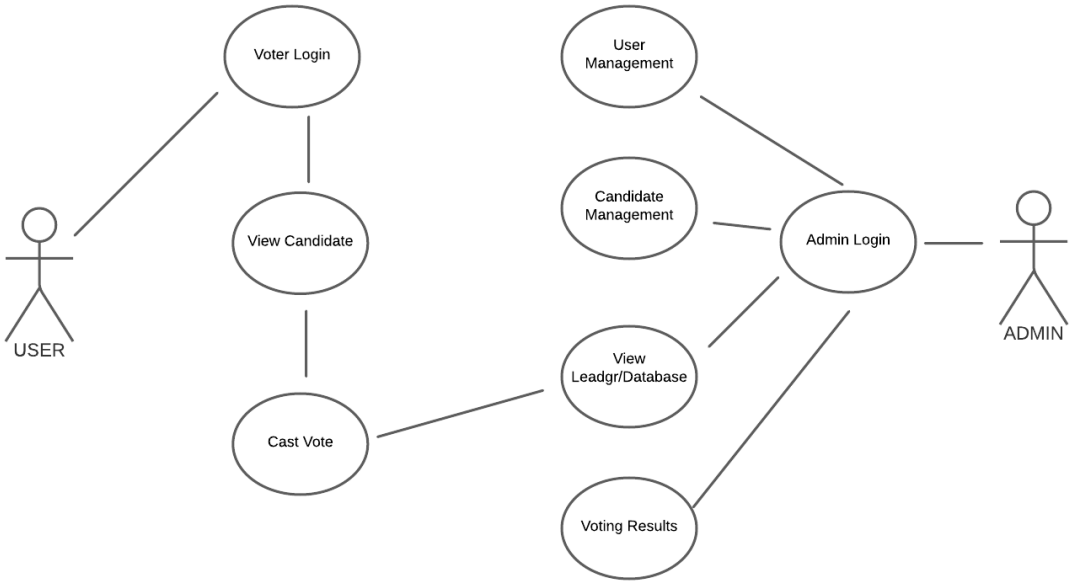
CSL7090 Assignment 1

Solution 1:

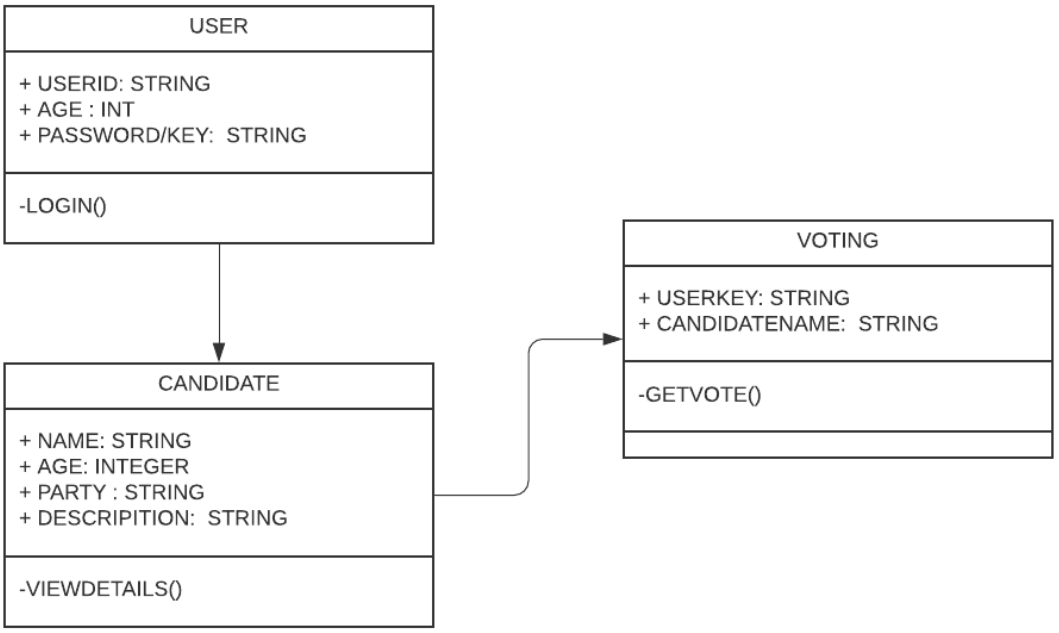
The blockchain-based application that was selected is based on an Electronic Decentralized Voting system using blockchain as a backend and HTML, CSS, etc. on the frontend. There are many applications available for this purpose like Follow My Vote, Voatz which use public blockchain and private blockchain respectively. For this assignment, a general application is considered that provides the user a way for voting in any type of election, based on blockchain technology.
Any blockchain-based application is decentralized, peer-to-peer, distributed that is free from a central server and the data is stored in the form of transactions and after the miners (users) mines them, and then after a valid consensus, they are added to the chain.
The basic working of this application can be understood by following the given below use case diagram.



