# **This ReadMe Includes:**

1. Deployment Instructions
2. Project Brief

# **Instructions on how to deploy:**

**Step 1.) (Required software)**

The following are the softwares required to deploy the smart contract:

a.) Node.js and npm

b.) Npm install web3 (web3 js)

c.) Truffle ganache (download stable truffle ganache desktop app)

d.) Npm install -g truffle (truffle)

e.) Metamask extension

**Step 2.)**

Create a new workspace in Granache.

**Step 3.) (Configure truffle-confiq.js using Ganache.)**

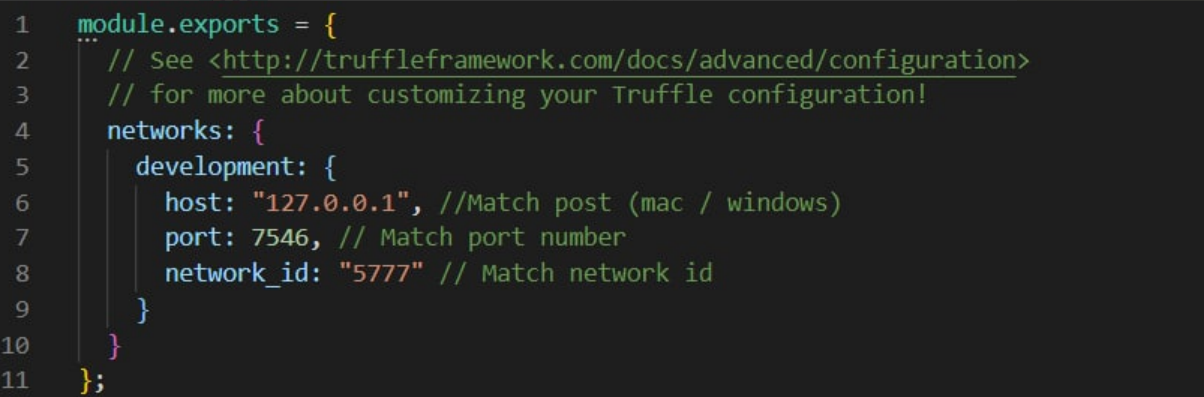
Ensure port number and network id matches in truffle-config.js as seen in screenshot of

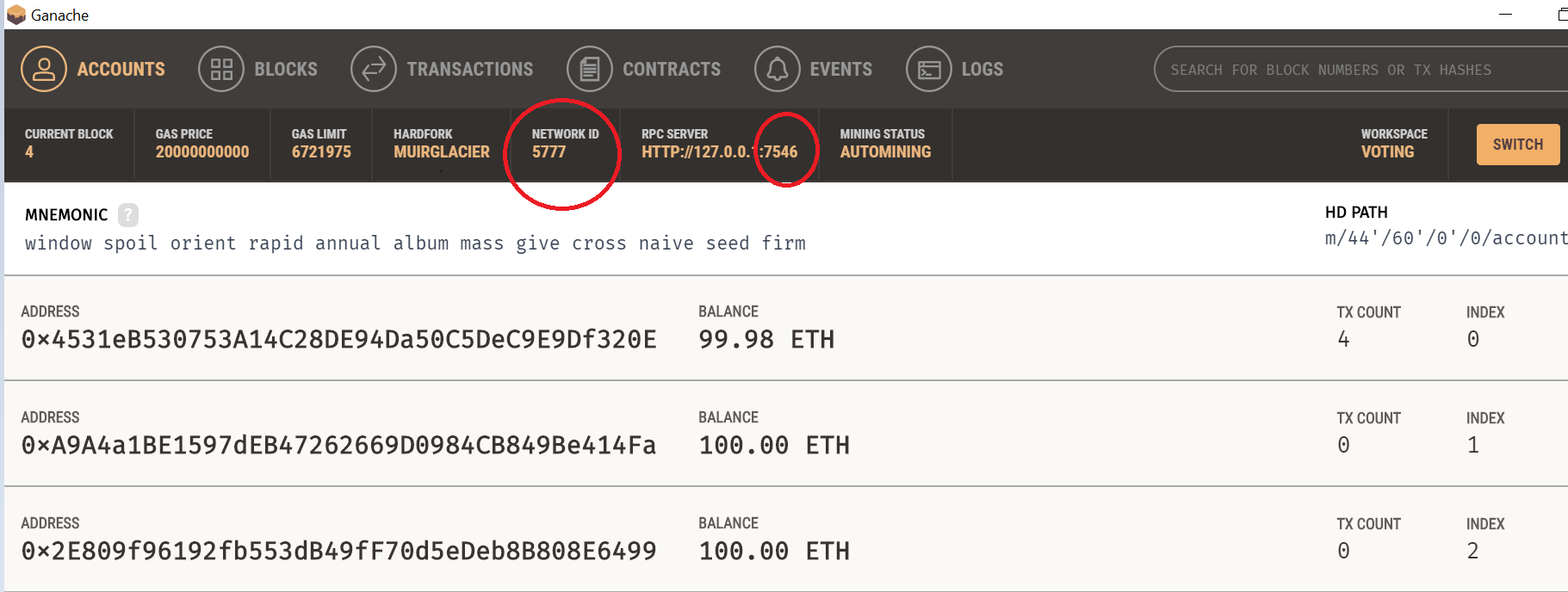
Granache setup:

1. Select extension icon, select metamask extension
2. Select “No, I already have a seed phrase”.
3. Copy mnemonic from ganache and add as seed phrase, create new password and confirm password



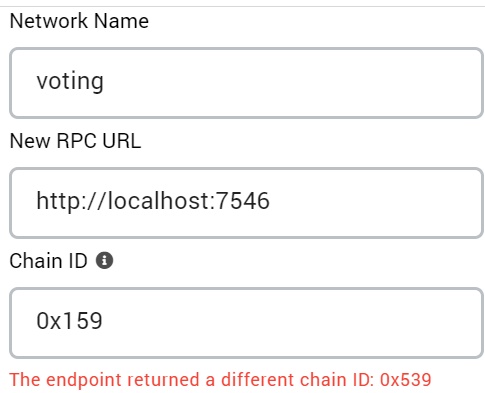
1. Select metamask networks from the dropdown
2. Select custom RPC
3. Enter the following credentials and make sure they match





**Step 3.) (Configuring MetaMask)**

Click chrome extension and select MetaMask. Fill in the details as shown below. For your convenience, enter a random chainId and upon the prompt as shown below, change the chainId to match the one given by the prompt.

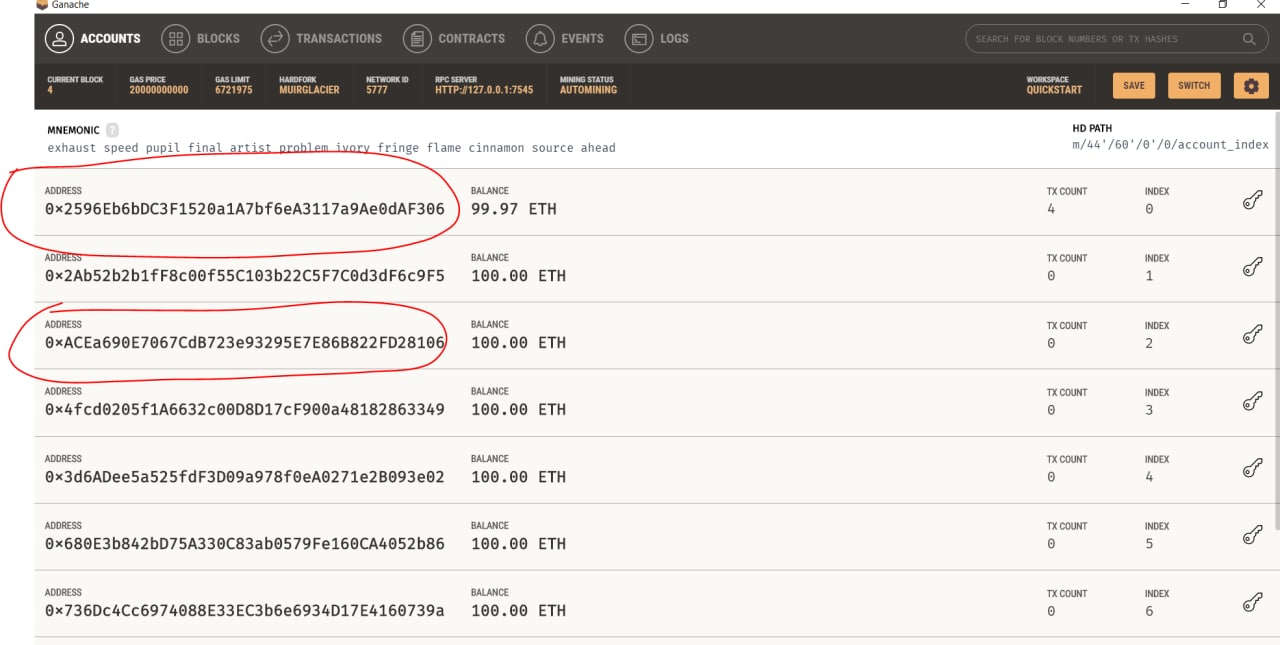


**Step 4.) (Creating new test cases)**

Edit the following code below in Election.sol to create new test cases. Voters will take in 2 parameters, address and number of shares.



