FRANKFURT UNIVERSITY OF APPLIED SCIENCES

Blockchain Solution to Healthcare Record System using Hyperledger Fabric

Final Presentation

Jathin Sreenivas, Kshitj Yelpale, Varsha Vasudev Kamath

Agenda

Introduction

Background

- Specialization in the health care services and patient's mobility.
- Patient's medical history can help healthcare providers make precise diagnosis and treatment.
- Ensuring data integrity, confidentiality and privacy of patients while sharing the clinical data.

Introduction

Existing Systems

- Electronic Health Record (EHR) is used to share patient's medical records across different health care providers.
- EHR consists of medical information of the patient in the form of Electronic Medical Record (EMR).
- EMR contains a patient's medical diagnoses, allergies, history, treatment, and laboratory reports.
- Healthcare IT standards are Health Level 7 (HL7), Fast Healthcare Interoperability Resources (FHIR).
- The other models used by health care providers are push, pull, and view.

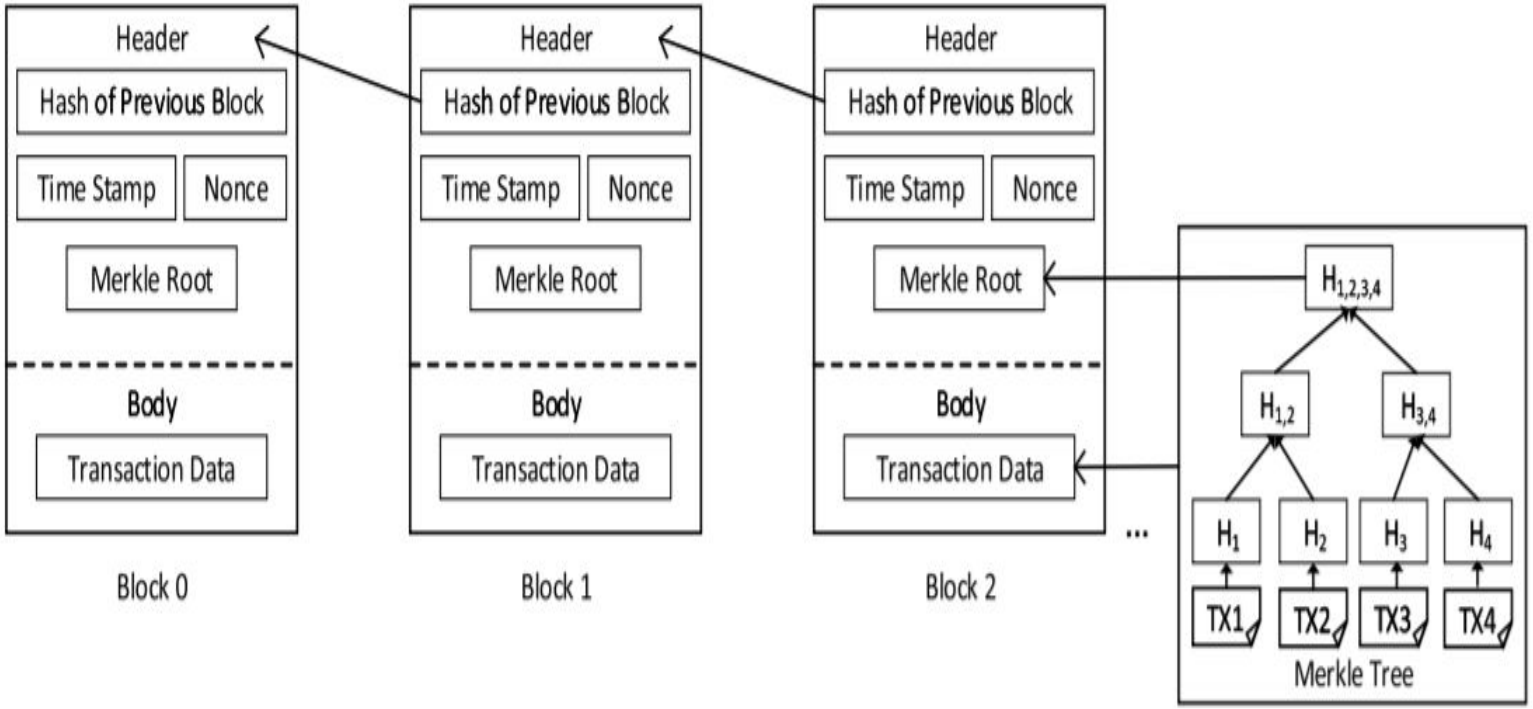
Introduction

Motivation

- Medical data storing and sharing is an integral part in healthcare systems.
- Sharing personal data among various participants through unsecure means can lead to leakage of critical information
- The lack of the a client control over their personal information leads to harmful consequences such as unauthorized identities can access/edit the personal medical details.
- The critical issues in the electronic health/medical records (EHR/EMR) is maintaining the interoperability among various involved identites.
- Data security and privacy are also challenges in the current ways of data storing and sharing data through EHR/EMR systems.

