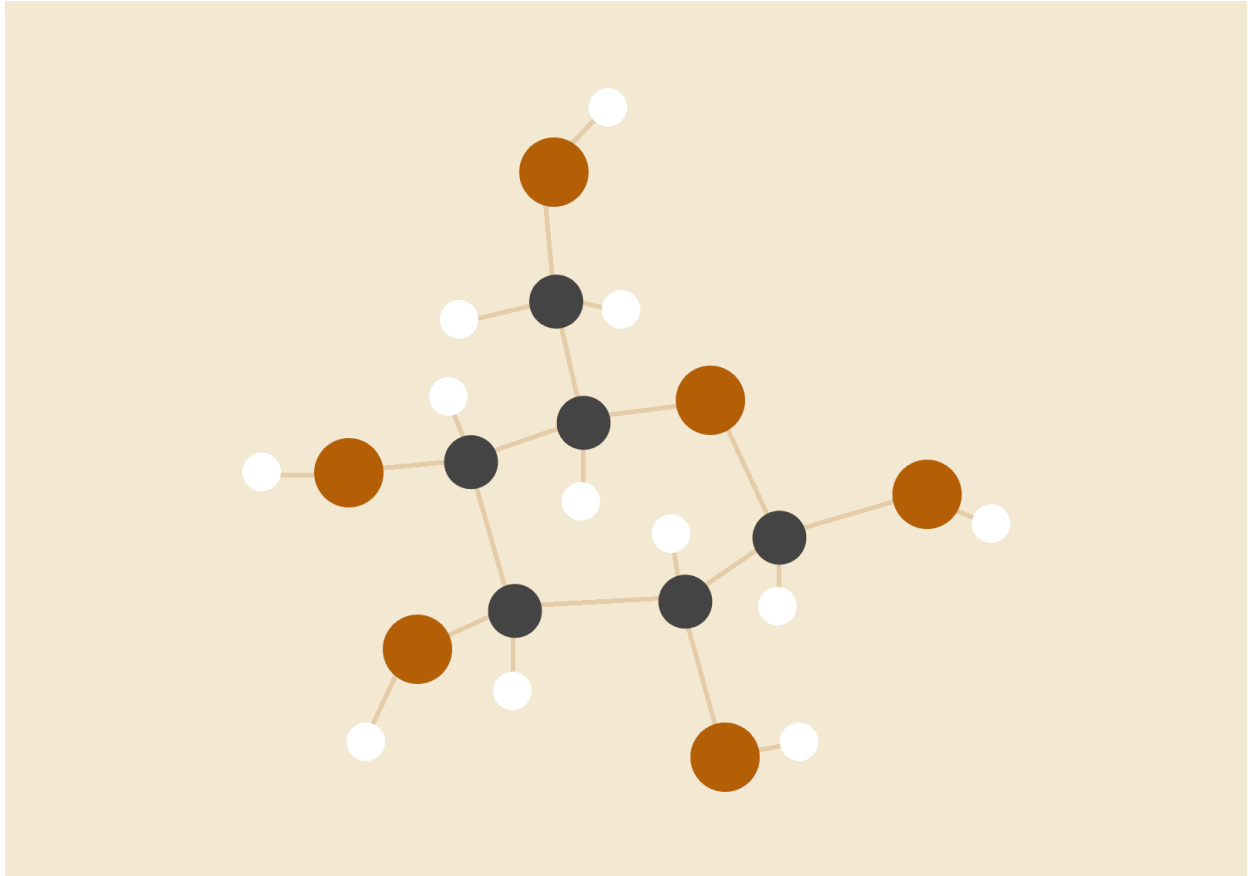


Blockchain - CSE1003

A1 Slot

Digital Assignment 2



Sri Vishva E - 18BCE0833

Niharika Gupta - 19MIS0263

Contents

Topic Create an application using smart contracts	2
Abstract	2
Preliminaries Of E-voting And Blockchain	2
Design Considerations while creating the app.....	3
Blockchain as a service	4
Methodology	4
Voting transaction:.....	6
Tools & Technologies	7
Technologies:.....	7
Tools:.....	7
Application	8
Conclusion:.....	12
References	12

Topic Create an application using smart contracts

Abstract

Smart contracts are trackable and irreversible applications that execute in a decentralized environment (e.g., blockchain). Once the smart contract has been deployed nobody can edit the code or change its execution behavior. Smart contract execution guarantees to bind parties together to an agreement as written. This creates a new powerful type of trust relationship that does not rely on a single party. Smart contracts enable better management for realizing and administering digital agreements because they are self-verifying and self-executing.

