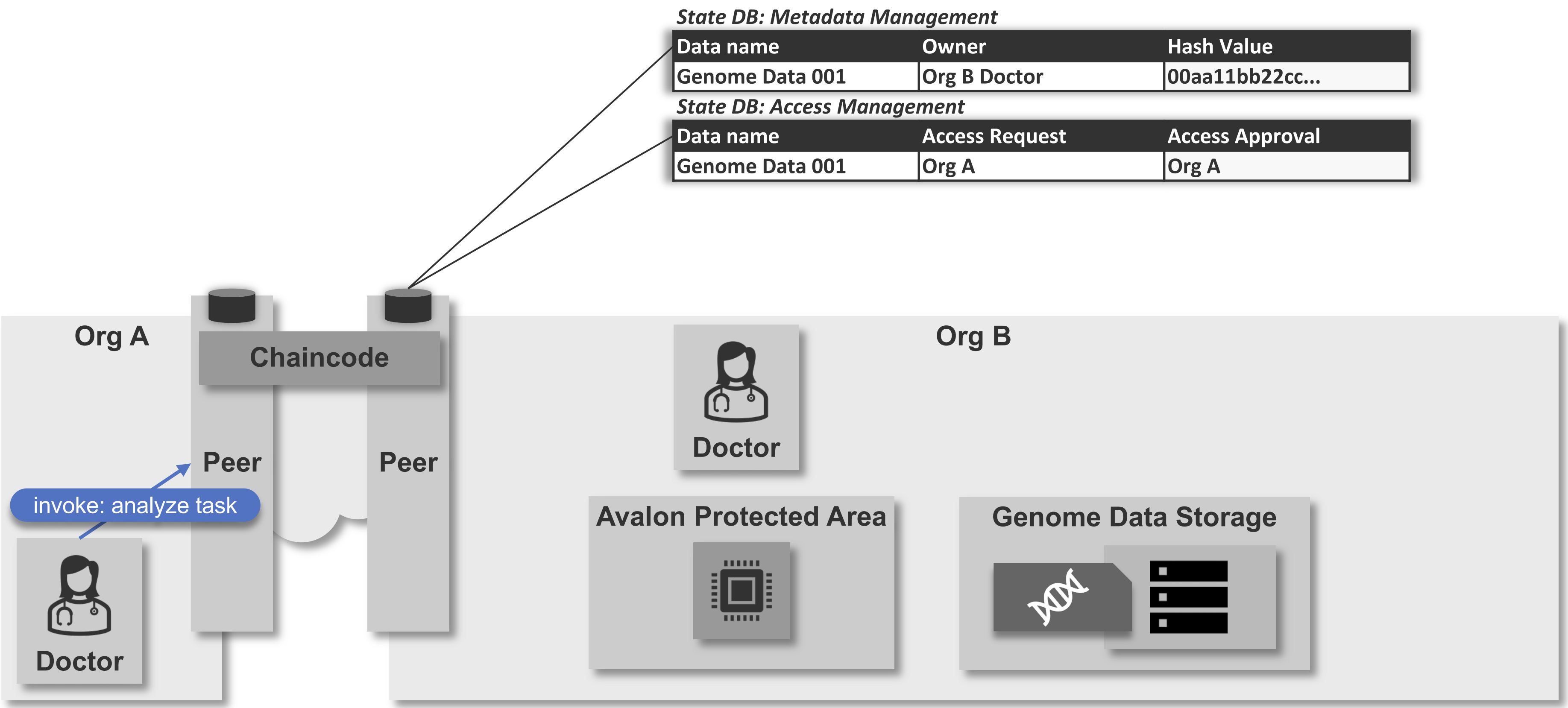
Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc…