4 + 1 Views of Two Scenario/use cases of the application

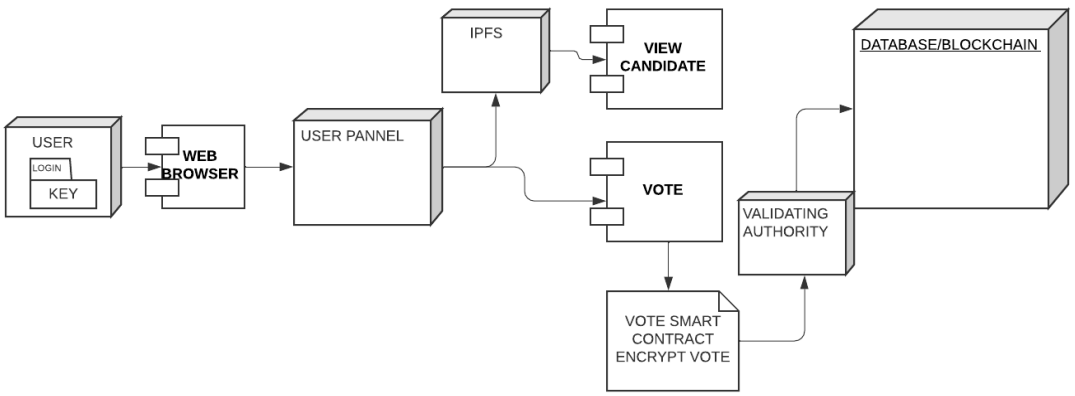
Use case/Scenario 1: Cast Vote - In this use case the user logs into the system with an authentic user id and password and after viewing the details of the candidates who are participating in the election can cast his/her vote for the appropriate candidate he/she has selected.
The four views are:-

Logical View: Describes the system of smart contracts used in this application. There is only one smart contract election that is used in the system which is written in solidity language (used for writing the smart contracts). In this smart contract after the user enters his/her vote on the UI, the data is encrypted using the public key of the Asymmetric key pair generated by the admin, and then after a very small amount is deducted from the user account, the contact is put into the chain where only the admin can access the data as only he posses the decryption key.

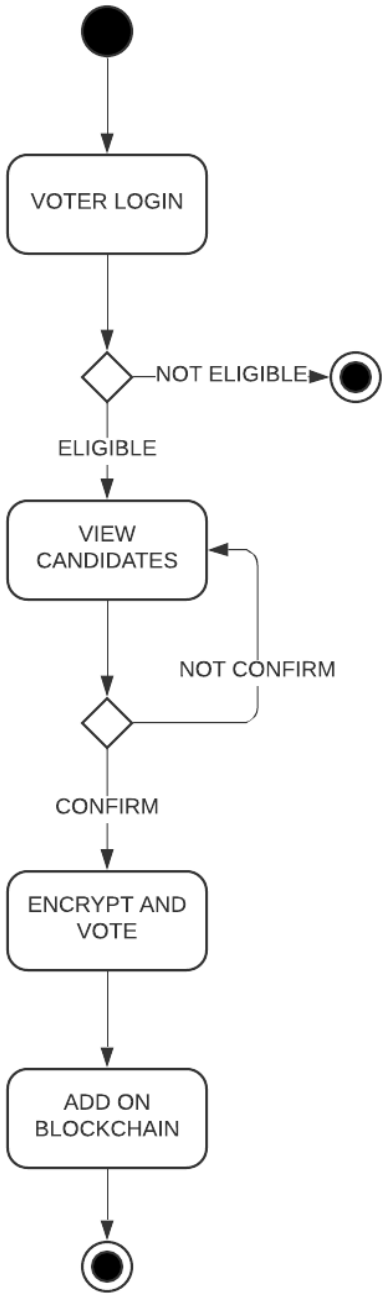


Development View: Describes the components and modules used for assembling this application like

