E-Voting System Using Blockchain

ANIKET MUKADE
ComputerEngineering
International Institute of Information Technology
Pune, India
anikethmukade55@gmail.com

TANMAY SAMDANI
ComputerEngineering
International Institute of Information Technology
Pune, India
tanmaysamdani12345@gmail.com

VIKAS PRADHAN
ComputerEngineering
International Institute of Information Technology
Pune, India
pradhanvikas11@gmail.com

UNDER THE GUIDANCE OF

PROF. SACHIN KOLASE
ComputerEngineering
International Institute of Information Technology
Pune, India

***Abstract* — India being the largest democracy in the world, it has an abundance of different cultures, religions, languages, and beliefs. But unity in diversity comes with its own costs. It is a challenge to conduct nationwide elections for such a big and diverse population. The recent upsurge in mistrust towards electronic voting machines and trends like voter apathy where the number of people showing up to cast their vote dwindles each year is adding to the challenge of conducting fair elections. EVM machines lack auditing capabilities and require sealing, police protection, and large logistic efforts to make sure they are not tampered with. This huge logistical and security overhead adds to the cost and variables of the already delicate electoral system.**

A growing list of records that are linked using the cryptographic hash of previous blocks, is called a blockchain. Blockchain technology allows data to be captured in real-time in a secure and encrypted manner and ensures that the data is tamper-proof. Bitcoin and other cryptocurrencies are the most common examples of blockchain behavior. This technology can be used to deploy a platform that provides maximum transparency and reliability to build a trustful relationship between voters and election authorities. The platform provides a framework that can be implemented to conduct voting activity digitally through blockchain. The proposed platform provides a framework that can be implemented to conduct voting activity digitally through blockchain without involving any physical polling stations. Our proposed framework supports a scalable blockchain, by using flexible consensus algorithms.

Integration with the national database of voters will be used to validate the voter and their votes. Smart contracts are used to provide a secure connection between the user and the network while executing a transaction in the chain. By providing an irrefutable and easy way to vote from one's phone or pc, the number of people voting will likely rise. Furthermore, it will decrease the logistics and security needed for various polling booths as the records will be stored on the blockchain in real-time, unlike traditional methods that need to be sealed and transported to secure locations for the counting of votes

Keywords* — *Blockchain, cryptocurrency, consensus algorithm, tamper-proof.

I. INTRODUCTION

An electoral system or voting system is a set of rules that determine how elections and referendums are conducted and how their results are determined. Political electoral systems are organized by governments, while non-political elections may take place in business, non-profit organizations and informal organizations. E-voting systems can crash on election day, can lose or scramble votes, or can operate incorrectly. Even minor errors can be catastrophic because a fault in an electronic system has the potential to be systematic and centralized, whereas in manual systems faults tend to be random and localized.

Even minor errors can be catastrophic because a fault in an electronic system has the potential to be systematic and centralized, whereas in manual systems faults tend to be random and localized. Even the world's largest democracies like India, United States still suffer from a flawed electoral system. Vote rigging, hacking of EVM (Electronic voting machine), election manipulation, and polling booth capturing are the major issues in the current voting system.

Many of the studies show that blockchain technology has gained significant impact on the E Voting system. In 1981, David L. Chaum [3] introduced a very first blockchain-based electronic voting system in which the system used public-key cryptography and blind signature theorem. After this first announcement of the blockchain-based voting system, many of the researchers have shown their interests in this particular field. Moreover, most of the study was focused on only electronic records and the online voting system. E-voting system can make life easier to casting vote but on the other hand's threats to these traditional systems have always been a concern. The E-voting system we are going to recommend in this study will deal with the security concerns by using decentralized Blockchain technology and open source code to develop the secure E Voting system.

II. Related Work

G. Rathee et al.[1] introduced a digital voting system based on blockchain that could be implemented in a technologically advanced environment. The system assumes that all the connected external entities are trustworthy. However, the security flaws in system could be a huge risk, as intruders can enter the system to rig the votes. Whereas in our proposed voting system, the use of encryption and secure networks minimize the risk of intruders barging into the votes.

M. Pawlak et al. [2], proposed a system that does not require any operating entities. However, it could not secure a voter's identity, and also required complex computing. The system was able to collect votes from users but due to complex computation, upon higher user rate latency became an issue. The identities of the voters became vulnerable. The system could not compute a large amount of data hence it has failed to be implemented at a large scale. Whereas in our proposed voting system the latency is managed by flexible use of consensus algorithms. The use of cryptographic hash in blockchain omits risk of the vulnerability of a voter's identity.

A proposed system by D. Chaum et al. [3] improved the robustness and fair tallying of votes. End-to-end verification was made possible for voters to assure their count of the vote is integrated. Each voter was able to view if his vote was considered and recorded correctly. The voters were given a unique code that they could enter into the system to verify their vote. Whereas in our proposed voting system the verification of votes has been further simplified. Voters can verify their votes through registered phone numbers and email addresses and also can be verified through their Aadhaar IDs. Verification of votes after the voting activity builds up the trust of voters.