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A



Approach | Step 3: Analyze Task Request



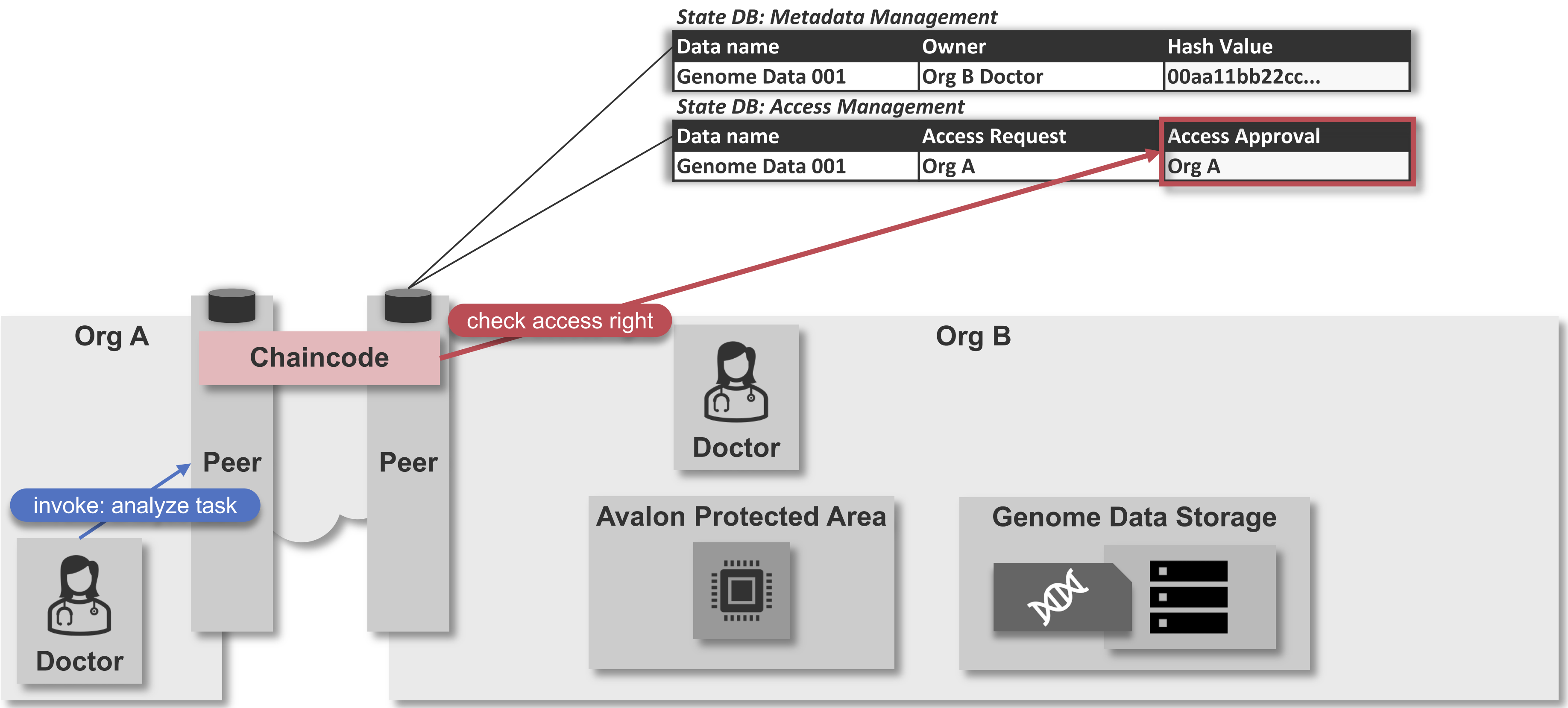
State DB: Metadata Management

Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

Approach | Step 3: Analyze Task Request



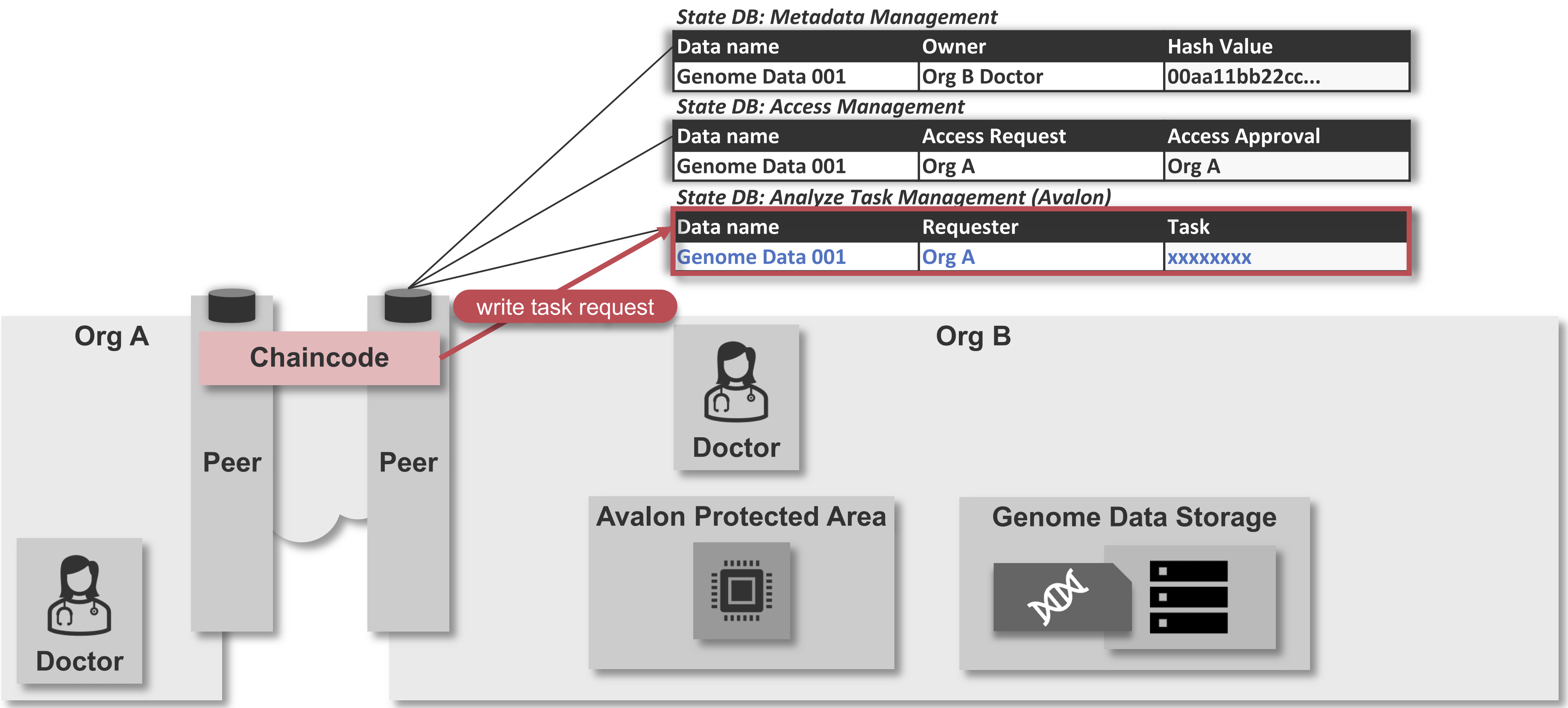
State DB: Metadata Management

Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

Approach | Step 3: Analyze Task Request