State of the art

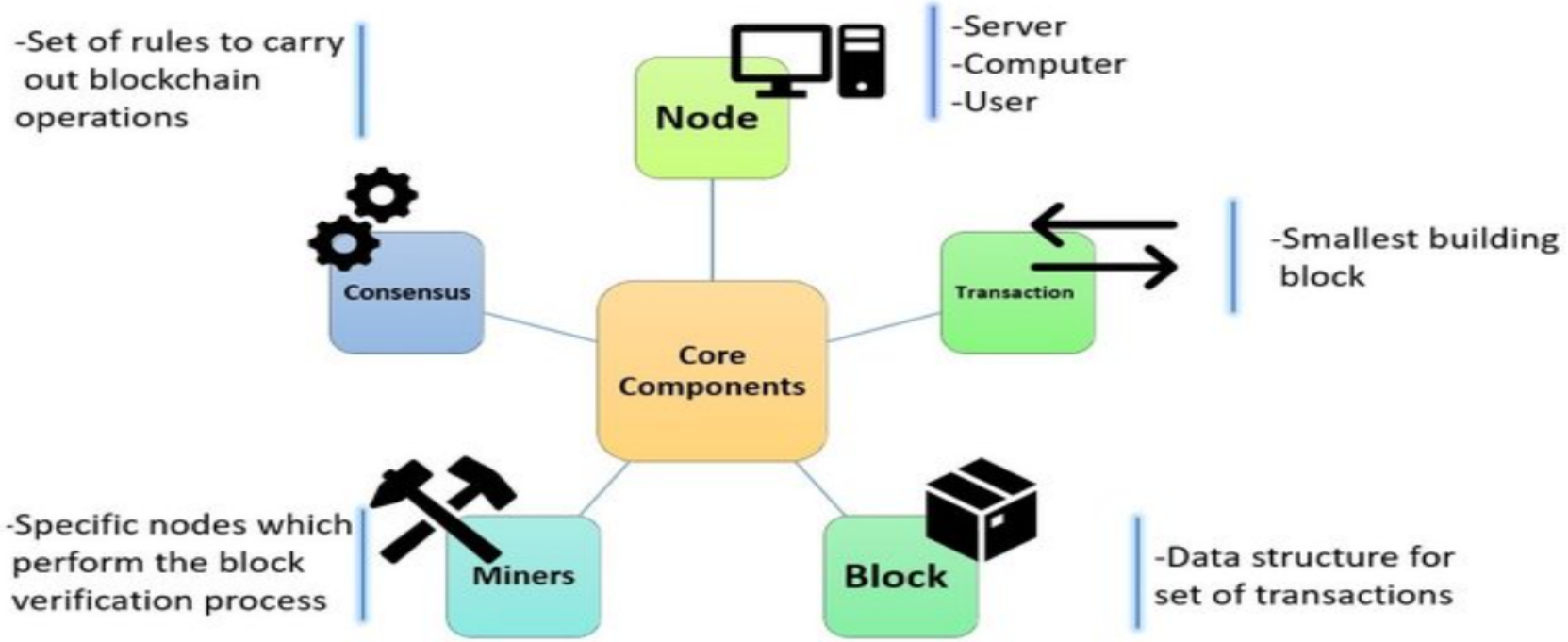
What is blockchain?



Block Structure [6]

State of the art

What is blockchain?



Blockchain core components [7]

State of the art

Types of blockchain

Public Blockchain (Permissionless)

- Everyone can access the public blockchain and participate in the transactions.
- Fully decentralized.
- Examples are Bitcoin, Litecoin, and Ethereum.

Private Blockchain (Permissioned)

- Restrictions on who can join the network and who can participate in the transactions.
- Used by organizations or companies for its internal usage.
- Centralized.
- Example, Hyperledger Fabric.

The Solution

Scenario

- Map fabric components to EHR systems.
- Organizations in fabric mapped to hospitals
- Hospitals of same interest connected on same channel. New hospitals will be connected once approved by channel configuration owner hospitals.
- Assets in fabric are patient data accessible all over the network.
- Store all data in blockchain database
- Doctor should see history of a patient to understand condition and prescribe proper medication
- Patient should be responsible to make his data available to doctor.

