Blockchain based Healthcare system Using Off-Chain Storage

Mentor :

Dr. Yamuna Prasad Shukla
Dr. Mauro Conti (External)
Dr. Chaggan Doot (External)

Members:

Aman Pawar • 2016UCS0016
Rahul Nirania • 2016UCS0015

Overview

Current Health record system: Status and problems

Intro to blockchain

Why Hyperledger

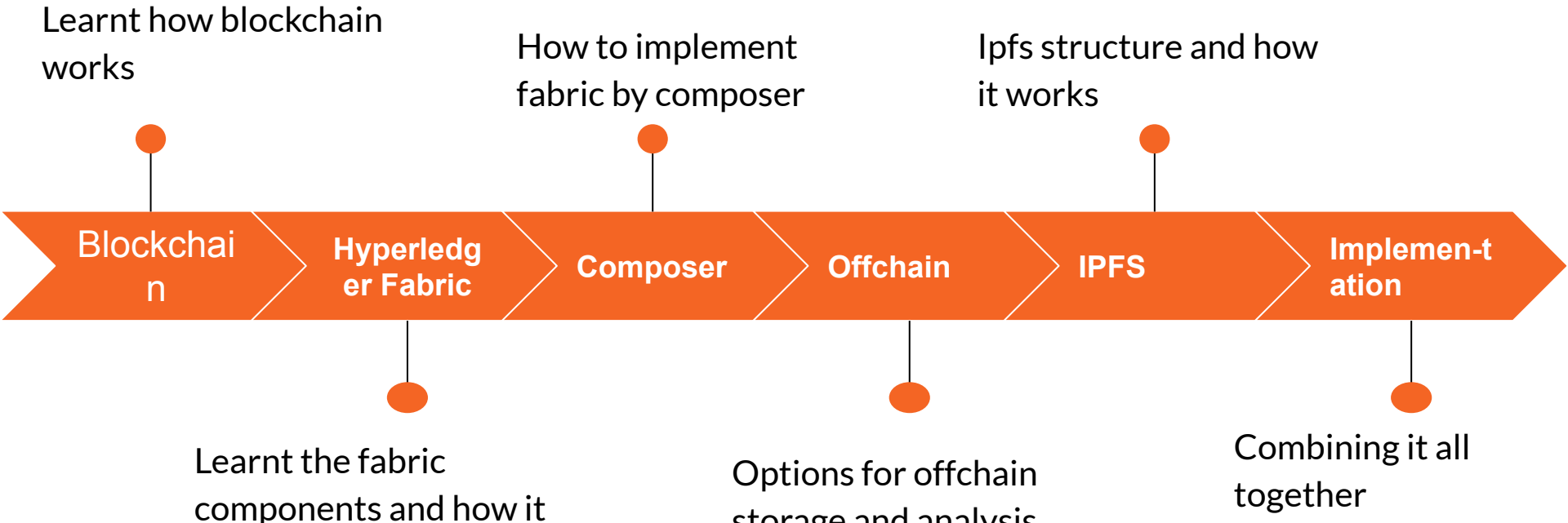
Off-Chain Storage and its need

Why IPFS

Implementation of Blockchain and adding Off-Chain Storage

Future Works

Workflow


Learnt how blockchain works
How to implement fabric by composer
Ipfs structure and how it works
Blockchai n
Hyperledg er Fabric
Composer
Offchain
IPFS
Implemen-t ation
Learnt the fabric components and how it works
Options for offchain storage and analysis
Combining it all together

Healthcare recording System

- It means recording of medical data such as prescription, medical history, bills, medical images, lab reports etc.
- Its a data intensive system in which large-scale data is generated, disseminated, stored, and accessed daily.
- Data created when a patient is monitored or undergoes some tests, need to be stored in order to be accessible at a later time by a healthcare provider **within the same or even a different network or context**.

Healthcare recording System

- As the sharing of data to different network grows the concerns about secure and efficient transmission of the medical data increase.
- It helps insurance company to know the medical history of the person so that he can be provided with the insurance.