State DB: Metadata Management

Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

State DB: Analyze Task Management (Avalon)

Data name	Requester	Task
Genome Data 001	Org A	xxxxxxxx

Approach | Step 3: Analyze Task Request

State DB: Metadata Management

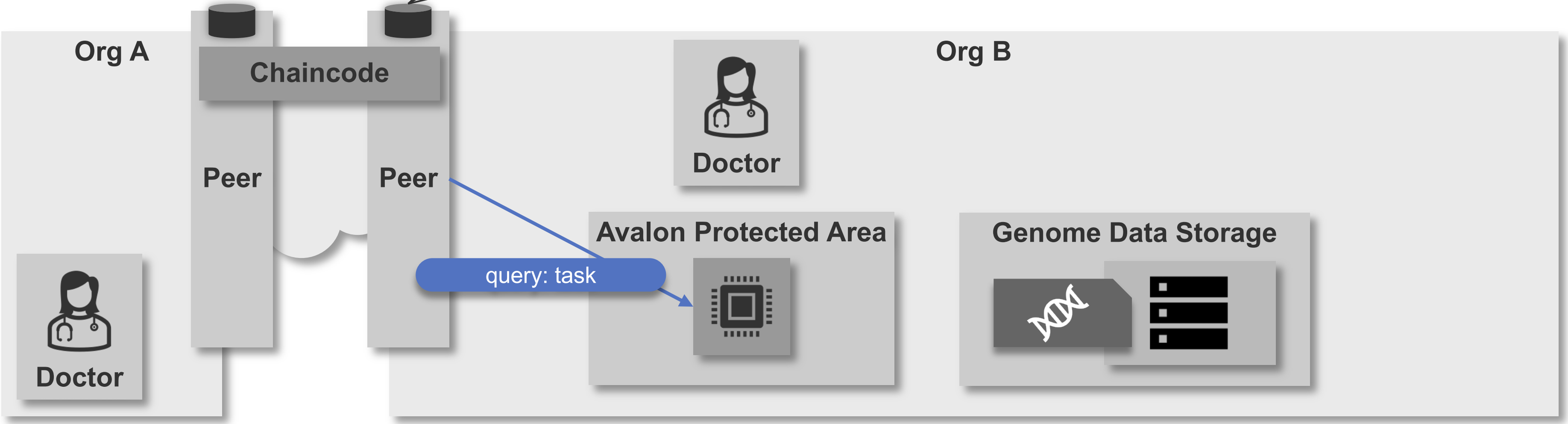
Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

State DB: Analyze Task Management (Avalon)