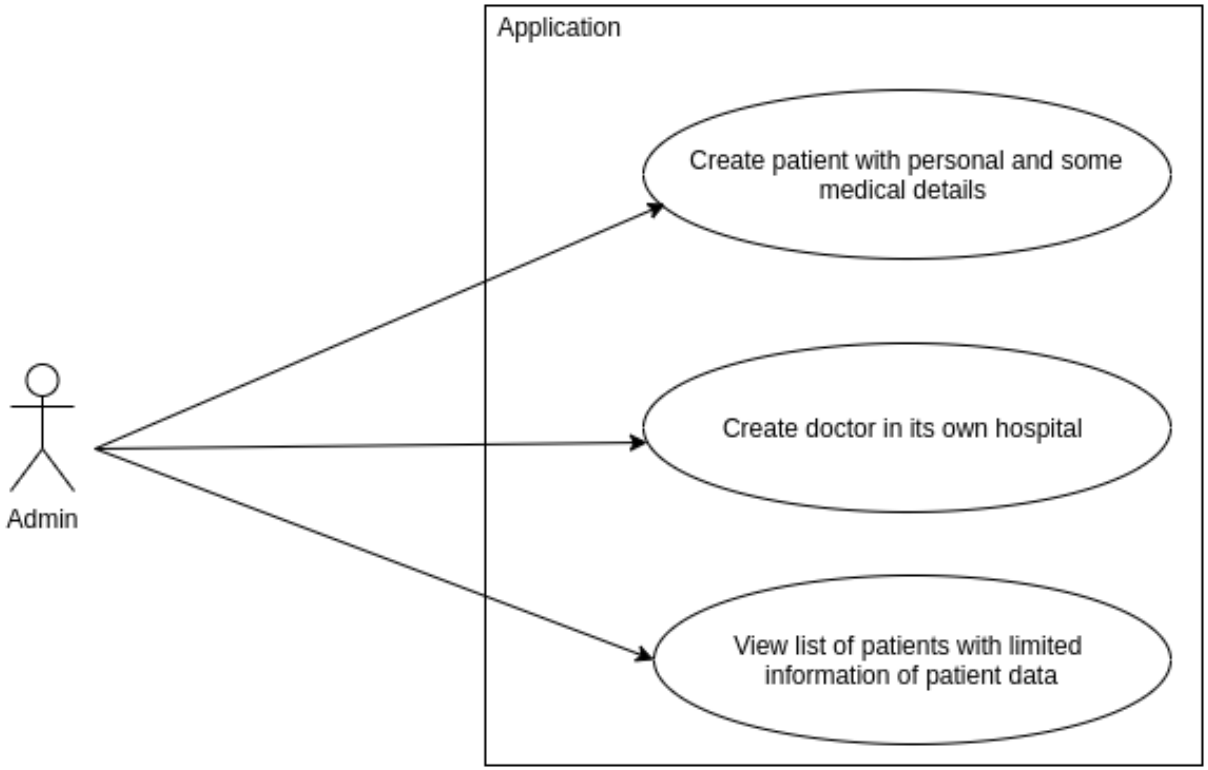
The Solution

Why blockchain and fabric?

- Blockchain stores data cryptographically secure
- Authentication and authorization - fabric provides CA and MSP components which provide secure indetities like private key and certificates and validation done when make connection to network.
- Confidentiality - fabric is a permisionned blockchain framework.
- Availability - distributed nature of blockchain makes data available to all permissioned systems.
- Data integrity - blockchain records are immutable
- pBFT consensus algorithm
- Fabric provides history API which helps doctors to analyse a patient's history.
- Scalablity - New organization, peers and users with different roles.
- Pluggable modules