Current status

- Currently most of the medical data resides on a hard copy in india especially the images(like x-ray, sonography etc) and reports of different test.
- Some good hospitals manage the data on their systems but it is centralised as it never got shared digitally with other hospitals even if the patient wants to.

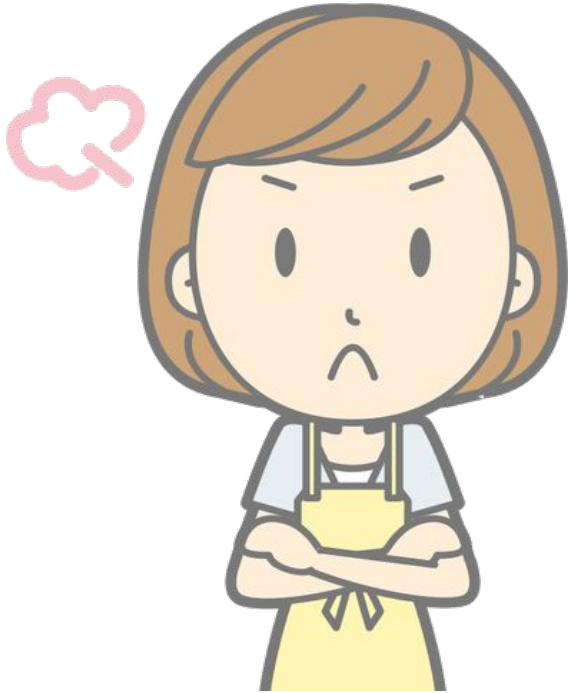
concerns

- The first and main concern is this digital access is also far away from patient access.
- Second is security as if any hospital has our data do we know is it safe? And what if they shares it with others? We can’t control the access.
- The third is legitimately and temper proof i.e. if the data haven’t been tampered.
- And also what if the server crashes or server go down no other option to gather data.

The solution

- A **decentralised system** in which every patient has access to their data easily
- Patient can share their data **securely** with other hospitals or doctors.
- Patient can **control** who can **access** his data and if he want he can give or remove anyone access.
- And the most important once the data is recorded it should not be tampered , it means data should be **immutable**.

So what it should be?



Blockchain

Seems to be a good option

Introduction to blockchain

- A blockchain comprises a set of nodes without a preexisting trust relationship and connected through a peer-to-peer topology.
- Each node hosts the same copy of a blockchain creating a **decentralized structure**.
- It uses different **consensus** mechanism so that nodes can mutually agree on the legitimacy of the next valid block in the chain to be added.

Introduction to blockchain(Cont.)

- A blockchain is an append-only distributed ledger i.e. **Immutable**.(In contrast with a traditional relational database)
- Additionally it also consist of **provenence** which refers to awareness that participants know where the asset was originated from and its ownership history.
- Also it also consist of finality which refers to the status of a transaction as complete.

Types of blockchain

- Permissionless blockchain

- Permissioned blockchain

Permissionless Blockchain

- In a permissionless blockchain, any node can join the network.
- Useful in a network can ‘commoditize’ trust, where the identity of the facilitating parties does not need to be verified.
- Examples of a permissionless blockchain is Bitcoin or Ethereum.

Permissioned Blockchain

- In a permissioned (private) blockchain, pre-verification of the participating parties, which are all known to each other, is required.
- Useful when it is vital that the blockchain participants require permission to execute transactions.
- Example of these type of blockchain is Hyperledger.

Why Hyperledger ?

- Our aim is healthcare recording system.
- It consist of many critical data and need to be secure.
- Only known people either to any hospital or clinic should be allowed to participate in the network.
- For this concern it makes sense to have the participants vetted.

For All the above reason we picked Hyperledger i.e. best option for permissioned blockchain.

Hyperledger

Hyperledger

- Hyperledger is an umbrella of open source projects and tools which is managed by Linux foundation which started in December 2015.
- **Hyperledger fabric** is a ‘permissioned’ blockchain platform or an infrastructure for running smart contracts.
- **Hyperledger composer** is a tool which create and deploy business network applications (ie. smart contracts) over Hyperledger network using high level composer language.