- **Web Browser:** Used for creating an interactive user interface.
- **Ethereum blockchain:** Used for storing the data can use other databases like BigchainDB.
- **Validation Authority:** The third-party authority that validates whether the entered block is entered by an authentic user.
- **IPFS:** A module that is used for host dataset, software, etc. in a network.



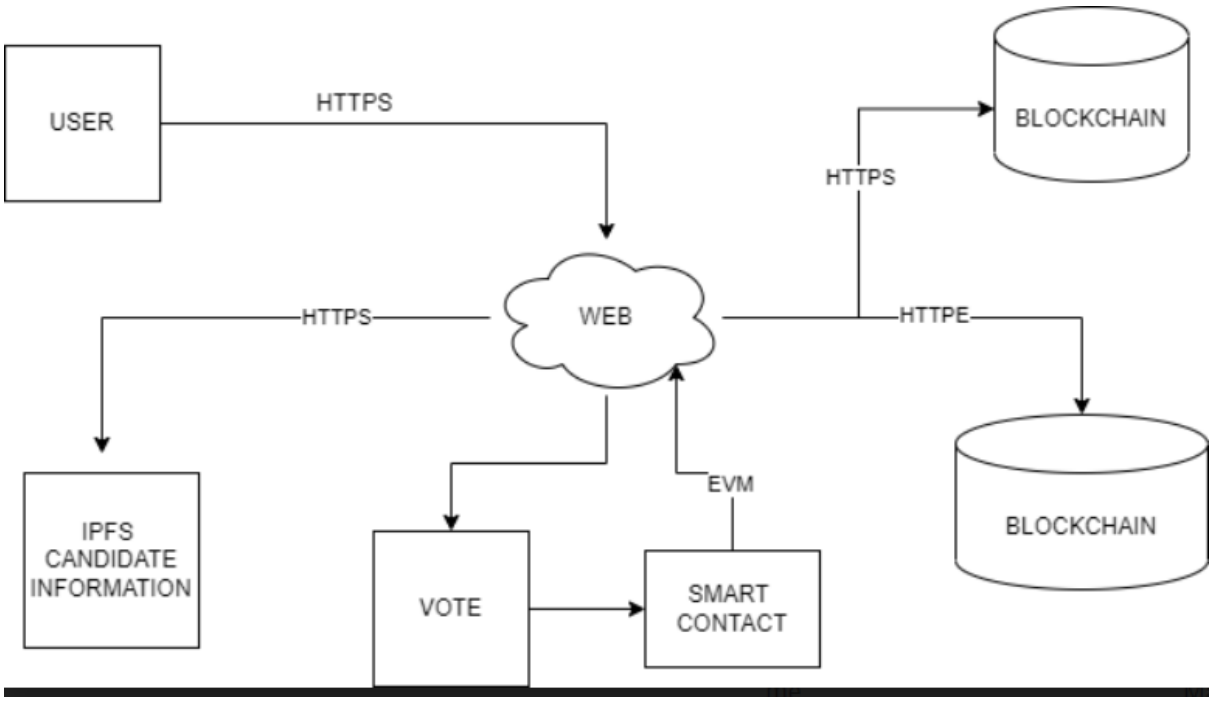
Process View: Describes the interaction of the users with the system. For this use case, the interactions consist of User logging, Checking the Candidate's information, and only one vote for the respective candidate from a user.