Data name	Requester	Task
Genome Data 001	Org A	xxxxxxxx



Approach | Step 3: Analyze Task Request

State DB: Metadata Management

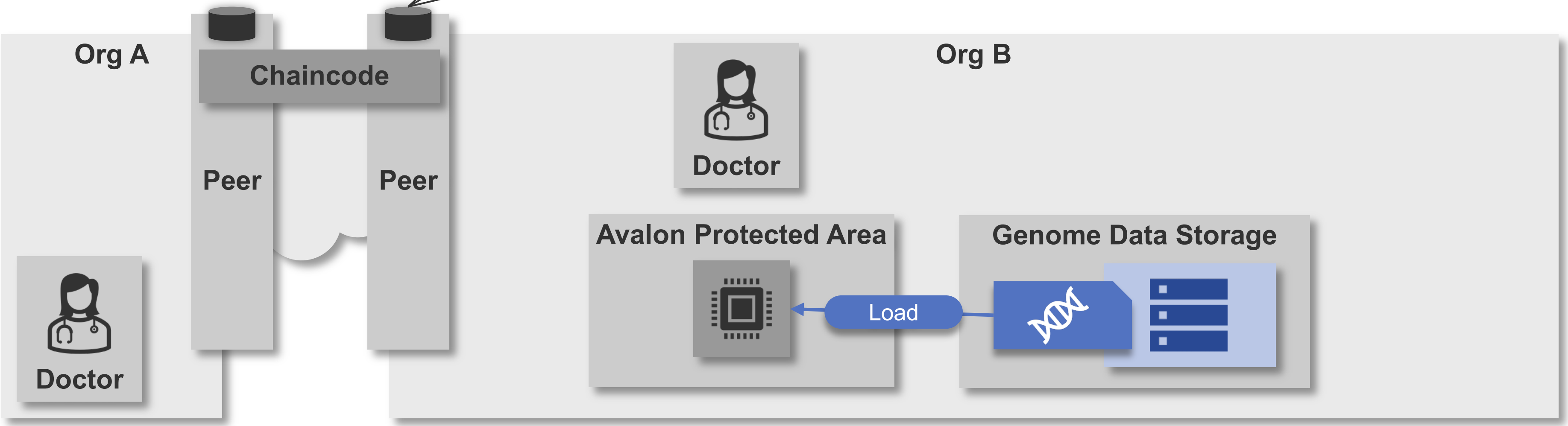
Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

State DB: Analyze Task Management (Avalon)

Data name	Requester	Task
Genome Data 001	Org A	xxxxxxxx



Approach | Step 3: Analyze Task Request

State DB: Metadata Management

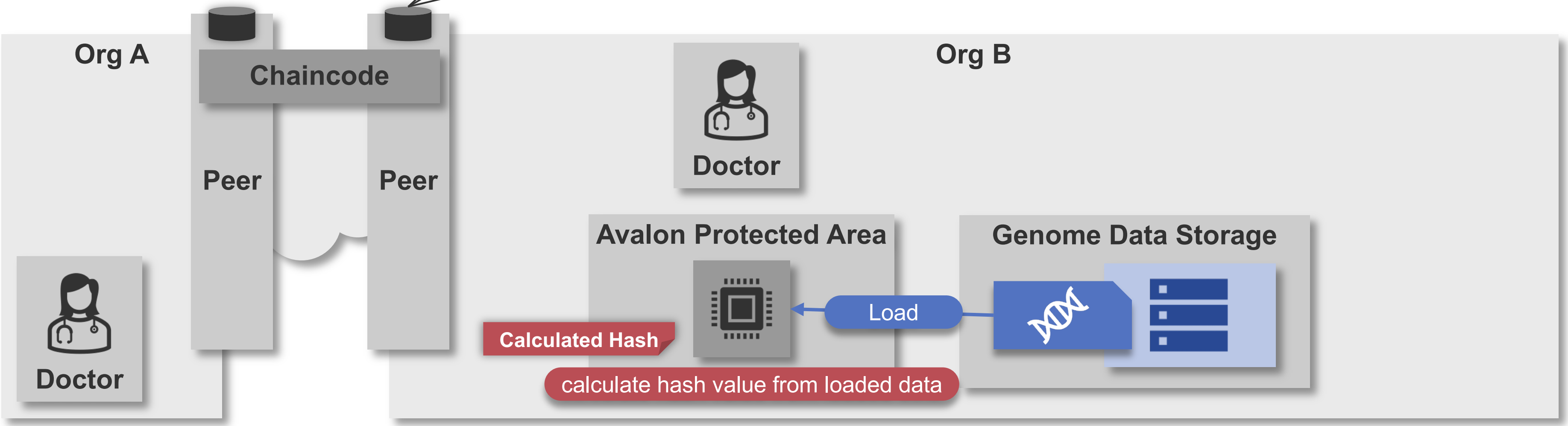
Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc…