Addresses of shareholders can be obtained from Granache.



**Step 5.) (Launching of Voting platform)**

Under Command prompt, go to dir /Voting.

Run “truffle compile” into the command prompt.

Run “truffle migrate” into the command prompt.

Run “npm run dev” to launch the dApp.

MetaMask will prompt you to connect with MetaMask.

Click “Next”.

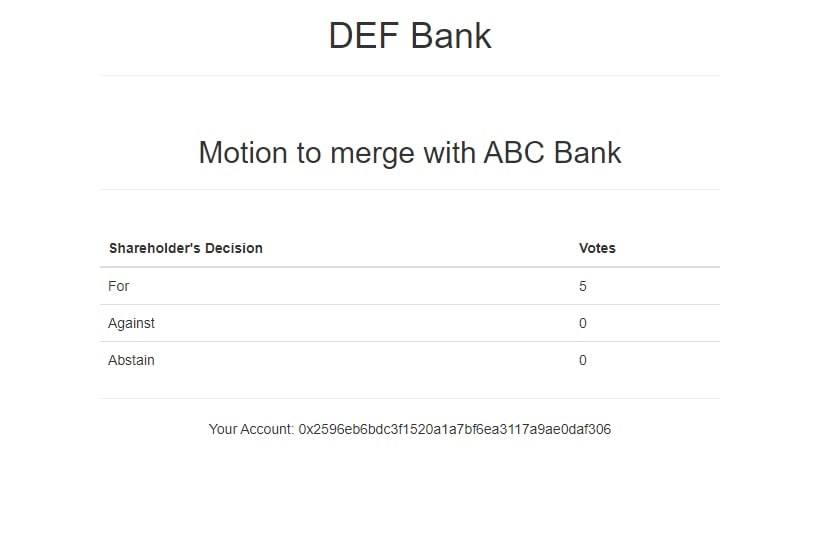
Click “Connect”.

Click refresh on your brower.

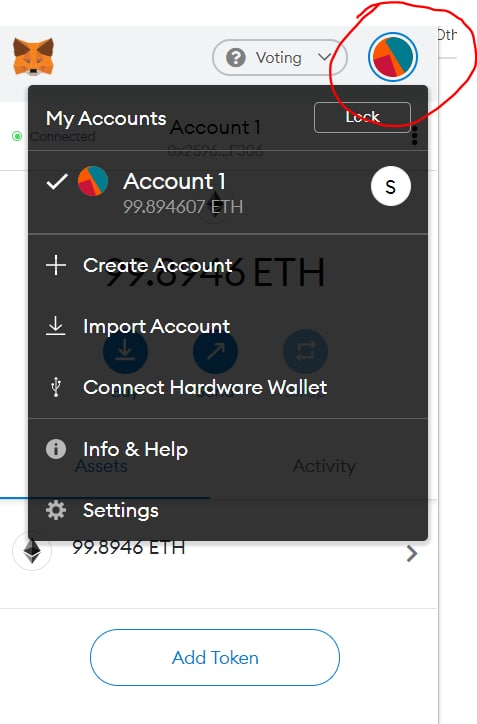
**Step 6.) (Test cases)**

Using one of the accounts, choose a vote(For, against, abstain) and click “vote”.

Metamask would prompt a transaction. Click “confirm”. The number of votes would increase by the number of shares.