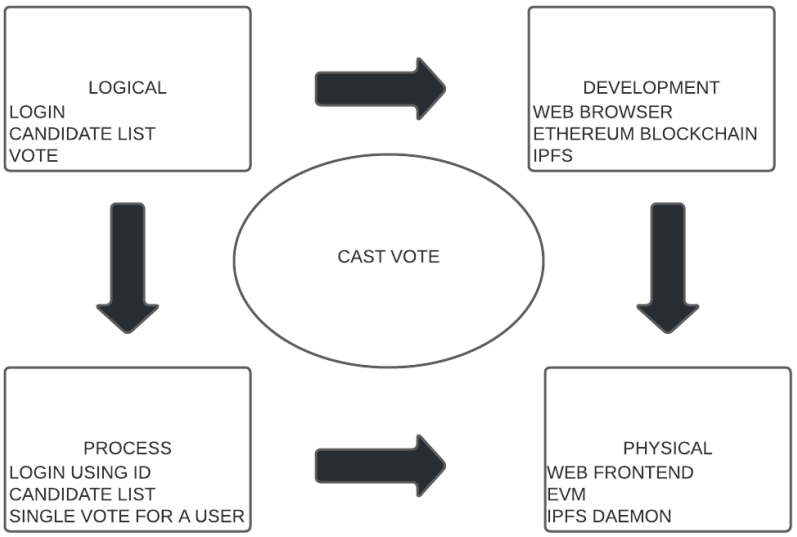
ACTIVITY DIAGRAM

Physical View: Describes the interconnection between hardware and software and the implementation of the application that is web front-end using HTML, CSS, etc or frameworks like Ganache, EVM (Ethereum virtual machine) used for running Ethereum blockchain, IPFS Daemon for Network, Validate.js that is used for validation.

The above described 4 Views Logical, Development, Process, and Physical with a certain use case constitute the 4 + 1 View of and Application