State DB: Access Management

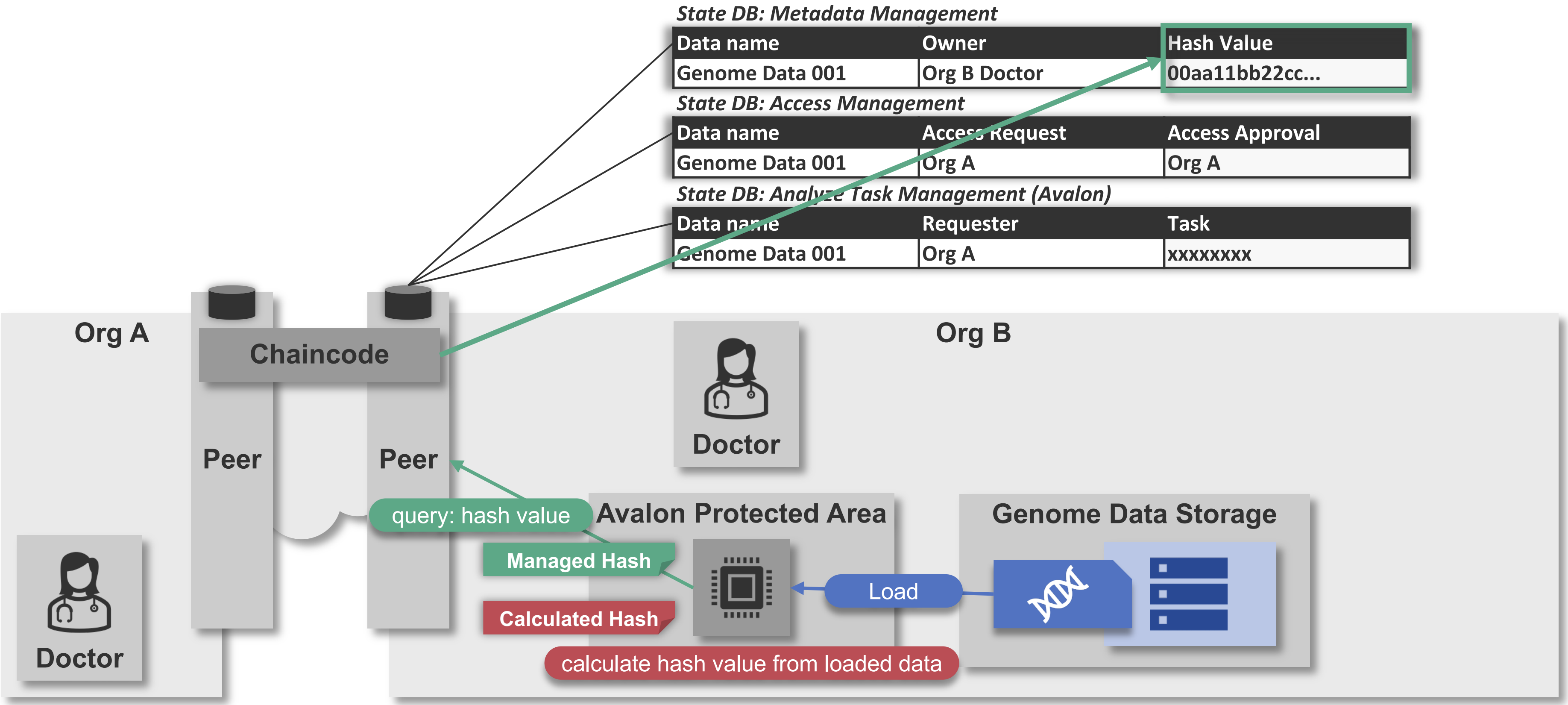
Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

State DB: Analyze Task Management (Avalon)

Data name	Requester	Task
Genome Data 001	Org A	xxxxxxxx



Approach | Step 3: Analyze Task Request



State DB: Metadata Management

Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

State DB: Analyze Task Management (Avalon)

Data name	Requester	Task
Genome Data 001	Org A	xxxxxxxx

Approach | Step 3: Analyze Task Request

HITACHI
Inspire the Next

State DB: Metadata Management

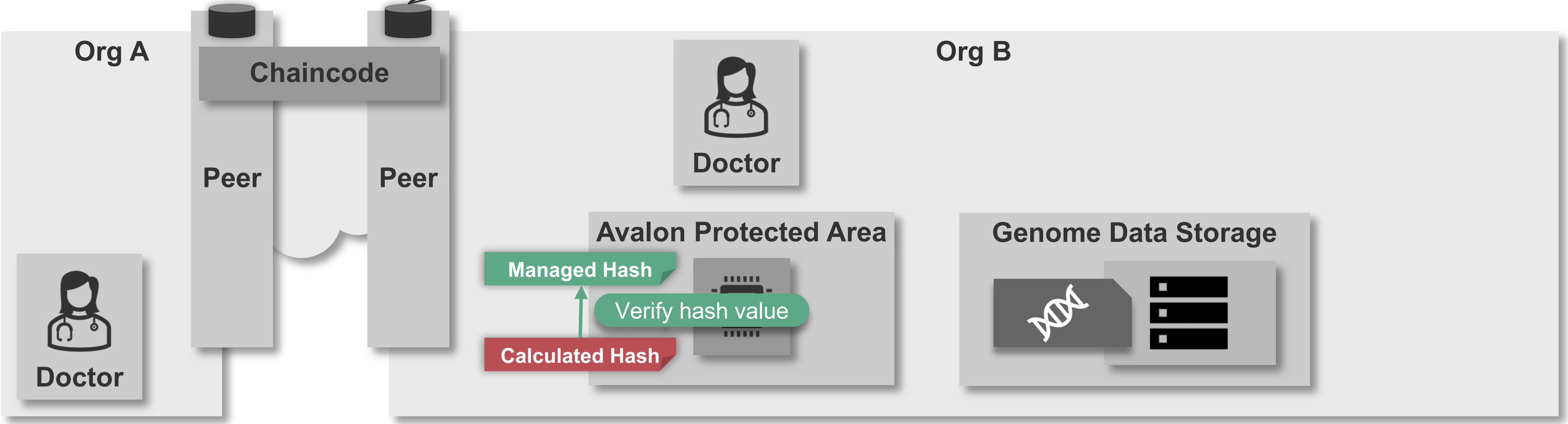
Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