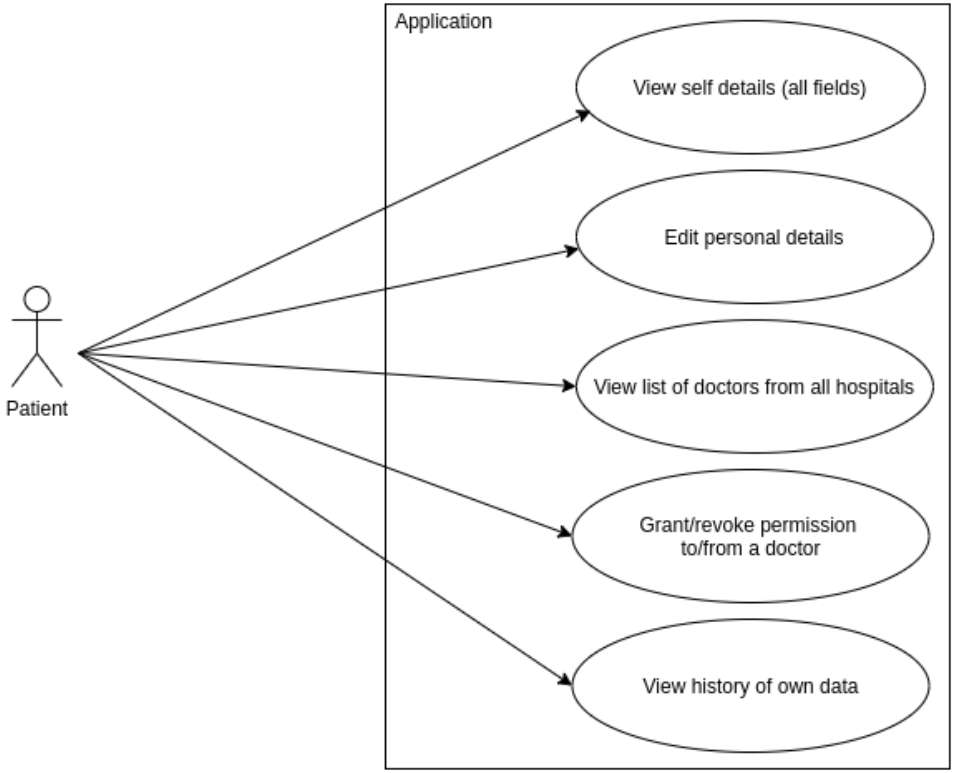
The Solution

Use cases



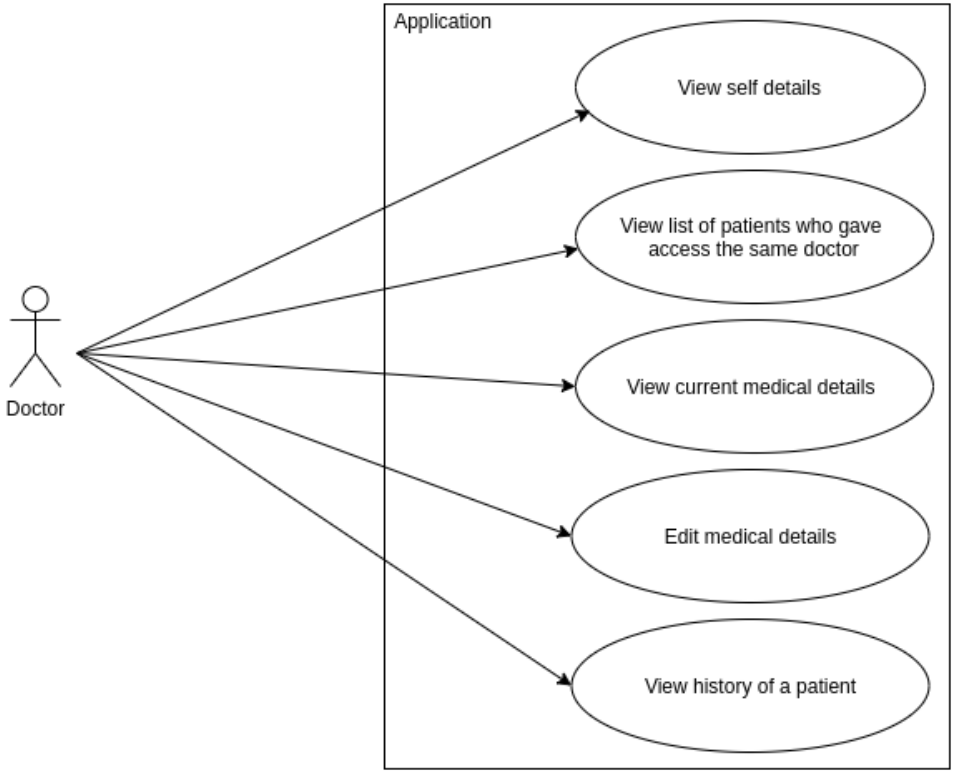
The Solution

Use cases



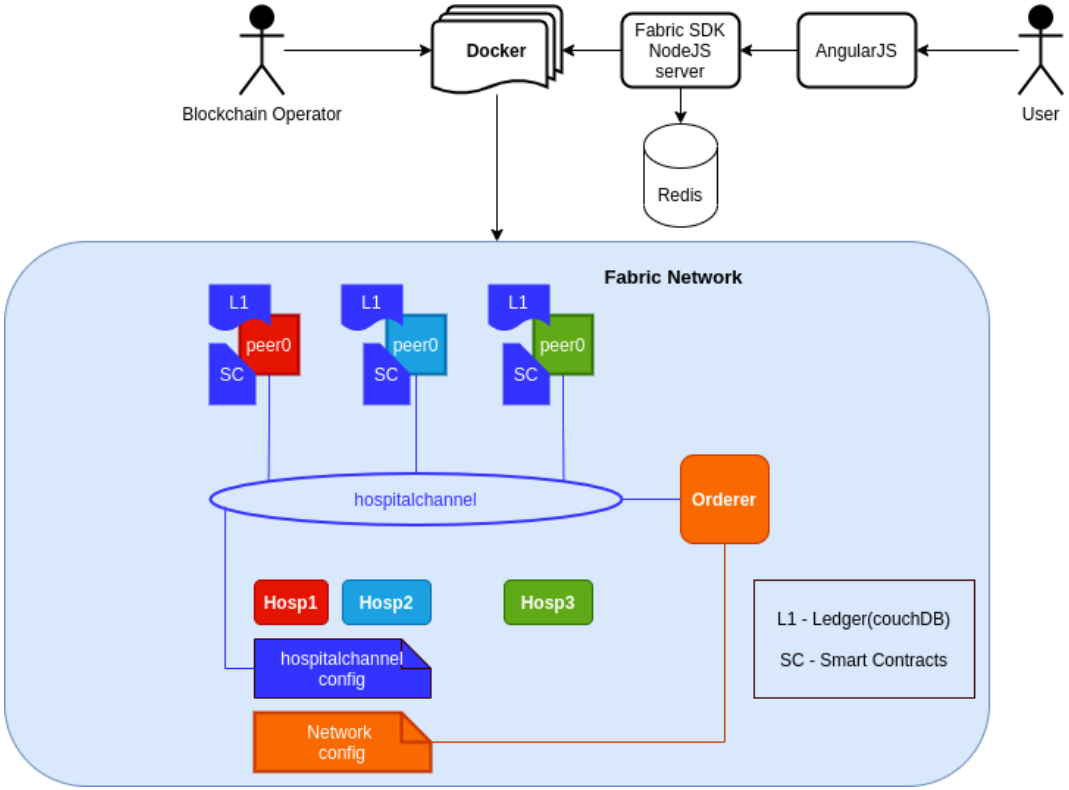
The Solution

Use cases



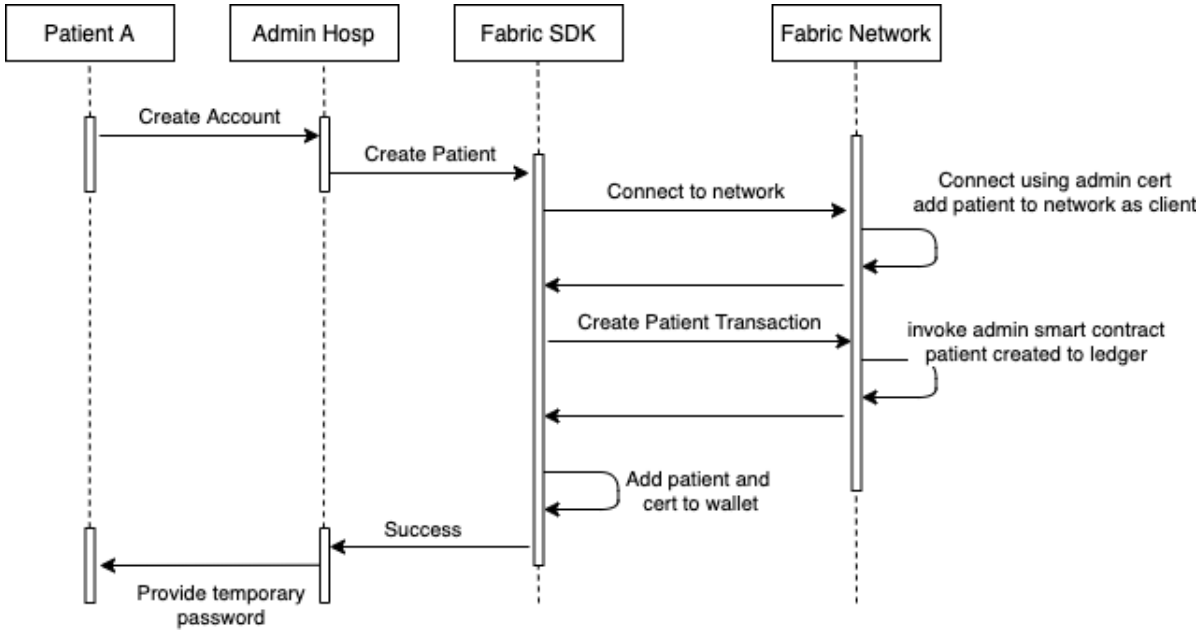
The Solution

Architecture



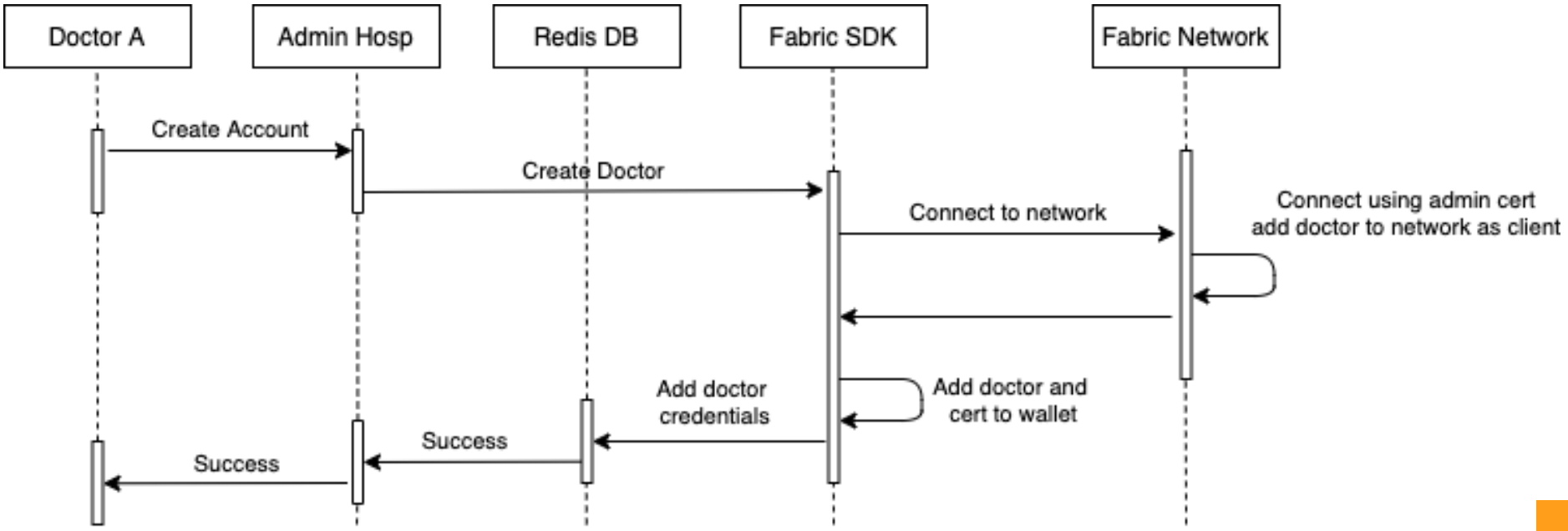
The Solution

Activity diagram - Create Patient



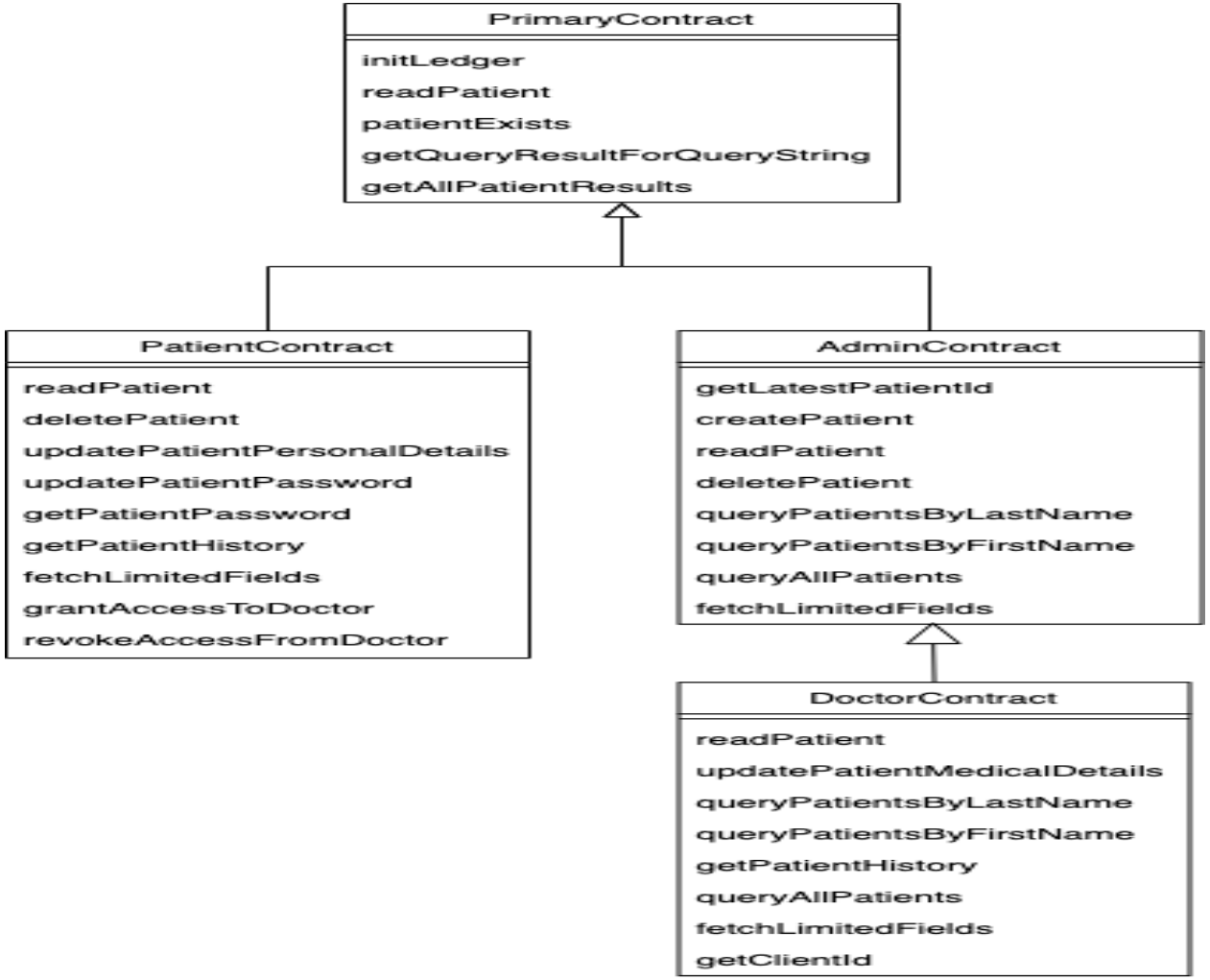
The Solution

Activity diagram - Create Doctor



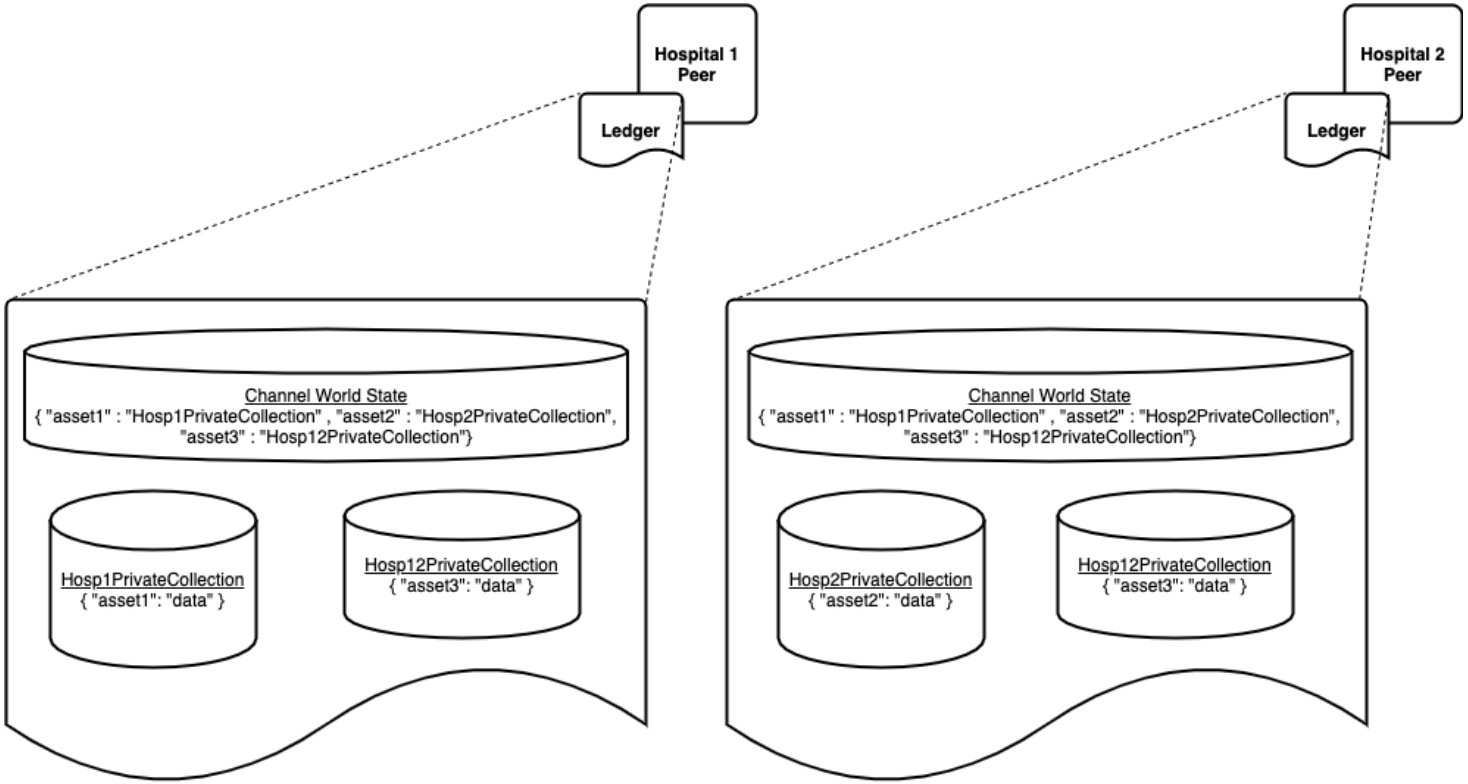
The Solution

Class diagram - Smart Contract



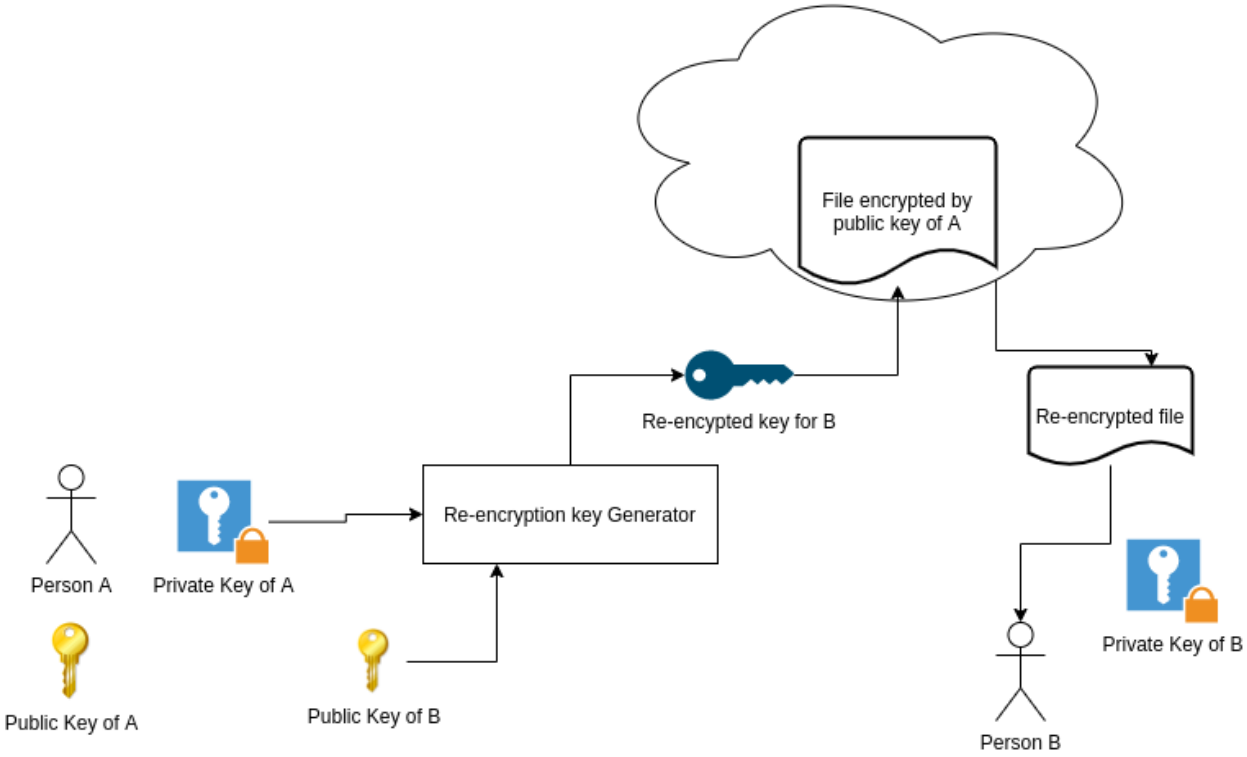
Security Mechanisms

Private Collections



Security Mechanisms

Data re-encryption



Security Mechanisms