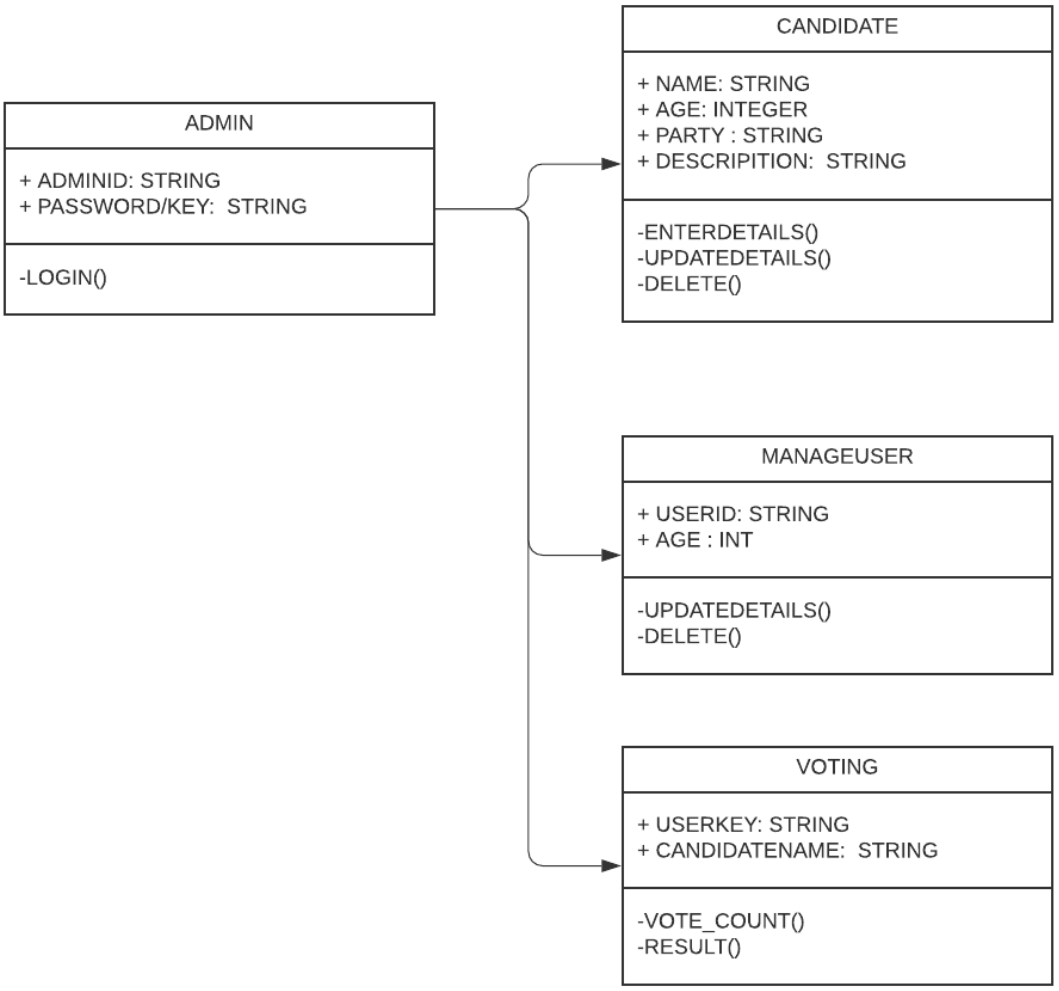


Combining the Views.



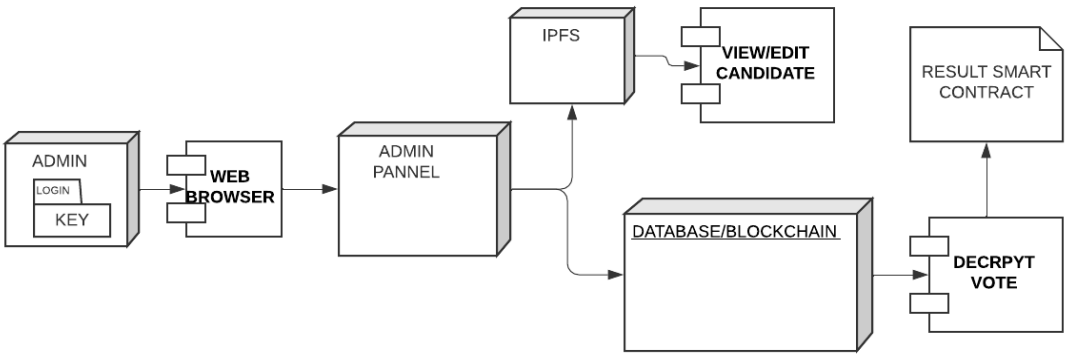
Use case/Scenario 2: Result - In this use case the admin after logging in using his/her authentic id and password and accessing the data in the ledger publishes the result after the voting is closed. This is because only the admin possesses the decryption key that can be used for decrypting the data and hence only he knows the vote counts.
The four views are:-

Logical View: Describes the system of smart contracts used in this application. There is one smart contract used for this scenario called as result in which the admin just needs to access all the vote counts and provide the result.

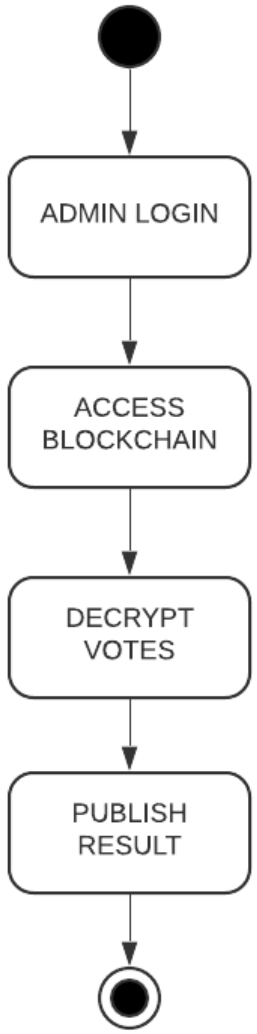


Development View: Describes the components and modules used for assembling this application like

- **Web Browser:** Used for creating an interactive user interface.
- **Ethereum blockchain:** Used for storing the data can use other databases like BigchainDB.
- **Validation Authority:** The third-party authority that validates whether the entered block is entered by an authentic user.
- **IPFS:** A module that is used for host dataset, software, etc. in a network.