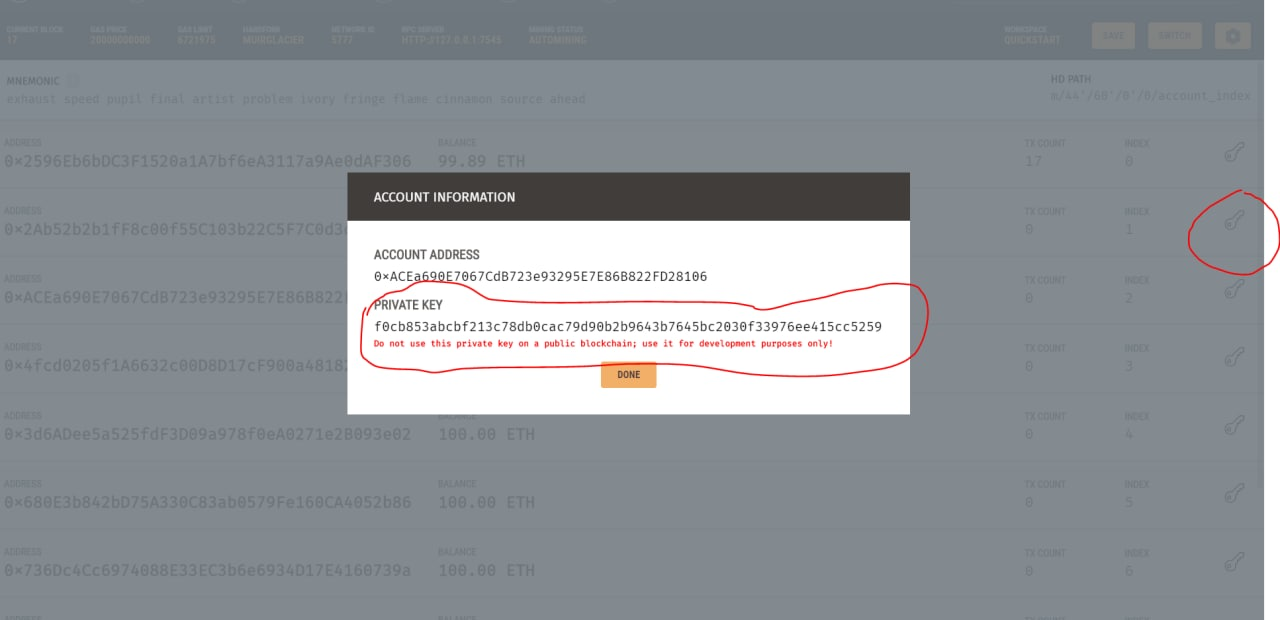


**Step 7.) (Using different accounts to cast vote)**

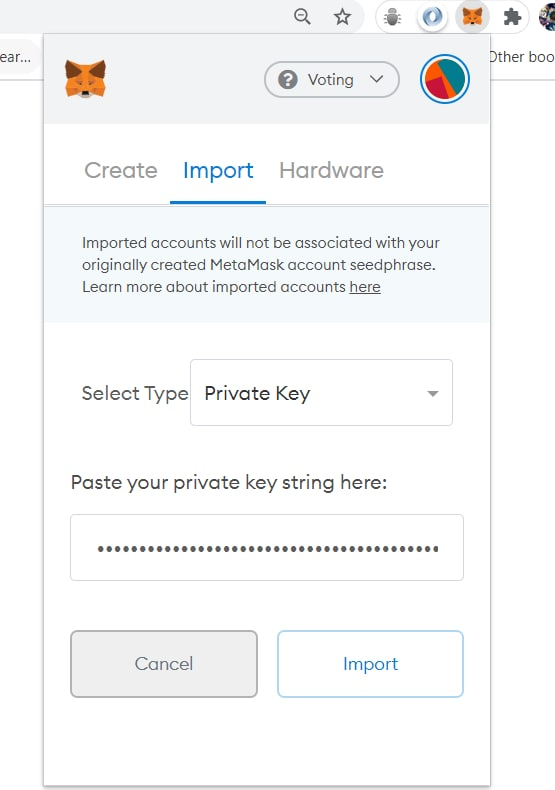
Click MetaMask extension and select the pie chart on the top right.

Select “Import account”.

Select private key belonging to one of the addresses that is added in step 4. You can do this via Granache and clicking the key icon on the extreme right. Next, copy the private key in the text box.

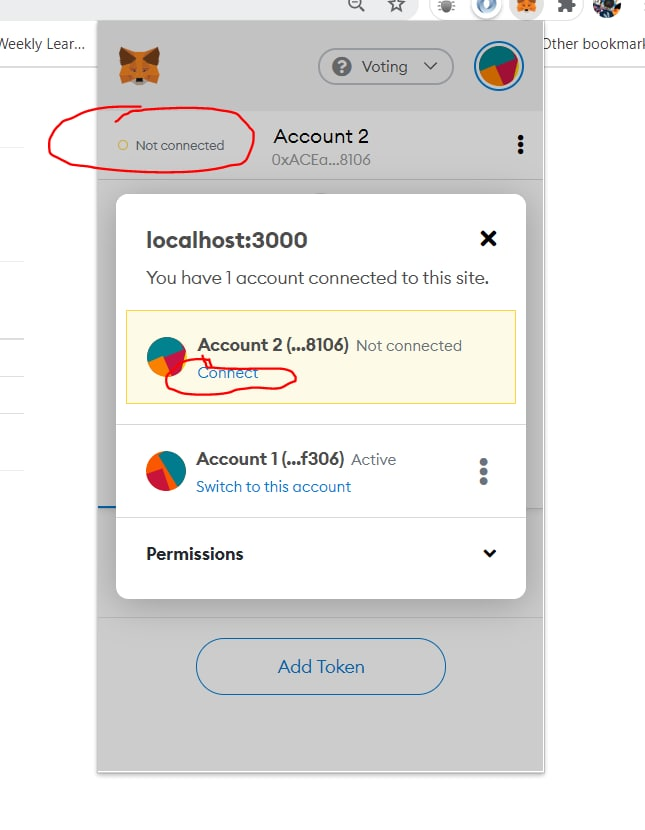


Input the private key obtained from Granache into MetaMask.