In this project we will be creating a Decentralized Voting App using smart contracts. The use of blockchain in such an application would eliminate the need of third party apps thus increasing security which leverages the unique characteristics of the blockchain network.

Preliminaries Of E-voting And Blockchain

1. Liquid Democracy Design Considerations

The main idea in a **liquid democracy** is that the voter has the power, at any given moment, to review the way his vote was cast in terms of a specific legislative proposal or a bill. This allows people with domain-specific knowledge to better influence the outcome of decisions, which should lead to an overall better governance. The concept of liquid democracy could be a possible answer to the public requests, but there are technical and social barriers in the way. The solution to the technical concerns associated with the liquid democracy concept could be vital for the evolution of democracy as we know it.

2. Blockchain as a Service

The Bitcoin blockchain technology uses a decentralized public ledger combined with PoW(Proof-of-Work) based stochastic consensus protocol, with financial incentives to record a totally ordered sequence of blocks. The chain is replicated, cryptographically signed and publicly verifiable at every transaction so that no-one can tamper with the data that has been written onto the blockchain. This structure is an append-only data structure, such that new blocks of data can be written to it, **but cannot be altered or deleted**. The blocks are chained in such a way that each block has a hash that is a function of the previous block, providing the assurance of immutability.

Design Considerations while creating the app

After evaluating both existing e-voting systems and the requirements for such systems to be effectively used in a national election, we constructed the following list of requirements for a viable e-voting system:

- (i) An election system should not enable coerced voting.
- (ii) An election system should allow a method of secure authentication via an identity verification service.
- (iii) An election system should not allow traceability from votes to respective voters.
- (iv) An election system should provide transparency, in the form of a verifiable assurance to each voter that their vote was counted, correctly, and without risking the voter's privacy.
- (v) An election system should prevent any third party from tampering with any vote.
- (vi) An election system should not afford any single entity control over tallying votes and determining the result of an election.
- (vii) An election system should only allow eligible individuals to vote in an election

Blockchain as a service

The blockchain is an append-only data structure, where data is stored in a distributed ledger that cannot be tampered with or deleted. This makes the ledger immutable. The blocks are chained in such a way that each block has a hash that is a function of the previous block, and thus by induction the complete prior chain, thereby providing assurance of immutability. There are two different types of blockchains, with different levels of restrictions based on who can read and write blocks.

A public blockchain is readable and writeable for everyone in the world. This type is popular for cryptocurrencies. A private blockchain sets restrictions on who can read or interact with the blockchain. Private blockchains are also known as being permissioned, where access can be granted to specific nodes that may interact with the blockchain. In addition to cryptocurrency, blockchain provides a platform for building distributed and immutable applications or smart contracts.

Smart contracts :

They are programmable contracts that automatically execute when pre-defined conditions are met. Similar to conventional written contracts, smart contracts are used as a legally binding agreement between parties. Smart contracts automate transactions and allow parties to reach agreements directly and automatically, without the need for a middleman. Key benefits of smart contracts compared to conventional written contracts are cost saving, enhanced efficiency and risk reduction. Smart contracts redefine trust, as contracts are visible to all the users of the blockchain and can, therefore, be easily verified. In this work, we define our e-voting system based on smart contracts

Methodology

Our project uses the **proof-of-authority (POA) consensus algorithm**. In POA-based networks, transactions and blocks are validated by approved accounts, known as validators. This process is automated and does not require the validators to be constantly monitoring their computers.