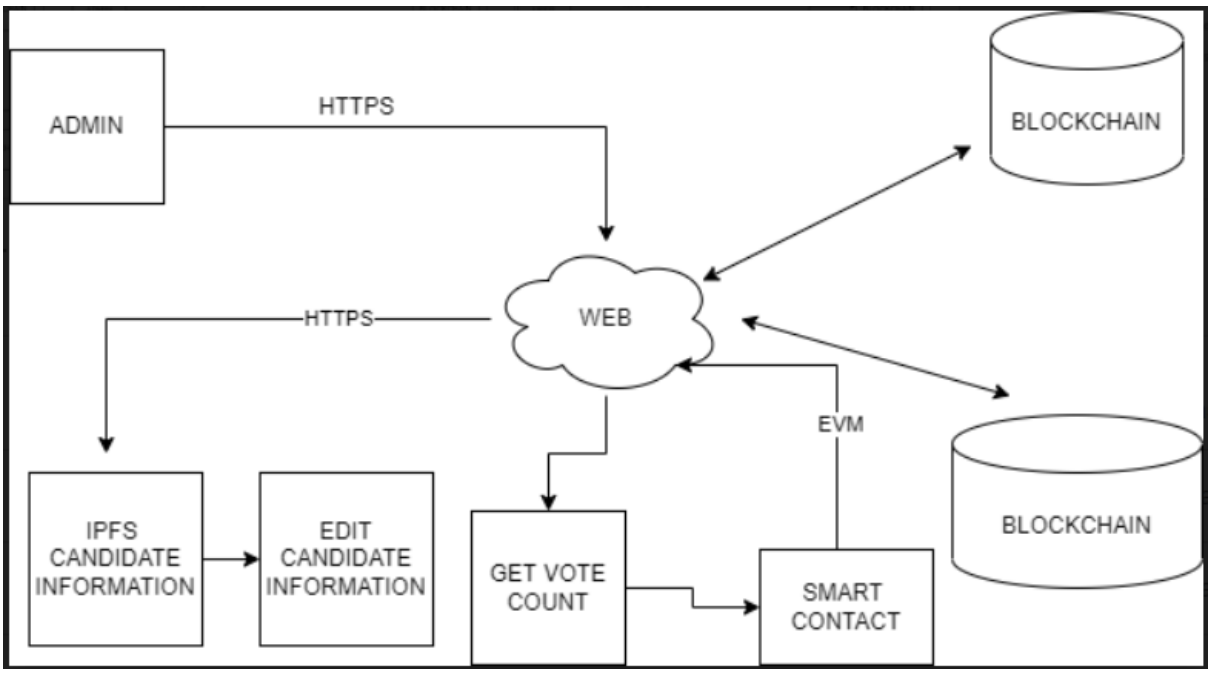
Process View: Describes the interaction of the admin with the system. For this use case, the interactions consist of Admin logging, Checking the User's and Candidate's information, accessing the database for the vote count, and providing the result.



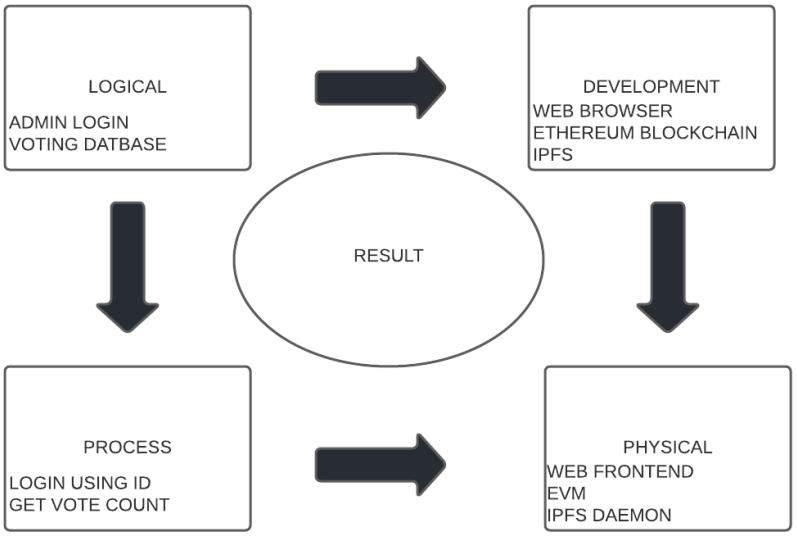
ACTIVITY DIAGRAM

Physical View: Describes the interconnection between hardware and software and the implementation of the application that is web front-end using HTML, CSS, etc or frameworks like Ganache, EVM (Ethereum virtual machine) used for running Ethereum blockchain, IPFS Daemon for Network, Validate.js that is used for validation.