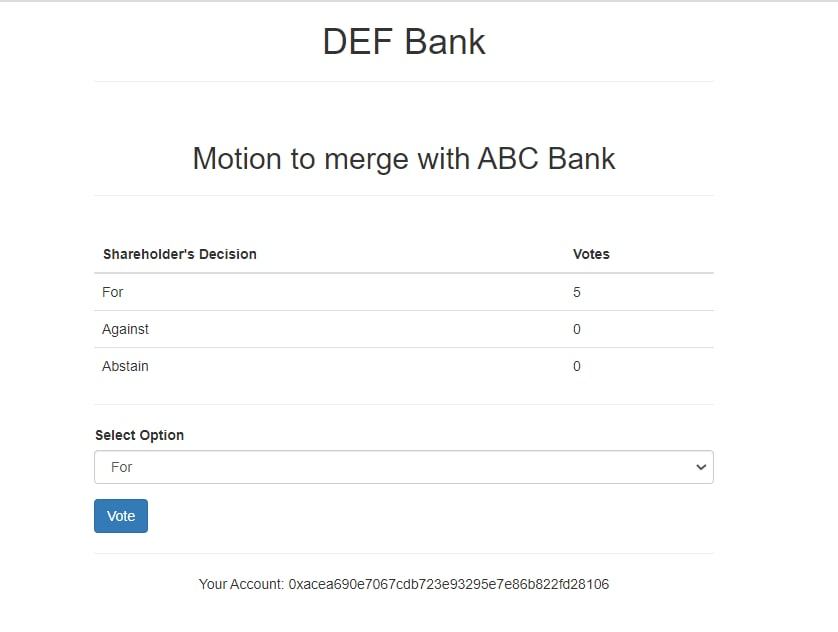


Click “Import”.

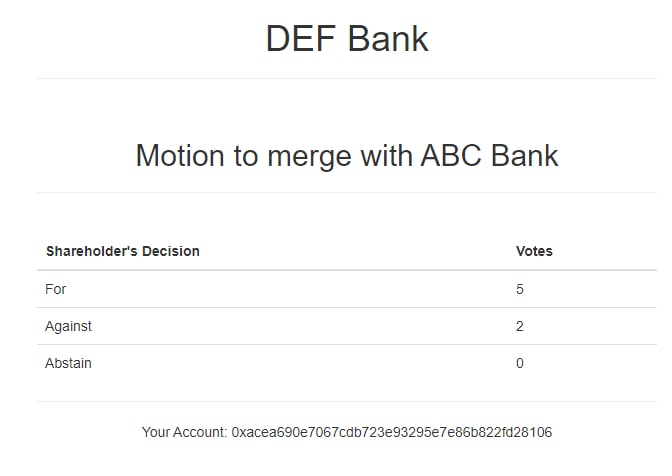
In MetaMask extension, click “Not connected” followed by connecting to the new account you just added.



The voting platform should now have the updated account address, ready to vote.



Click an option of your choice and click confirm when MetaMask prompts you with a transaction. The Voting result should be updated with the new voting result.

**Additional procedures(If encounter errors):**

To re-initialize the smart contract, open command prompt/terminal. Run the command “truffle migrate --reset”.

Due to block delay, you may need to refresh the browser an additional time.

