COURSE NAME OPEN SOURCE TECHNOLOGY

Project Name : MEDICAL VAULT

GROUP MEMBERS:

AYUSH KUMAR	**2017UCO1586**
VIPIN YADAV	**2017UCO1581**
HIMANSHU	**2017UCO1588**

Introduction

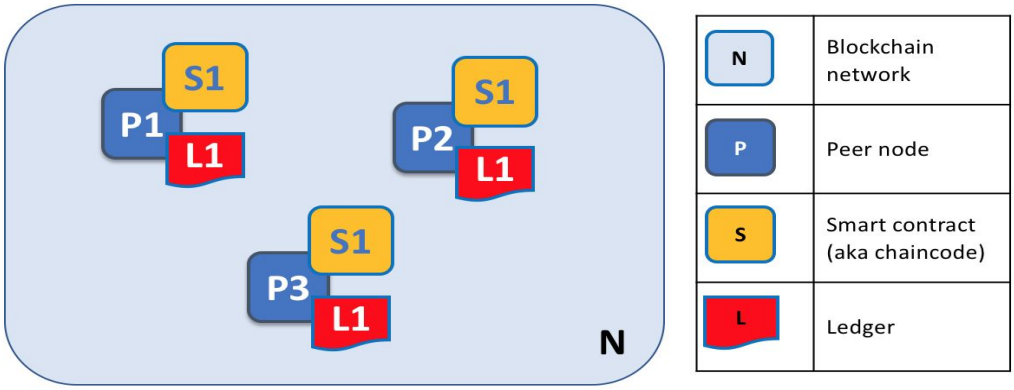
Medical Vault is an application which stores a patient's medical history in a distributed and cryptographically secure manner. It is built on the concepts of blockchain in which a distributed immutable ledger is maintained among the nodes present in the network with no central authority to manipulate the data.

Here, the nodes consist of different trusted hospitals and clinics around the world.The permissed nature of this network only brings trusted hospitals in the network guaranteeing the correctness of medical records of the patients.

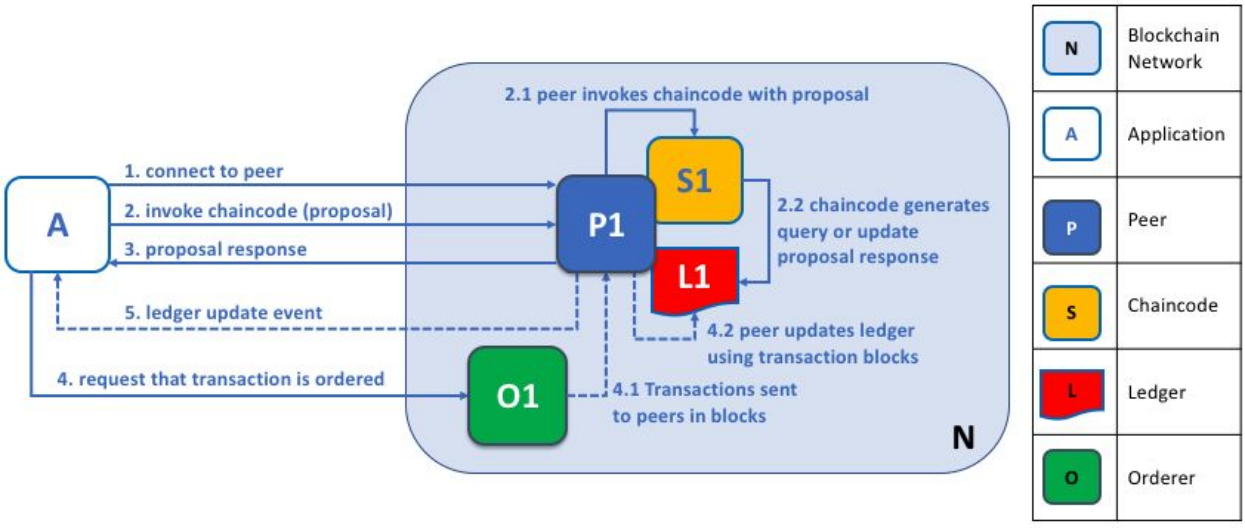
Data is always prone to getting corrupted, manipulated or lost. Since medical history of patients is among the most valuable assets to them, hence we need to store this precious data in a way that this data is always accessible without having a risk of it getting lost/manipulated.