Data re-encryption

```
1   {
2   "patientId": "p1",
3   "password": hash(pwd),
4   "pwdTemp": true
5   "firstName": "abc",
6   "lastName" "xyz",
7   "data": encrypted patient data using symmetric
       key,
8   "changedBy": "doctorId XX",
9   "permissionGranted": [doctorId1: re-encrypted
       key for doctor 1,doctorId2: re-encrypted key
        for doctor 2,...],
10  "encryptedSymmetricKey" :"######"
11  }
```

Demo

Results

Pros and Cons of using hyperledger Fabric

Pros

- Fabric architecture allows to add plugins for the identity management and consensus algorithm.
- Confidentiality and security of data can be achieved through MSP.
- Performance is optimized, since mining is not required.
- Creation of a private channel for only a few participants among a large blockchain network.

Cons

- The architecture of hyperledger fabric is quite complex.
- It is not a network fault tolerant.
- Limited database support.

Results

Issues in hyperledger

- getHistoryForKey - Private Data Collection. [5]
- Create a user defined role instead of client. [4]
- Access user attributes using client

Results

Challenges in developing application

- Implementing security mechanism
- Re-encryption - Nodejs lacks a decent re-encryption library, need to implement own library
- Tracking of public key of created user through fabric SDK
- Scaling of peers

Conclusion

- Hyperledger fabric is a promissing blockchain framework comes with policies, smart contracts and provision of secure identities.
- Enable the EHR scenario interoperable among multiple hospital organizartions
- A promissing framework for private and closed blockchain scenarios
- Provide reliable and secure solution in managing medical field records

Conclusion

Future Work

- Overcome security challenges
- Improve source code to make to provide scalable and pluggable solution in terms of increasing hospitals and peers
- Implement powerful ordering service on large scaling of fabric network
- Updation of consortium policies
- Wallet can be stored in distributed way with database storage machanism
- Bring REST network calls under HTTPS to make data transformation secure using TLS
- Integration of email functionality for temporary password of users
- Implement functionality of patients
- Kubernetes - best tool to deploy and manage production grade application

References

- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7010942/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7474412/
- https://www.sciencedirect.com/science/article/pii/S2214212-619306155
- https://jira.hyperledger.org/browse/FABC-548, Accessed-On:28/03/2020
- https://jira.hyperledger.org/browse/FAB-5094, Accessed-On:28/03/2020
- Dynamic Spectrum Management, Signals and Communication by Ying-Chang Liang
- https://www.mdpi.com/1099-4300/22/2/175