Hyperledger fabric

Components and how it work

Hyperledger fabric

- Hyperledger Fabric is a permissioned blockchain framework, with a modular architecture (plug-and-play).
- It leverages container technology to host smart contract (Chaincode) which contains application logic.

Components (Major)

- **Membership Service Provider(MSP)**: Defines the rules in which, identities are validated, authenticated, and allowed access to a network.

- **Client**: Applications that act on behalf of a person to propose transactions on the network using a Fabric SDK in order to communicate with the network.

Components (Major)

- **Peers:** A node that commits transactions and maintains the state and a copy of the ledger.Besides, peers can have a special endorser role. Its types are endorsing, committing, anchor and leading.

- **Orderer**: Validly order the transaction to update world state. Fabric uses SOLO, Kafka, and Simplified Byzantine Fault Tolerance (SBFT).

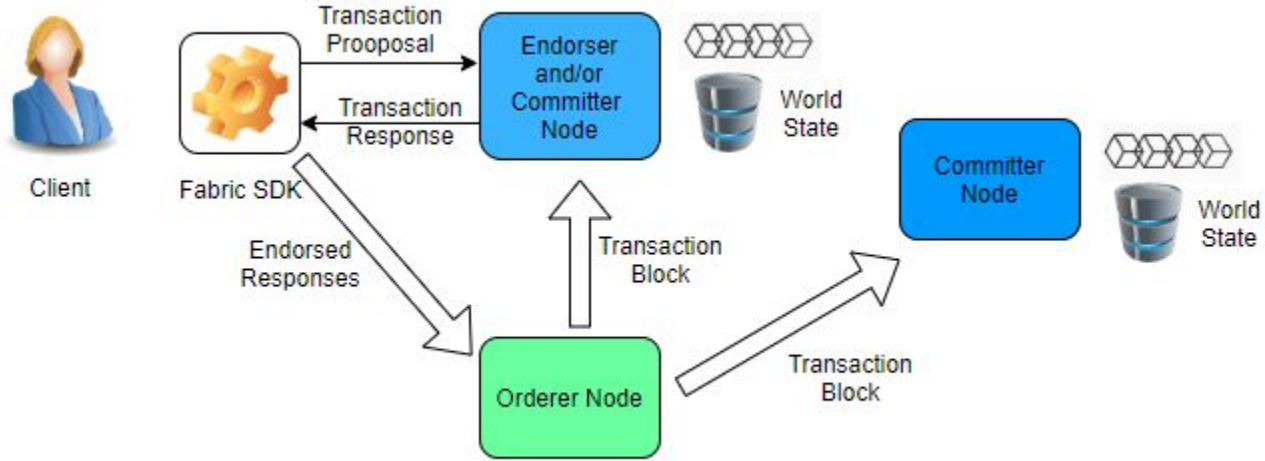
Components (Minor but Important)

- **Channels:** Partition the network in order to allow transaction visibility for selected orgs/members only.
- **Identity:** Each actors in a network peer, orderer, client, admin have some digital identity in the form of certificate
- **Policies:** Its a function which accepts as input a set of signed data and evaluates successfully or returns an error because some aspect of the signed data did not satisfy the policy.

Components (Minor but Important)

- **Ledgers:** It is a current state of the business as a journal of transaction. A ledger consists of two different parts, a **world state,** and a **blockchain**.
- **Endorsement:** This is the list of signed transaction responses from each required organization sufficient to satisfy the endorsement policy.
- **Chaincode:** It is a technical container of a group of related smart contracts for installation and instantiation. Every chaincode has endorsement policy attached to it.

Transaction Flow



Why we want composer?

As making each of the component separately is a very hectic so the tool “**Hyperledger Composer**” was developed which incredibly reduces the effort to make and deploy the blockchain network. It reduces the work of months to mere some weeks.