The hospital does not rely on the medical history provided by patients for their treatment. Through MedicalVault, they can easily retrieve a patient's reliable medical history with an easy go. The hospitals can also add medical reports and diagnosis. If a patient is new to the network, then the hospitals can also register them to the network.

BLOCKCHAIN NETWORK



These components are typically peer nodes(hospitals in the network), orderer nodes(order the transaction into the block) and applications and, by joining a channel(network), they agree to collaborate to collectively share and manage identical copies of the ledger associated with that channel. Conceptually, you can think of channels as being similar to groups of friends (though the members of a channel certainly don't need to be friends!).



Web3 - APIs enable applications to connect to peers(hospitals), invoke chaincodes(smart contract) to generate transactions, submit transactions to the network that will get ordered, validated and committed to the distributed ledger, and receive events when this process is complete.Through a peer connection, applications can execute chaincodes (smart contract) to query or update a ledger. The result of a ledger query transaction is returned immediately, whereas ledger updates involve a more complex interaction between applications, peers and orderers.

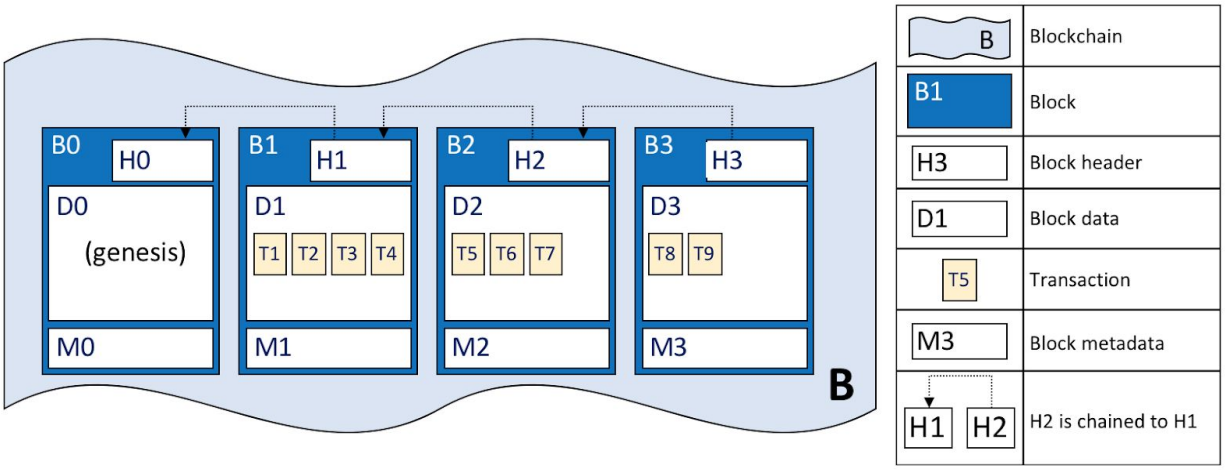
SMART CONTRACT (chaincode)

A smart contract defines the rules between different organizations in executable code. Applications invoke a smart contract to generate transactions that are recorded on the ledger.

MEMBERSHIP PROVIDER

If a hospital requests for a membership in the blockchain network of hospitals, then it needs to provide its details like hospital's name, its license number etc. After submitting the request, a voting is held among the members of the network for the proposal of adding the new member. If the requesting hospital organization is endorsed with more than 50% votes, then it is accepted as a new member in the network. The new member gets all the privileges of the network as others do.