State DB: Analyze Task Management (Avalon)

Data name	Requester	Task
Genome Data 001	Org A	xxxxxxxx



Approach | Step 3: Analyze Task Request

State DB: Metadata Management

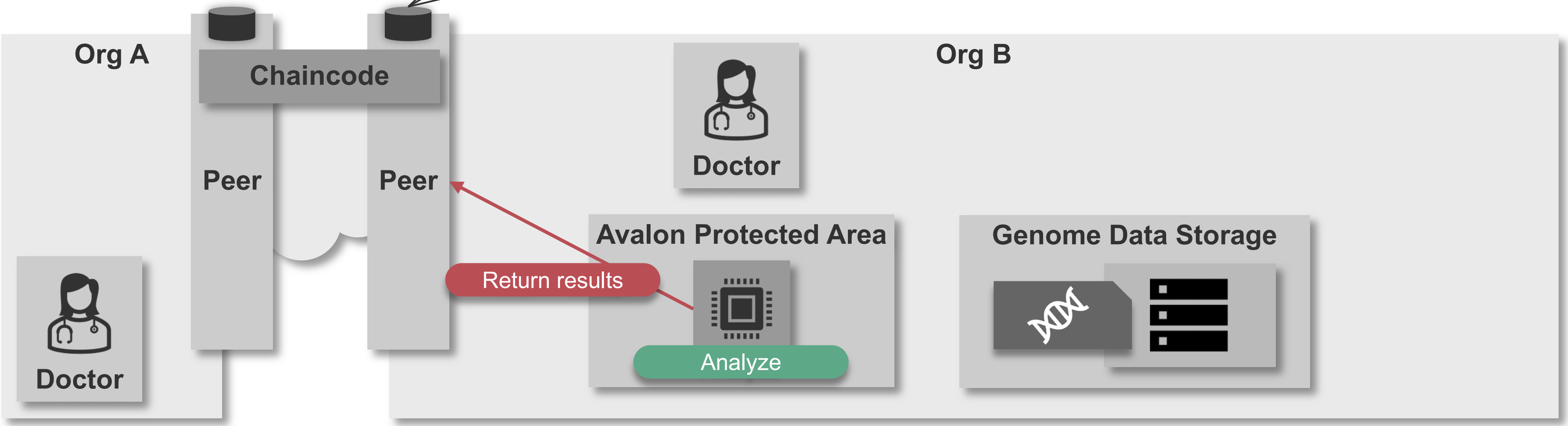
Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

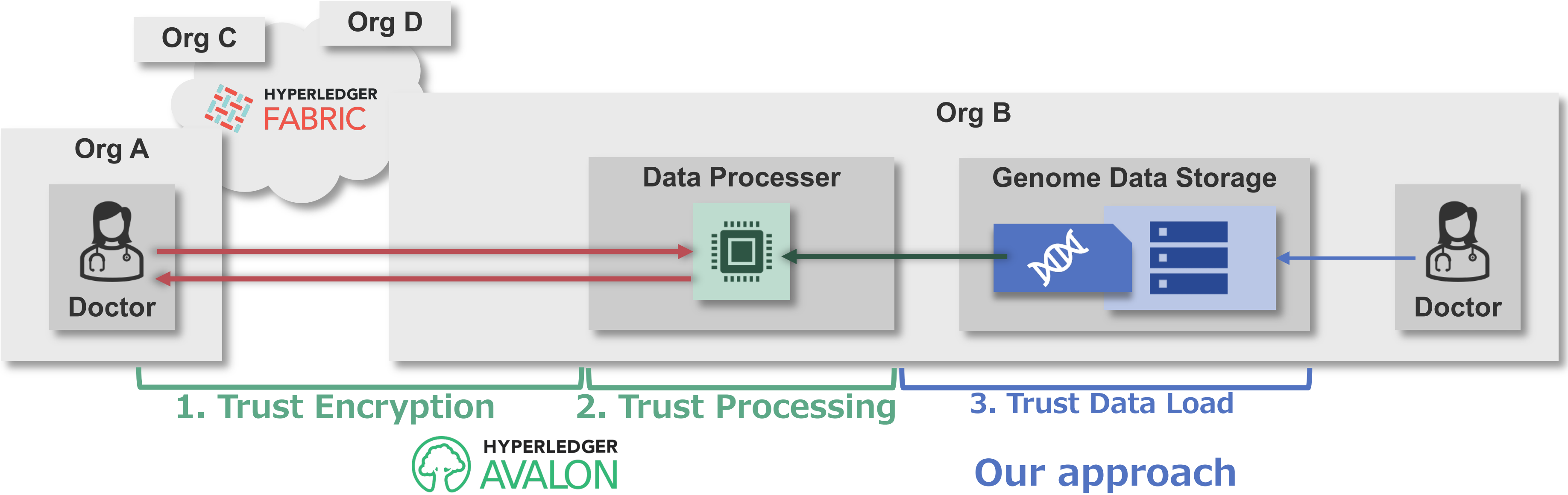
State DB: Analyze Task Management (Avalon)