A permissioned blockchain which uses the POA consensus algorithm enables us to set restrictions on a set of selected known entities to validate and certify transactions on the blockchain and censor transactions arbitrarily, with their identity and reputation at stake. This otherwise needs to be done by miners on a public blockchain which uses the POW consensus algorithm. Rather than employing mining fees, like the public blockchains in operation require, using a permissioned blockchain, validators get paid for the service they provide by acting as validators in the system. Moreover, using a private network limits the possibility for an eavesdropper to monitor traffic or read the incoming data. This is needed to fulfill voting rights so that voters can cast votes without leaking their identity or voting data, thus ensuring data privacy and security.

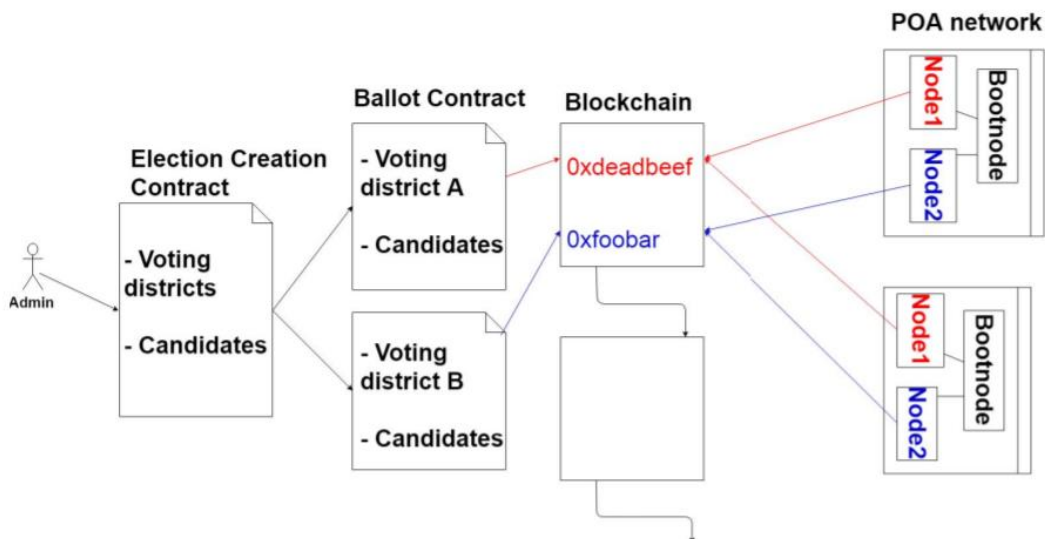


Fig 1: Election as a smart contract

Since a blockchain is a permanent record of transactions that are distributed, every vote can irrefutably be traced back to exactly when and where it happened without revealing the voter's identity. In addition, past votes cannot be changed, while the present can't be hacked, because every transaction is verified by every single node in the network. And any outside or inside attacker must have control of 51% of the nodes to alter the record.

Voting transaction:

Each voter interacts with a ballot smart contract for her corresponding voting district. This smart contract interacts with the blockchain via the corresponding district node, which appends the vote to the blockchain. Each individual voter receives the transaction ID for their vote for verification purposes. Every vote that is agreed upon, by the majority of the corresponding district nodes, is recorded as a transaction and then appended on the blockchain. Figure 2 is a visual representation of this process.