Hyperledger Composer

Architecture and how it work

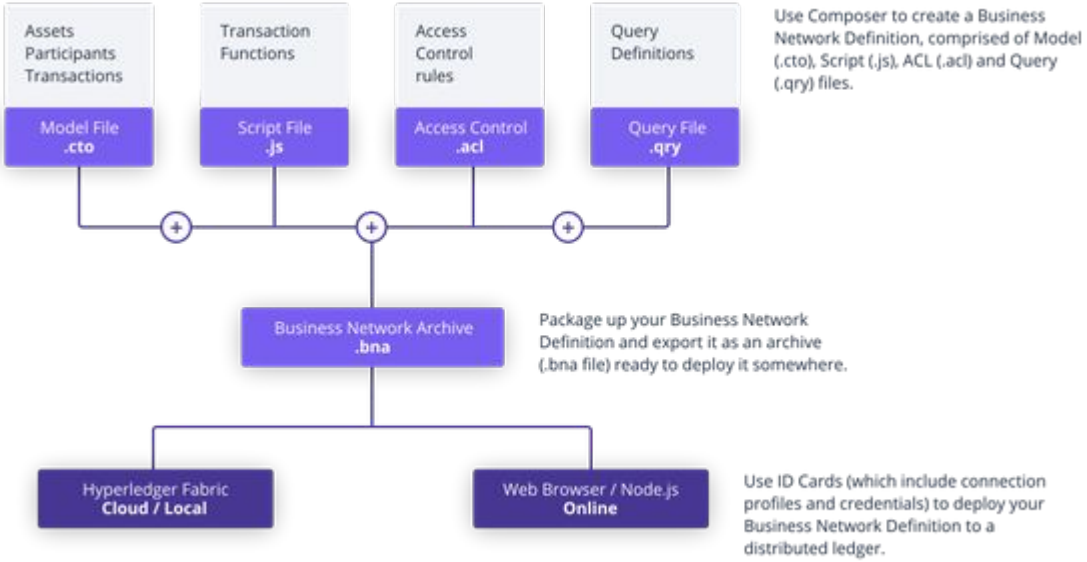
Hyperledger Composer

- Hyperledger Composer is a set of tools that allows a way to create blockchain applications and smart contracts aimed at solving business problems and/or improving operational efficiencies.
- Hyperledger Composer simplifies application development on top of the Hyperledger Fabric blockchain infrastructure.
- Hyperledger composer is written in javascript

Component files

- Model — The file that defines all the system objects and transactions. All the network participants, assets and transactions are included.
- Scripts — The behavior for the defined transactions, whenever they are called.
- Queries — A file with defined queries for retrieving information out of the system.
- Access Control — A set of rules that will help define who can access the information, and what type of access they have.

Architecture



Looking at Healthcare data

- Prescription data
- Medical History
- Apointment data

} Just texts so can be stored in blockchain's onchain storage

- Medical Images (X-Ray, Sonography etc.)
- Medical report (Like blood report, malaria report etc.)

} Each may be of many MBs so can't be stored onchain. So we need an offchain storage solution.

Offchain Storage

Options

What are the options

- IPFS
- StorJ
- Swarm
- Filecoin
- Siacoin
- Etc...

}

We will discuss only these as they are the best among all the opstions

InterPlanetary File System (IPFS)

- The InterPlanetary File System (IPFS) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system.
- IPFS uses content-addressing to uniquely identify each file in a global namespace connecting all computing devices.
- Decentralised storage of large files for faster access.