Data name	Requester	Task	Result
Genome Data 001	Org A	xxxxxxxx	yyyyyyy



Realize trust infrastructure

By using Avalon and implementing our approach, we can realize a trustworthy data utilization infrastructure.



Our approach

HITACHI
Inspire the Next

Contents

1. Introduction
2. Design and Approach
3. **Work in Progress**
4. Summary

Further improvements

We can improve our infrastructure even further

Not encrypted
(because processing in on-chain is required)

State DB: Metadata Management

Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

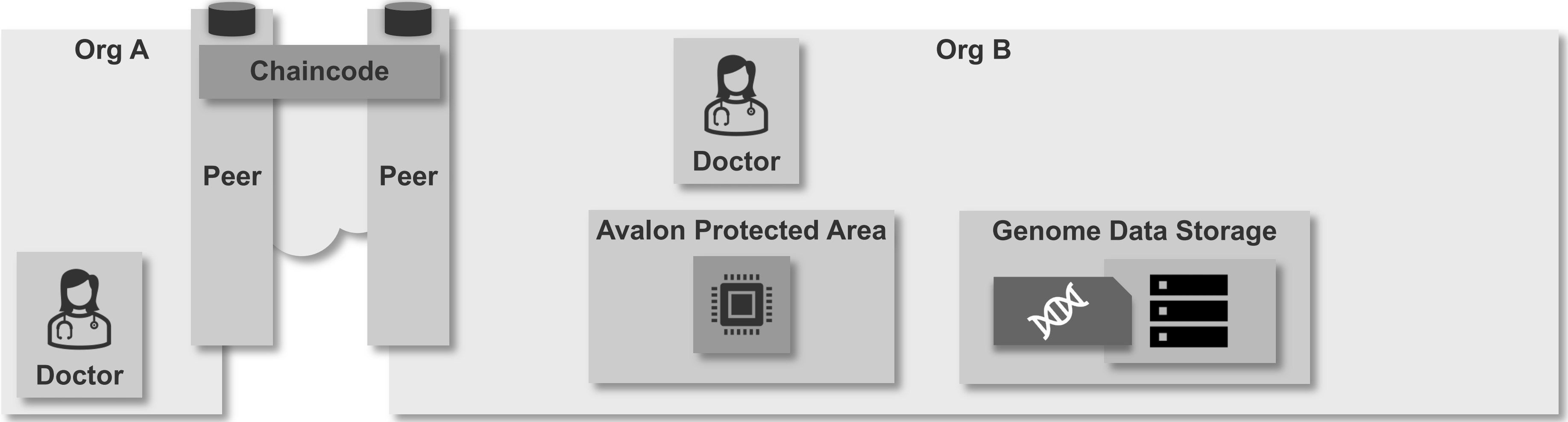
State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

Encrypted using Avalon

State DB: Analyze Task Management (Avalon)

Data name	Requester	Task	Result
Genome Data 001	Org A	xxx	yyy



Further improvements

We can improve our infrastructure even further

No need for encryption
(Metadata is shared info)

State DB: Metadata Management

Data name	Owner	Hash Value
Genome Data 001	Org B Doctor	00aa11bb22cc...

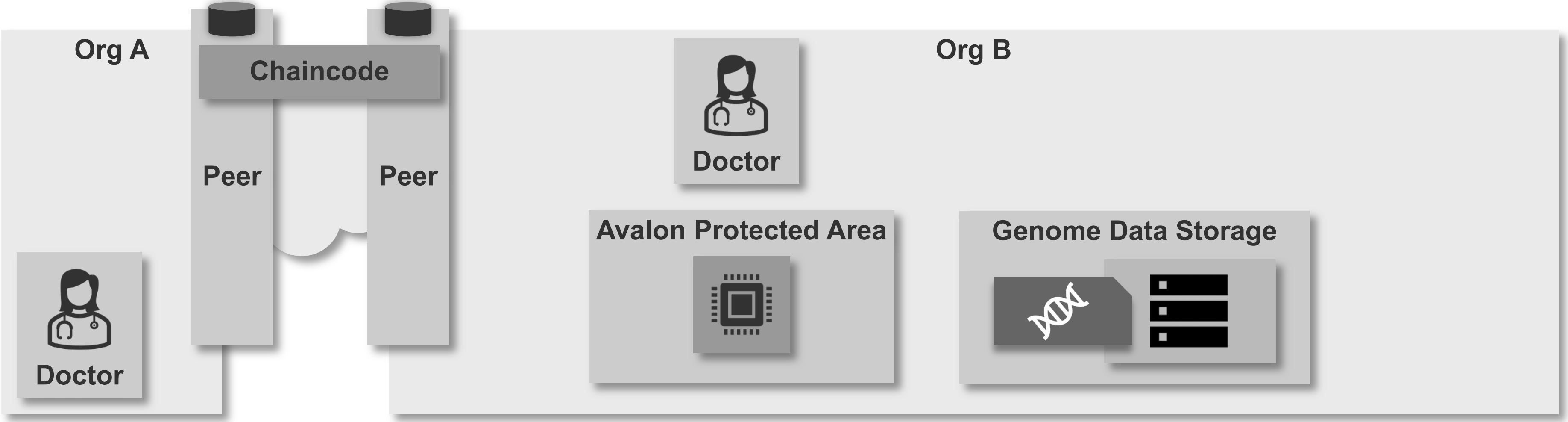
Should be encrypted
(Information about who requested access should be kept confidential)