The above described 4 Views Logical, Development, Process, and Physical with a certain use case constitute the 4 + 1 View of and Application



The combine 4+1 view are described below.



Solution 2:

The application "FOLLOW MY VOTE" is a Blockchain-based Electronic Voting System. In this system, users can securely vote using the private Ethereum blockchain. The design patterns implemented in this application can be.

A. Patterns for Smart contract

➔ **Problem:** As voting is considered as a legal agreement and thus there cannot be any discrepancy in this system. Now the problem arises about binding the smart contracts on a trusted private environment such that only the user and the trusted authority can access the votes.

➔ **Context:** The legal industry all around the world is becoming digitalized and thus there emerges a need for digitalizing the voting system of a country as we have seen during covid19 there were many rallies related to voting which is not good in these times thus a legal digitalized voting system is required.

➔ **Forces:** There are three forces related to the above problem
- ◆ **Authorization:** The source must be an authorized citizen of the country.
- ◆ **Storage:** The blockchain should provide secure storage of votes.
- ◆ **Execution:** The blockchain-based system should provide a secure executable platform for the application where one-to-one mapping of votes to trusted authority is maintained.

➔ **Solution:** Blockchain is an ideal platform to run legal digital agreements since it used a private network and smart contracts to enable legal binding of the physical contract to legal digitalized contract which is stored on the chain. Also since blockchain is based on hashing the legal contract is first converted to hash and then stored on the chain which increases the security. And this binding from physical to digitalized contract is a one-to-one mapping between user and trusted authority (only the user knows whom he has voted and only the trusted authority knows the total count of votes).

➔ **Consequences:**
- ◆ **Advantages:**
  - **Audit Trail:** As blockchain is a ledger all the audits are recorded and we can know easily if any discrepancies to our data are done or not.
  - **Automation:** For each vote by a user a small amount is deducted from their account automatically.
- ◆ **Disadvantages:**
  - **Enforceability:** For each block to be included in the chain a consensus is required and if there are some problems with that the block may not be included in the chain.
  - **Time:** If private blockchain is used then for each block 10 minutes are required to be included in the chain.

B. Patterns for Data encrypting

- **Problem:** The lack of data privacy is a major concern for the use of legal documents in the blockchain as all the data of the users are visible to all the users as blockchain is a distributed network. This is the case with all types of blockchain private, public, or consortium and hence a need for encrypting this data is required for confidentiality.
- **Context:** The legal industry all around the world is becoming digitalized and thus there emerges a need for digitalizing the voting system of a country as we have seen during covid19 there were many rallies related to voting which is not good in these times thus a legal digitalized voting system is required. When we use these systems there may be a chance that our data is accessed by other users and thus we need to securely provide our data so that there may not be any confidentially related issues like we do not want other users to know whom we voted for.
- **Forces:** There are two forces related to the above problem
  - **Transparency:** The data of all the users are accessible to all users whether public, private or consortium-based blockchains.
  - **Confidentiality:** Since there is very much transparency of data confidential information should not be stored on the blockchain in plain form.
- **Solution:** The trusted authority should create a private key pair using Asymmetric key encryption and share its public key then all the users should encrypt the data using this public key and add that on the chain then only the trusted authority can access the data by decrypting it using the private key and hence votes will be confidential.
- **Consequences:**
  - **Advantages:**
    - Confidentiality: Using Asymmetric key encryption.
  - **Disadvantages:**
    - **Key Sharing:** If the keys are compromised it may lead to problems.
    - **Immutable data:** As data is always present in the blockchain in the late future some measures may be developed to crack the Asymmetric key encryption using quantum computing and thus this may lead to problems.