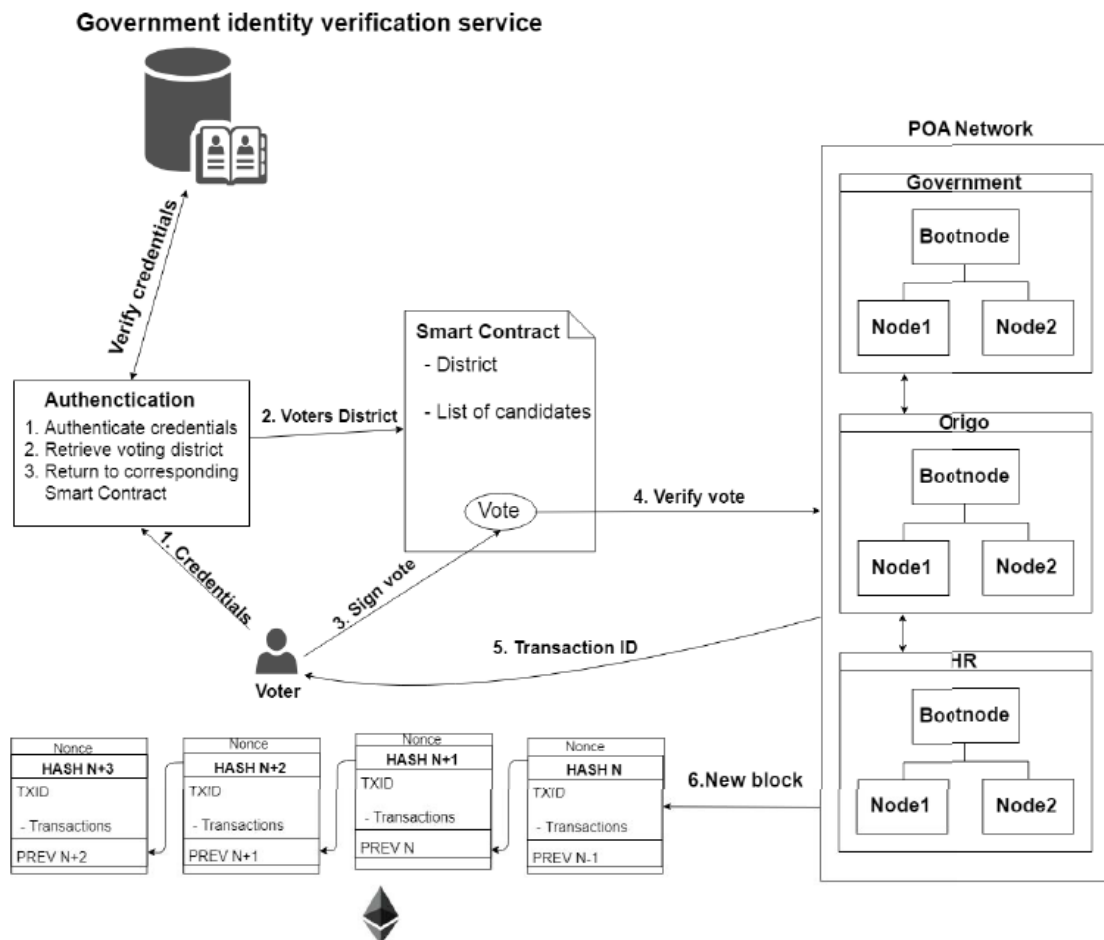


Fig 2: The voting process

Tools & Technologies

Technologies:

1. NodeJs: A backend Javascript framework for developing and testing web applications.
2. Smart Contracts using solidity: Solidity is a OOPs paradigm smart contract language. Developing a contract using solidity is of ease to the developer.
3. Ethereum Virtual Machine(EVM): EVM takes care of the internal state of the Ethereum network. EVM is similar to a phone book directory, containing cryptographic addresses that are capable of interacting , executing and exchanging data.
4. Web3.js: This is a Javascript API for interacting with blockchain, it is used to make calls and interact with smart contractors. This provides abstraction to developers, thereby allowing them to focus solely on their web application.

Tools:

1. Truffle: It is an Ethereum testing and development framework. It includes development, compilation, testing and deployment.
2. Truffle Contracts: This acts as an abstraction on top of Web3.js API. This allows us to efficiently connect and interact with smart contracts.
3. Metamask: It is a browser extension for securely using decentralized blockchain applications. We will be using this based on the necessity for deployment. It helps in masking your real-life personal id and helps to increase more privacy. We can also use our own Web3 instance during development.

Application

We built a client-side application that will talk to our smart contract on the blockchain. This client-side application has a table of candidates that lists each candidate's id, name, and vote count. It has a form where we can cast a vote for our desired candidate.