State DB: Access Management

Data name	Access Request	Access Approval
Genome Data 001	Org A	Org A

State DB: Analyze Task Management (Avalon)

Data name	Requester	Task	Result
Genome Data 001	Org A	xxx	yyy



Work in Progress

We are trying to use Hyperledger Fabric Private Chaincode!

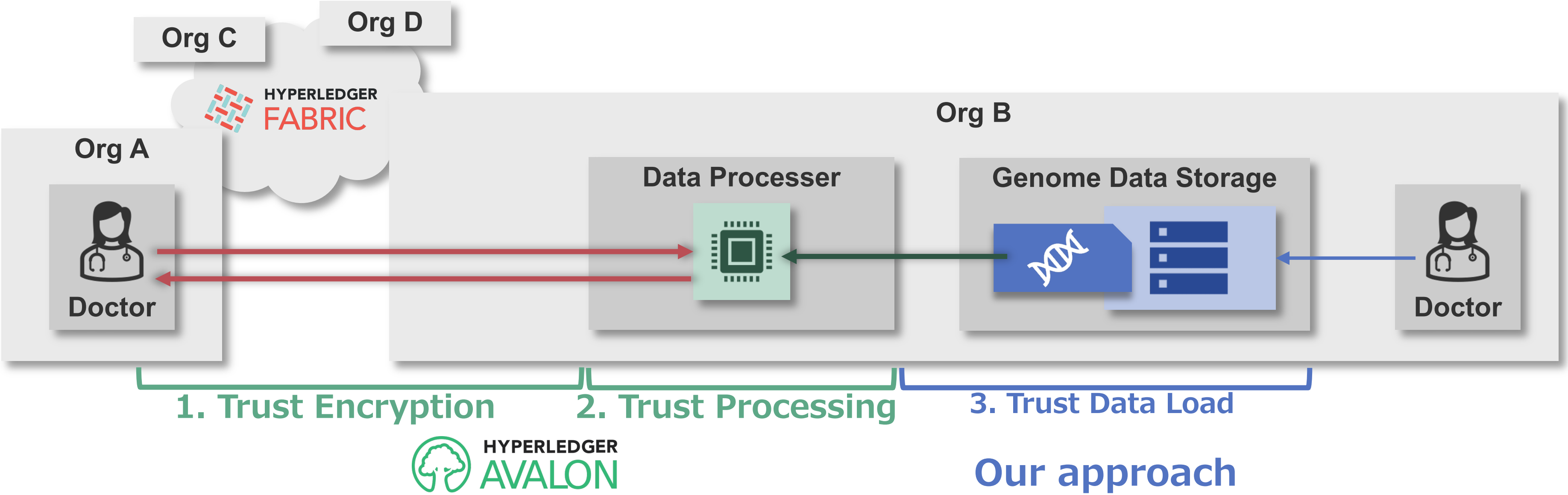
- Hyperledger Fabric Private Chaincode (FPC) enables the execution of chaincodes using Trusted Execution Environment
- **The combination of Avalon and Fabric Private Chaincode can make both On-chain and Off-chain trustworthy**
- We have started
  - try to use FPC
  - contact FPC community
  - contribute to FPC

Contents

1. Introduction
2. Design and Approach
3. Work in Progress
4. **Summary**

Summary

- We introduced one of implementation to realize a trusted infrastructure for sharing & utilizing sensitive data
- With Avalon and our approach, we have made the following three points into a trust
- We are trying to use Hyperledger Fabric Private Chaincode for make both On-chain and Off-chain more trustworthy



HITACHI

Inspire the Next

Hyperledger Global Forum 2021

Virtual 2 / ● Business

Trust Data Sharing and Utilization Infrastructure for Sensitive Data using Hyperledger Avalon

Thursday, June 10th, 2021

Hitachi, Ltd., Research and Development Group

Koshi Ikegawa, and Nao Nishijima