IPFS- Pros

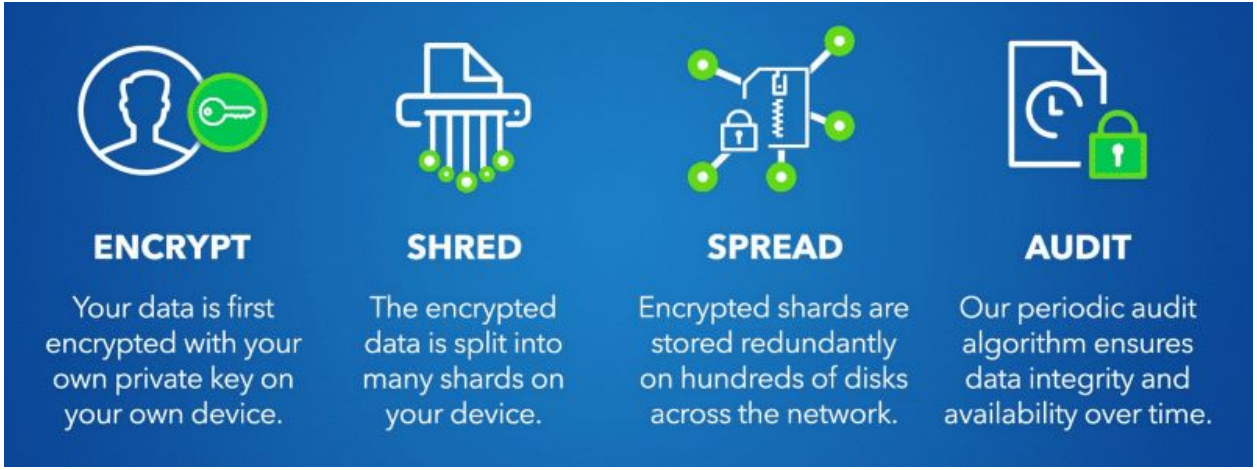
- Ease of access.
- Since multiple nodes have the same data even if some nodes are down, still the files are accessible.
- Files are content addressed rather than location addressed.
- No need of high bandwidth as data is served from multiple nodes and not a single server

IPFS- Cons

- Security and access control concerns means anyone having access to the file's hash can access the file.
- Secondly the authorship protection means a person can get a file from ipfs and change it a bit and upload with a different name causing plagiarism

StorJ

- Storj is an open source, decentralized file storage solution.
- It uses encryption, file sharding, and a blockchain-based hash table to store files on a peer-to-peer network.



StorJ- Pros

- Encryption
- Redundancy solution using parity shards
- Erasure coding rules for too much redundancy.
- Regular Audits and verification in the network to ensure that no data is lost.

StorJ- Cons

- Not developed for File sharing.

Swarm

- Swarm is censorship resistant, permissionless, decentralised storage and communication infrastructure.Swarm is also said to be BitTorrent on Steroids.

Swarm- Pros

- Provides schemes that make storers individually accountable for particular content.
- Incentives for Long term storage of various content.

Swarm- Cons

- Less Popular and content can get deleted as there is no storage insurance currently, Does not provide easy editing capabilities.

So what should we choose

We want it to be used with hyperledger composer so we can’t use swarm and since we have to share the file and it is one of the most important use case so we can’t use StorJ. So now we left with the best among all these **IPFS.**

IPFS- How it works

- It works by connecting all devices on the network to the same file structure.
- This file structure is a Merkle DAG.
- It combines Merkle trees and Directed Acyclic Graph. Think of it as a large BitTorrent swarm.
- Identifying a data object (like a Merkle DAG node) by the value of its hash is referred to as content addressing. Thus, we name the node identifier as Content Identifier, or CID.

IPFS- How it works

- It uses Distributed hash table (or DHT) to locate the file in the network
- This table is also distributed in the network and it contains key value pair
- IPFS uses a piece of software called Kademlia to learn which nodes have what data. This is called providing.

Implementation

Participant

- Doctor
- Insurer
- Patient

Concept

- Insurance
- Medical Record

Transaction

- CreateMedicalRecord
- CreateInsurance

The Implementation

https://drive.google.com/file/d/1QQm1VeHt2Kv98bNC_UNM0JqnbYl6Ue80/view?usp=sharing

Goals for future

1. We can expand the use cases of the blockchain network
2. We can make angular apps for each client in the orgs
3. Make our own offchain storage system
4. Checking the performance by choosing different offchain storage and by some tweeking in Blockchain network

Thank You

Any Question?????