We have successfully developed a blockchain based voting application. This helps in maintaining the confidentiality, integrity and availability of the voting system.

Our dapp (decentralized application) would be a combination of frontend code + Ethereum contracts.

A user can select the candidate from the dropdown menu and vote for his choice of candidate. We can see the vote count increase as per the number of votes.

Screenshots of the application developed are as follows:

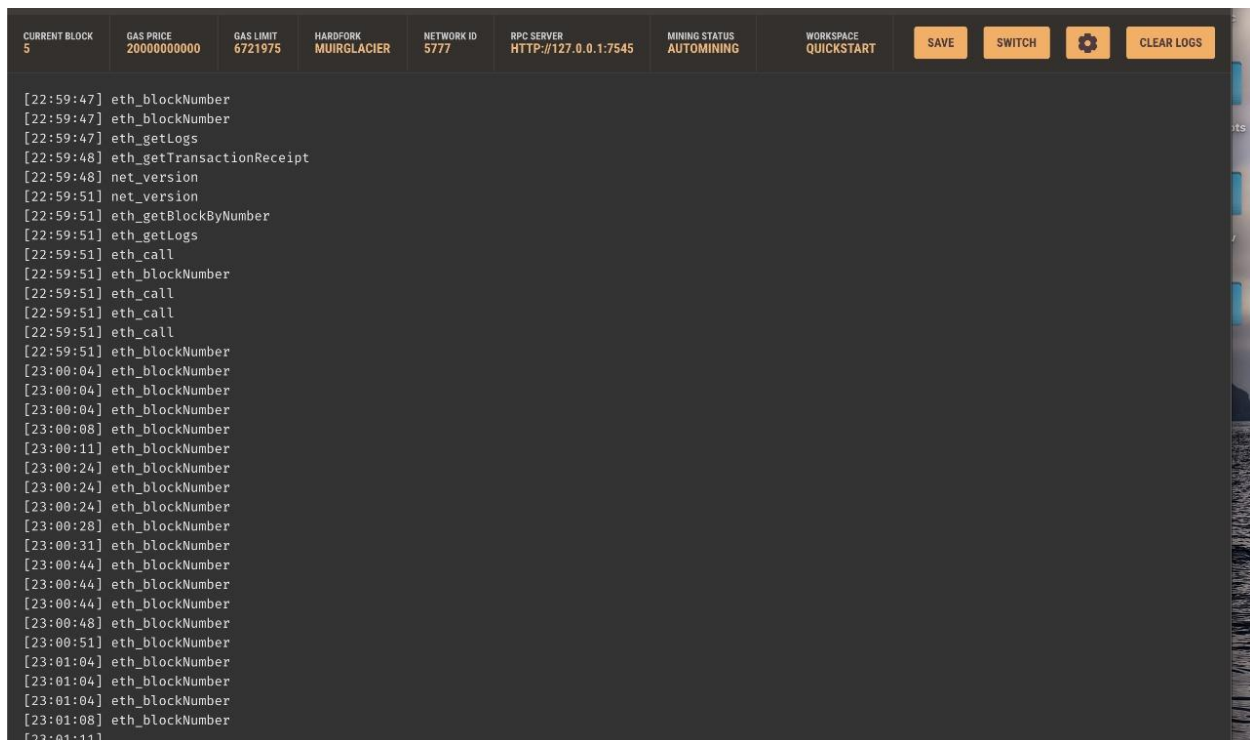



Fig 3: Ganache Setup:

CURRENT BLOCK5GAS PRICE2000000000GAS LIMIT6721975HARDFORKMUIRGLACIERNETWORK ID5777RPC SERVERHTTP://127.0.0.1:7545MINING STATUSAUTOMININGWORKSPACEQUICKSTARTSAVE SWITCH 

MNEMONIC ⓘroad orient quick humor life load nasty science decide spirit patch banner