Project Brief

# 1. Why blockchain

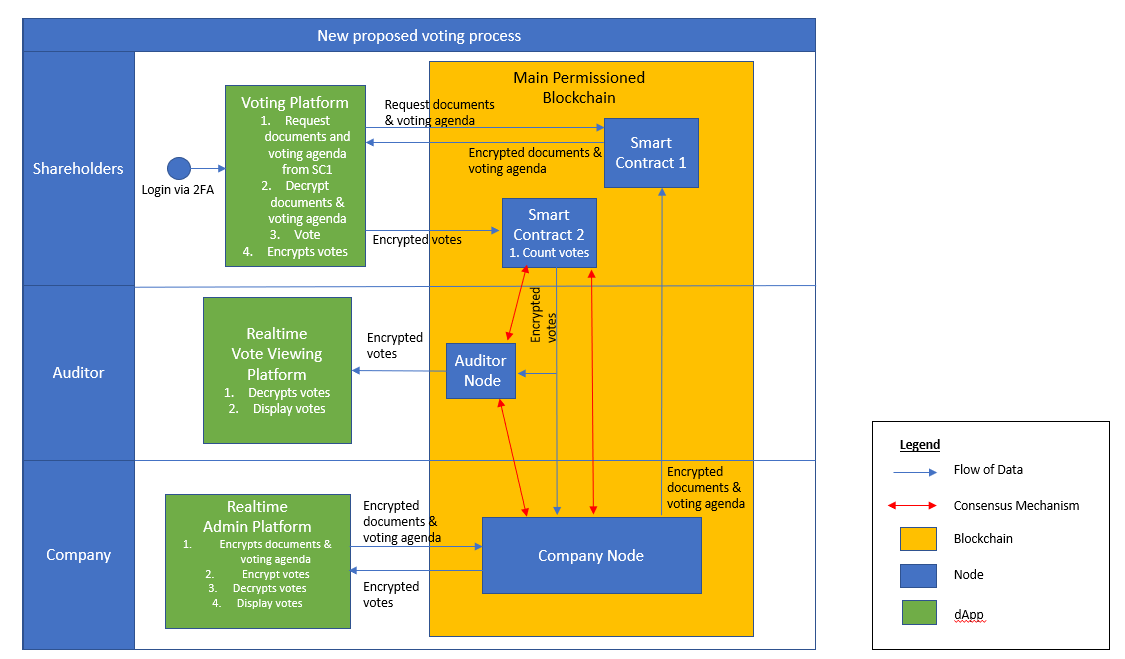
The current issue plaguing the shareholder voting system is that the voting process is currently too opaque to its shareholders and auditors. The company controls the process of voting through the web services they host and the various other methods such as proxy voting and mail-in voting. This places the trust solely in the hands of the company, every shareholder must trust that the various voting processes together with the votes in-person at annual general meetings (AGM) are accurate. In addition to voting by being at the physical AGM itself, there would be occasions where shareholders are unable to attend due to inconveniences. Hence, alternatives to voting in person must be made available to shareholders as well as it being an equitable process. The risks are mitigated through the hire of auditors to ensure the processes, however, there is still an inherent issue of the conflict of interest between the auditors and the shareholders.

Our proposed solution will focus on further enhancing the viability of a blockchain solution to the online voting process for AGMs.

**Benefits of a blockchain solution**

* **Immutability** - Immutability ensures the equitable treatment of shareholder’s votes, ensuring that once their vote is cast, it cannot be manipulated. The inherent characteristics of blockchain will aid in complicating any fraudulent behaviours.
* **Anonymity** - The blockchain can ensure the anonymity of the user by utilisation of other forms of identification such as public/private key or 2-factor authentication(2FA). This will be well-perceived in the United States as many shareholders would wish to remain anonymous. In addition, regulations in the US heavily prioritise freedom of choice and with that, anonymity.
* **Ease of Voting** - Through the utilisation of the blockchain solution, the voting process can be further simplified for shareholders. The blockchain can ensure an easy, safe and fair voting process for all shareholders, even for those who choose to vote via proxy voting. This will allow the company employing the blockchain solution to have an easier time in engaging its shareholders.
* **Efficiency** - The vote tally can be quickly and accurately counted with the help of the blockchain. Minimisation of human error and fraudulent resolutions are also key benefits as any authorised user can verify the authenticity and accuracy of the shareholder’s votes.

# 2. High-Level System Diagram



The user will firstly, access the voting platform and authenticate through 2FA to confirm the identity of the shareholder. The platform will then display the relevant documents and options available for the shareholder to vote. Once the vote is entered, the data will be encrypted and hashed before it is added to the blockchain by a smart contract. The data once received through the company nodes and auditor nodes will be added to the blockchain through the consensus mechanisms which will be elaborated later in the document.

# 3. System Design

The decentralised blockchain will allow for ease of scaling through the addition of multiple parties into the blockchain consortium. The voting platform will be a decentralised application which holds a private and public key required for encryption and decryption of data and documents. This adds another level of security as should any information within the process be compromised or stolen, the information would be meaningless to the perpetrator unless the person has the private key for decryption.

Based on our proposed solution, the deployment of the nodes will be through 2 main parties, the company itself and the auditors of the company. This will allow the auditors to ensure the accuracy as well as enforcement of the company and corporate governance policies during the AGMs. The parties involved are recommended to employ an even split of auditor nodes and company nodes to prevent a 51% attack. This would also increase the byzantine fault tolerance of the system should some nodes fail or act maliciously. The company will be in charge of deploying a web-server to allow the shareholders to access the blockchain through a web layer online. Additionally, the source codes should be shared between the auditors or source code auditors to ensure that the vulnerabilities of the smart contract and blockchain are discovered and rectified quickly.