LEDGER

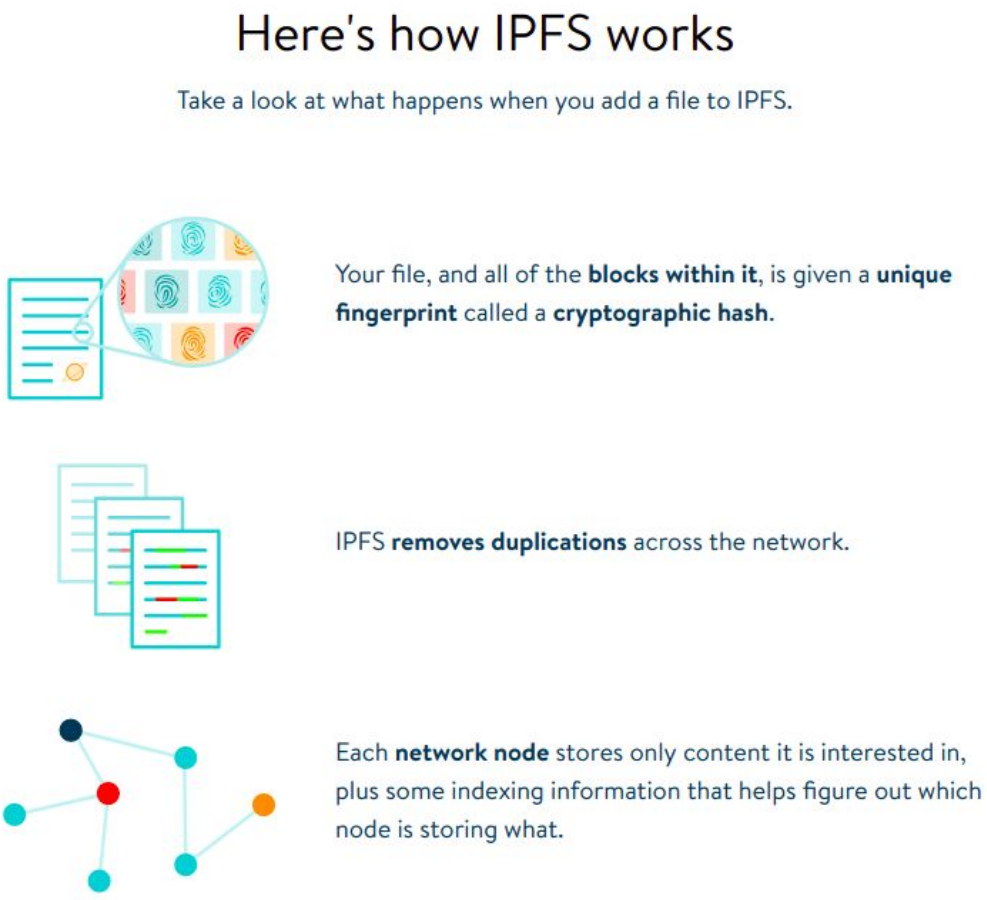


Each block's header includes a hash of the block's transactions, as well a hash of the prior block's header. In this way, all transactions on the ledger are sequenced and cryptographically linked together. This hashing and linking makes the ledger data very secure. Even if one node hosting the ledger was tampered with, it would not be able to convince all the other nodes that it has the 'correct' blockchain because the ledger is distributed throughout a network of independent nodes.

Block B2 has a **block header** H2, which contains a cryptographic **hash** of all the transactions in D2 as well as a hash of H1. In this way, blocks are inextricably and immutably linked to each other, which the term **blockchain** so neatly captures!

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 (way to store information so it can be retrieved based on its content, not its location) to uniquely identify each file in a global namespace connecting all computing devices



When you **look up a file** to view or download, you're asking the network to find the nodes that are storing the content behind that file's hash.

You don't need to remember the hash, though — every file can be found by **human-readable names** using a decentralized naming system called **IPNS**.