HD PATHm/44'/60'/0'/0/account_index








ADDRESS0x7f9BFaD7c0E04290f14AB5AfF2f9E7f982348075	BALANCE99.99 ETH	TX COUNT5	INDEX0	
ADDRESS0x328658697c085E8138f858e0cdb99B00E4D18eAF	BALANCE100.00 ETH	TX COUNT0	INDEX1	
ADDRESS0xb6bE5ebe7C664eCE68c3069E5ACdCF6e2d37dFb0	BALANCE100.00 ETH	TX COUNT0	INDEX2	
ADDRESS0x61a6bCEDA6fC0ab14F6E322da7664F078Ca53D63	BALANCE100.00 ETH	TX COUNT0	INDEX3	
ADDRESS0x2559dA89fa84E0F4a951b1Ed4aF616A4466a397D	BALANCE100.00 ETH	TX COUNT0	INDEX4	
ADDRESS0xd535F1e7DD6120e7BC7B772D5D693e871850f7E5	BALANCE100.00 ETH	TX COUNT0	INDEX5	
ADDRESS0xc5A4BB47Ea097AB7ccC869B89718E6f542224102	BALANCE100.00 ETH	TX COUNT0	INDEX6	

Fig 4: The first node's balance has reduced because we have deployed contracts / written on the blockchain

CURRENT BLOCK
5

GAS PRICE
2000000000

GAS LIMIT
6721975

HARDFORK
MUIRGLACIER

NETWORK ID
5777

RPC SERVER
HTTP://127.0.0.1:7545

MINING STATUS
AUTOMINING

WORKSPACE
QUICKSTART

SAVE

SWITCH

TX HASH

0x1dc7cd523c8a87d7c6a8715b12ff16aff9a20e5a4d89d053b15e9c7df7b3ef8a

CONTRACT CALL

FROM ADDRESS

0x7f9BFaD7c0E04290f14AB5AfF2f9E7f982348075

TO CONTRACT ADDRESS

0xd42C9f7C1D0B13C484E5ED948fc990766CDFbc3E

GAS USED

66244

VALUE

0

TX HASH

0x48f4f96830c8c8ba54763aa67b83c15b7a63e5fdd3e46e356f913dd74f3239ef

CONTRACT CALL

FROM ADDRESS

0x7f9BFaD7c0E04290f14AB5AfF2f9E7f982348075

TO CONTRACT ADDRESS

0x6Ec384E87e2ba2D74a1218F56E84B4Dd532C01E7

GAS USED

27363

VALUE

0

TX HASH

0x92190dd68049e069936aa6033d5da46c907699f6daafd6d3af2f57c149726f26

CONTRACT CREATION

FROM ADDRESS

0x7f9BFaD7c0E04290f14AB5AfF2f9E7f982348075

CREATED CONTRACT ADDRESS

0xd42C9f7C1D0B13C484E5ED948fc990766CDFbc3E

GAS USED

385685

VALUE

0

TX HASH

0xe3462739490d0d362f87ac000be4468eb4ab03b737ab07ca2bfbeec8b662a6a6

CONTRACT CALL

FROM ADDRESS

0x7f9BFaD7c0E04290f14AB5AfF2f9E7f982348075

TO CONTRACT ADDRESS

0x6Ec384E87e2ba2D74a1218F56E84B4Dd532C01E7

GAS USED

42363

VALUE

0

TX HASH

0x6dc91e4bd52be28a461b2b200a504451d1180a87bf73e6bda9e7c26a4c6c27ae

CONTRACT CREATION

FROM ADDRESS

0x7f9BFaD7c0E04290f14AB5AfF2f9E7f982348075

CREATED CONTRACT ADDRESS

0x6Ec384E87e2ba2D74a1218F56E84B4Dd532C01E7

GAS USED

235227

VALUE

0

Fig 5: Ganache showing transaction's states.