# 4. Smart Contract Functionalities

## Number of smart contract

Our proposed blockchain solution will require a minimum of 2 smart contracts to facilitate the shareholder voting process. The smart contracts are not exhaustive and pertain only to the features and functions listed below. Companies can choose to add more smart contracts to better suit their company’s needs or regulations.

## Smart contract functions

### Documents.sol

Documents.sol will deal with the information downstream to be displayed to the users. Once the user has authenticated their identity through security measures on the web portal, this smart contract will call a function to retrieve encrypted documents from the private permissioned blockchain so that it can be displayed for users on the dApp. The information that will be retrieved includes:

Voter information - StockID | Number of shares

Voting Information - Questions | Options

Document.sol also validates that it has been called by the correct user account on the web portal. Once this is complete, the voting platform will decrypt the required documents using a private key, allowing the user to access them.

The documents retrieved will then be displayed for the users to see, mainly the proxy statement (DEF 14A), the Annual Report (10-K) and all other relevant information regarding the AGM. The web application will also display a list of options that will be listed on the agenda of the AGM, showing shareholders the questions raised during the AGM and the options available to them.

### Elections.sol

This smart contract will deal with the voting process itself, regarding the votes and the weight of the votes. It is designed to optimise the voting process for the auditors and the company to minimise the human time spent on hand-processing proxy cards and votes in person.

A cut-off date will also be implemented on this smart contract. Should the user attempt to submit his vote after the specified cut-off date, the smart contract will display a message on the web portal that the voting period has ended and that voting for this particular matter has ceased. This is to mitigate the risk of uncertain shareowners as shares are frequently traded on the Over-The-Counter (OTC) market. The company will announce an X date for voting on the agenda of the AGM, this is to minimise the confusion on which share holds which vote.

Hashing is added as an extra layer of security if another participant on the blockchain network can decrypt the user’s votes. In such an event, the party decrypting it will only have a hash of the user’s votes. On the other hand, since each voting matter is limited to a certain number of voting options (e.g. For, against, abstain), this hashed value can be compared to the company’s hashing algorithms to know what the vote is.

## Integration of smart contracts

Document.sol is in charge of ensuring that the shareholders are only given the specific proxy voting card as well as voting information as these documents and information can differ from one shareholder to another. This would facilitate the shareholder in making informed voting decisions.

Elections.sol is mainly in charge of vote management. From the collection of votes from the dApp, uploading the encrypted voting information as well as retrieving votes from the blockchain, this smart contract is responsible for tabulation of votes as well. This would serve as the main channel where there is high traffic of voting-related information.

Once the shareholder cast their votes, the submitted details will be parsed through Elections.sol. This smart contract would then proceed to hash the transaction and encrypt the information such as timestamps and votes for each agenda. These data will be sent to the blockchain nodes for addition into the distributed ledger as transactions.

# 5. Governance of System

The ledger will be based on the private-permissioned blockchain, as a result, the nodes and users who have access to the blockchain platform will be assumed to be trusted. However, we would still be implementing an elected leader approach for consensus to ensure the integrity of the entire blockchain is not compromised. This reduces the risk of having a rogue node from compromising the integrity of the blockchain through the elected leader process. Being a part of the permissioned blockchain, the auditors can also verify the authenticity of the voting process and the votes itself, leading to better corporate governance and transparency to shareholders.

# 6. Commercial Cost and Benefits

The commercial cost and benefits will be calculated based on development costs and the cost of running the blockchain system. The developmental cost of the blockchain system will be based on estimates for a medium-sized firm amassing approximately 100,000 individual shareholders as shown in Table 1. The ongoing costs will be based on a system that will handle small and large capital size investors,10,000 and 1,000,000 shares respectively as shown in Table 1.

|  |  |  |
| --- | --- | --- |
|  | Outsourced | Inhouse development |
| The development cost of blockchain and smart contract - Development time | 2 months | 3 months |
| cost per month for software developer | $3,000 | $5,000 |
| Number of Developers | 4 | 3 |
| **Total Development cost** | **$24,000** | **$45,000** |
|  |  |  |
| Project Management  - lead time | 3 months | 4 months |
| Project Managers Required | 2 | 1 |
| Cost Per month | $4,500 | $5,500 |
| **Total Project management cost** | **$27,000** | **$22,000** |
|  |  |  |
| Implementation and testing - lead time | 1 month | 1 month |
| Application Tester cost | $3,000 | $3,500 |
| System integrator cost | $5,000 | $5,000 |
| **Total Implementation and testing cost** | **$8,000** | **$8,500** |
|  |  |  |
| **Total Cost of solution** | **$59,000** | **$75,500** |

Table 1: Cost for development

The ongoing cost of running and maintaining the servers will be on a pay-on-demand basis. The annual general meetings (AGM) will be held only once a year and extraordinary general meetings are held only when there is a major issue regarding the firms that require the votes of its shareholders, therefore, the costing will be based on a single AGM. This can be extrapolated to any number of shareholder meetings that the firm requires.