CURRENT BLOCK 5	GAS PRICE 20000000000	GAS LIMIT 6721975	HARDFORK MUIRGLACIER	NETWORK ID 5777	RPC SERVER HTTP://127.0.0.1:7545	MINING STATUS AUTOMINING	WORKSPACE QUICKSTART	SAVE	SWITCH	⚙️
BLOCK 5	MINED ON 2021-05-08 22:59:47				GAS USED 66244		1 TRANSACTION			
BLOCK 4	MINED ON 2021-05-08 22:57:41				GAS USED 27363		1 TRANSACTION			
BLOCK 3	MINED ON 2021-05-08 22:57:40				GAS USED 385685		1 TRANSACTION			
BLOCK 2	MINED ON 2021-05-08 22:57:40				GAS USED 42363		1 TRANSACTION			
BLOCK 1	MINED ON 2021-05-08 22:57:40				GAS USED 225237		1 TRANSACTION			
BLOCK 0	MINED ON 2021-05-08 22:57:17				GAS USED 0		NO TRANSACTIONS			

Fig 6: Ganache summary

< → ↻ localhost:3000

Election Results

#	Name	Votes
1	Candidate 1	0
2	Candidate 2	0

Select Candidate

Candidate 1

Vote

Your Account: 0xc3b93e0aa82dcd49f4873eda659fcc7fa70a4714

Fig 7: The Main Landing page for an authenticated user to cast the vote

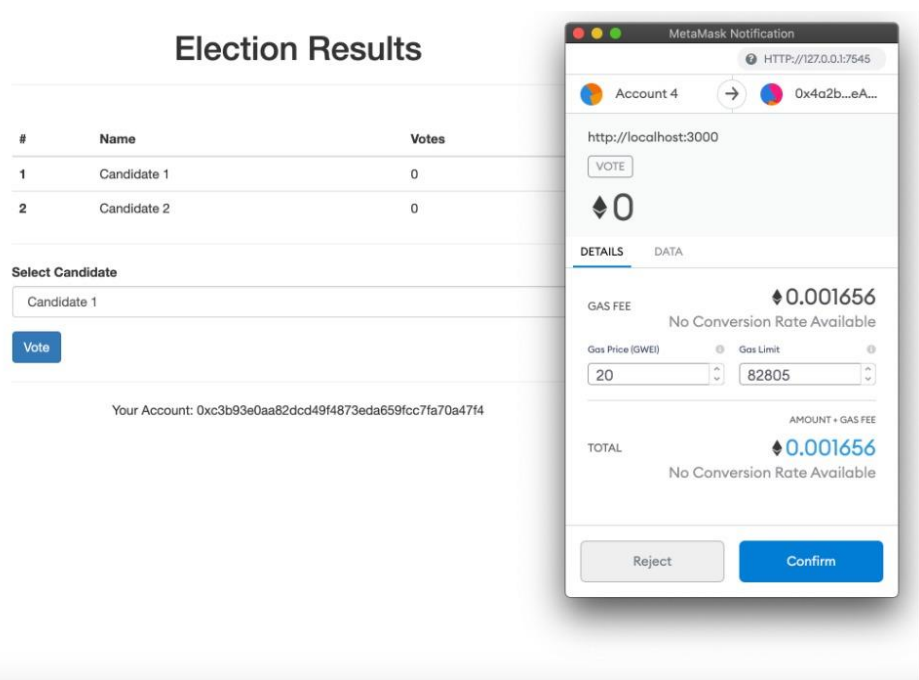


Fig 8: Notification from MetaMask after an user proceeds to vote.