The nodes will be assumed to be hosted by a single company to let us understand the full cost of hosting the blockchain voting system, the real-world example will be more decentralised with more stakeholders hosting nodes on their own.

Further assumption of the AGMs

1. Notice of AGM will be given 21 days in advance (the minimum required by the SEC).
2. A requirement of 1 node per 50,000 shareholders with a minimum of 2 nodes.
3. The company will require 7 days to implement and test the blockchain on the recently spun up servers.
4. Total storage would be 1GB per 100,000 shareholders.
5. The server will host the web portal to access and transact using the smart contract into the blockchain. As such, the cost of hosting the web server will be factored into the cost of hosting the nodes as the nodes will be hosting the web server concurrently.

|  |  |  |
| --- | --- | --- |
| Blockchain Costs - Firm Size | Small | Large |
| Number of shareholders | 10,000 | 1,000,000 |
| Node Pricing per hour | $0.32 | $0.32 |
| Nodes Required | 2 | 20 |
| Total Hours for running node | 672 | 672 |
| **Node cost** | **$427.39** | **$4,273.92** |
|  |  |  |
| Blockchain Storage per GB per month | $0.05 | $0.05 |
| Total Storage Required in GB | 1 | 10 |
| **Storage Cost** | **$0.05** | **$0.50** |
|  |  |  |
| Number of transactions | 10,000 | 1,000,000 |
| Blockchain transaction cost | $0.0001 | $0.0001 |
| **Transaction Cost** | **$1.00** | **$100.00** |
|  |  |  |
| **Total Running cost per AGM** | **$428.44** | **$4,374.42** |

Table 2 : Costing for running a single AGM

# 7. Risks and Challenges

**Authentication Risk:** A series of identity verification exercises have to be carried out to determine the authenticity of the shareholderbefore shareholders are granted access to the blockchain network. In our specific scenario, we are using 2FA to authenticate the user. 2FA is considered best practice in many industries, however, there is an inherent risk that the device or email containing the 2FA verification can be tampered with, leading to unknown parties assuming the identity of real shareholders and voting as them.

Mitigation: Biometric 2FA is preferred to an SMS or email One-Time Pin (OTP). If a shareholder’s phone has been stolen, or email hacked, the owner would still be the only individual capable of 2FA via biometrics.

**Privacy Risk:** The process of voting is private and confidential, as a result, our team strives to ensure that the blockchain voting process remains as such. However, the nature of blockchain technology means that any votes placed on the blockchain are accessible to all members on the blockchain through the transactions. Our team has minimised the risk through the voting portal encryption and the hashing of the values, leading to enhanced security of the transaction.

Mitigation: Voters who prefer complete anonymity may opt to use zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) proofs to authenticate themselves without giving any information to other parties about who they are.

**Infrastructure Challenge:** A foreseeable challenge to the blockchain voting adoption will be the need to for specialised leader nodes to be owned, operated, or adopted by the company and auditors. The cost analysis identified that there is potential that the blockchain solution can be cheaper as compared to the cost of handling all the proxy votes through mail, companies are still resistant to adopting cutting-edge and untested solutions. Furthermore, the talent required to develop and maintain the blockchain solution may place a financial burden on the company. The ramification of the adoption of blockchain can lead to many regulatory and legal challenges, impacting mainly the legal divisions and the auditors.

Mitigation: The blockchain solution can be implemented through a contracted blockchain solutions expert to develop and run the voting solutions to minimise development and infrastructure risks of the solution.

**Security Risks:** The system architecture has several dependencies, such as a voter’s phone or computer and a working Internet connection. While the blockchain itself may be private, permissioned and immutable, these devices serve as potentially-vulnerable access points where a black-hat may attempt to gain access to the blockchain.

Mitigation: The security risks can be mitigated through the use of biometric 2FA authentication.

**Fraud Risks:** The possibility of fraudulent voting or rigging of the votes is always present. Businesses or shareholders with malicious intent can attempt to unduly influence other voters to achieve their goal. Corporate espionage is also an inherent risk, the company’s nodes can be compromised, leading to fraudulent resolutions.

Mitigation: The blockchain minimizes this through the use of an elected leader system. When comparing this to a traditional voting system, any form of internal manipulation of the system will be recorded in the block, thereby providing evidence of manipulations for audits to identify.