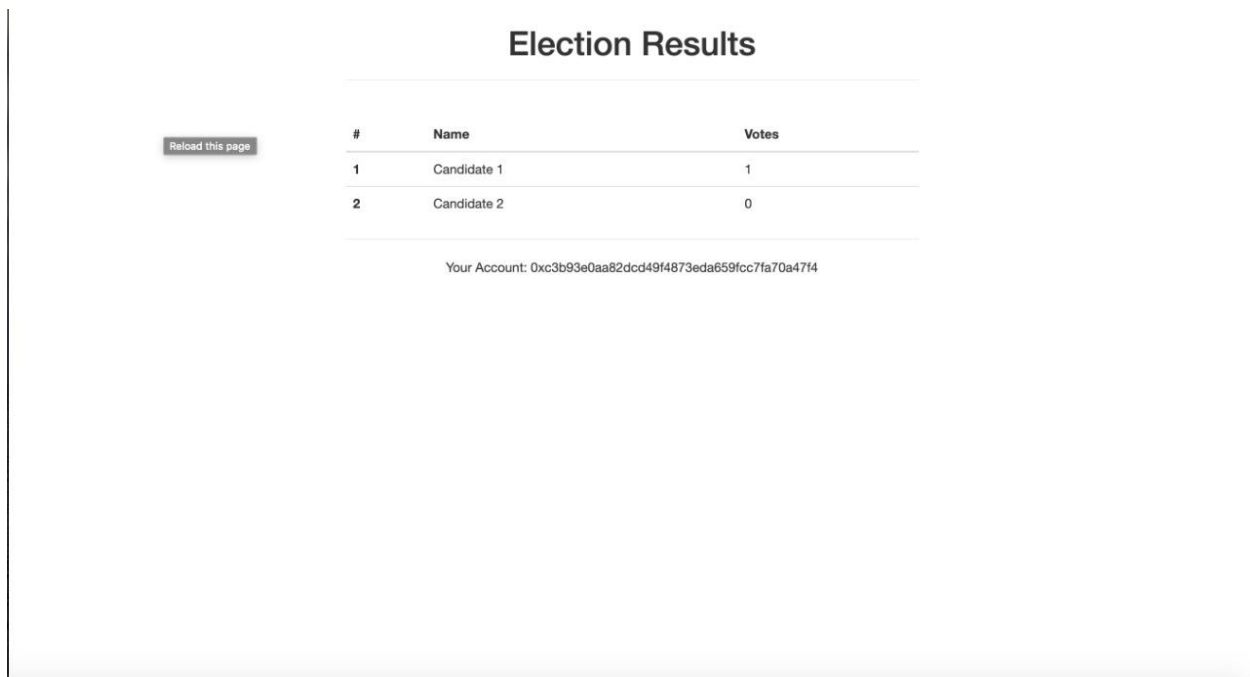


Fig 9: The Page displaying the total count of the vote each candidate receives

Conclusion:

In this paper, we introduced a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have shown that the blockchain technology offers a new possibility to overcome the limitations and adoption barriers of electronic voting systems which ensures the election security and integrity and lays the ground for transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. For countries of greater size, some additional measures would be needed to support greater throughput of transactions per second.

References:

1. Lyu, J., Jiang, Z. L., Wang, X., Nong, Z., Au, M. H., & Fang, J. (2019, August). A secure decentralized trustless E-Voting system based on smart contracts. In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 570-577). IEEE.
2. Hjalmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjalmtýsson, G. (2018, July). Blockchain-based e-voting system. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 983-986). IEEE.
3. Yu, B., Liu, J. K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., & Au, M. H. (2018, September). Platform-independent secure blockchain-based voting system. In International Conference on Information Security (pp. 369-386). Springer, Cham.
4. Panja, S., Bag, S., Hao, F., & Roy, B. (2020). A smart contract system for decentralized Borda count voting. *IEEE Transactions on Engineering Management*, 67(4), 1323-1339.
5. Dagher, G. G., Marella, P. B., Milojkovic, M., & Mohler, J. (2018). Broncovote: Secure voting system using ethereum's blockchain.
6. Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 9(3), 1-9.
7. Garg, K., Saraswat, P., Bisht, S., Aggarwal, S. K., Kothuri, S. K., & Gupta, S. (2019, April). A comparative analysis on e-voting systems using blockchain. In 2019 4th International

Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-4). IEEE.

8. Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2018, September). Crypto-voting, a Blockchain based e-Voting System. In KMIS (pp. 221-225).
9. Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure digital voting system based on blockchain technology. International Journal of Electronic Government Research (IJEGR), 14(1), 53-62.
10. Yang, X., Yi, X., Nepal, S., & Han, F. (2018, November). Decentralized voting: a self-tallying voting system using a smart contract on the ethereum blockchain. In International Conference on Web Information Systems Engineering (pp. 18-35). Springer, Cham.