The voting system without polling stations was discussed by P. Mccorry et al. [4]. He suggested that voting through the internet using blockchain can give good results if implemented correctly. They discussed some technical flaws in digital voting systems. The robustness of the system could not be controlled. The error of doubling users gets minimal by using end-to-end verification. These voting systems had low latency and did not secure the privacy of voters. This latency in system is controlled by using a flexible consensus algorithm and smart contracts in the blockchain voting system being proposed.

[5] "Votereum: An Ethereum-Based E-Voting System"- EthVote, on the other hand, is a site-divided app that runs on the Ethereum blockchain and benefits from a smart contract. In this process, only eligible voters are allowed to vote while their identity is unknown. This is achieved by using a Blind Signature when the message is signed unless its content is disclosed and verified as a standard digital signature.

[6] "ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication"- ElectionBlock adheres to the standard principles of central blockchain technology and integrated biometric authentication. Registered voters will have their biometrics registered on the website. will verify that the user is a registered voter, and secondly, will check the blockchain to ensure that the user has not cast a vote. Voting is accelerated using the Merkle Tree algorithm

[7] "Comparative Analysis on E-Voting System Using Blockchain"."FraudResistance"- The system should verify the identity of each potential voter and determine his or her status, but should not allow this information to be associated with their vote. The "Easy to Use" option should work for the whole community. It should be designed in such a way that it can be used with minimal training and some technical skills.

[8] "Securing e-voting based on blockchain in P2P network"- Designed a harmonized model of DLT-based voting records to avoid vote-rigging.Design an ECCbased user verification model to provide authenticity and non-refusal.Design a withdrawal model that allows voters to change their vote before the deadline.

[9] "A Smart Contract For Boardroom Voting with Maximum Voter Privacy" - doped an online voting protocol with separate features and greater voting privacy using Open Vote Network (OVN) .OVN is a smart Ethereum Blockchain contractor. After using the program the creators concluded that it cost $ 0.73 per voter in the program. Researchers soon found that OVN was at risk of being attacked by DOS and traffic jams at the time of purchase.

[10] “Implementation of a Blockchain Enabled E-Voting Application Within IoTOriented Smart Cities”- their approach is a two-pronged approach, namely, both national election bodies and the rest of the organization can ensure security when IoT devices are compromised using the blockchain method. The Blockchain voting system uses not only electoral bodies but also informed voters in case they interfere with their votes before the scheduled counting date.

III. Proposed Framework of Voting System

Blockchain is immutable, unlike other programming structures where an admin can add, delete or update the data. If such a system is used for voting, then anyone having access can tamper with the system and update or delete votes. This is not the case with blockchain technology. Once a node is added to the chain, it cannot be deleted or updated under any condition. If a node is attacked by an intruder, the corresponding node detects it and rebuilds the damaged node, hence the chain becomes immutable.

Online Voting System creates and handles information regarding polling and election so one can permit all citizens to solidify their vote through a web-based platform. Databases which include information and details of residents and applicants who are eligible to vote are maintained by way of the machine.

The software produced will be an online voting system. The main objective of this software is to increase the overall voting %. It will maintain the database of all the eligible citizens and candidates. It will manage all account details of the voters such as citizen name, date of birth, their constituency area, region, state, login id and password of the voter from one central location. The voters cast their votes using the web interface provided.

These votes are accepted by the system on the server. The election system must be openly verifiable and transparent.Keeping the election and vote casting necessities in mind, Online Voting System may be developed with modules: administrator module and user module. Administrator has whole authority over the system to preserve (add, update, alter and delete) information and information of all electorate and applicants. Users, alternatively, can view the list of candidates and see outcomes after the election is finished.

A system architecture is a conceptual model that defines the structure, behavior, and more views of a system. Our architecture consists of devices from which the user will be connected to the backend using the website. Our backend consists of a database and Smart contracts. The voter or user will be authenticated from the database(MongoDB) that is already approved by the administrator. Then the voter can vote, the vote will actually act as a transaction which will be verified by the miners using the Consensus algorithm. If a vote is successfully verified then the new block is added to the Blockchain. And the voteCount will be incremented for the respective candidate. The Administrator will be able to start and stop an election and also will be able to add candidates.

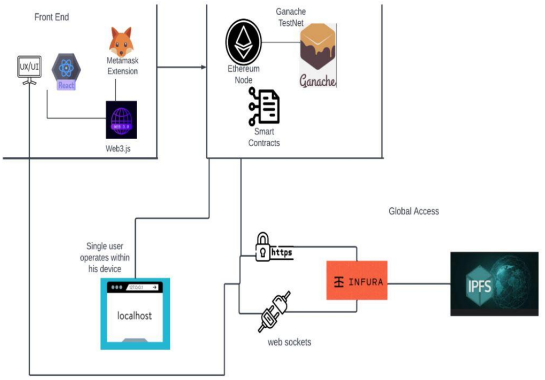

Fig.2. Voting System Architecture

IV. Technical Approach

A. System Implementation Plan

System implementation is done using the waterfall model. The complete system that mainly comprise of following components:

- Metamask
- Smart Contract
- Visual Studio Code
- React Framework
- Ganache
- Login profiles

Will be implemented in a step by step procedure where every member of the team will be working simultaneously on the prescribed path in the SRS document and the main project idea and motivation.

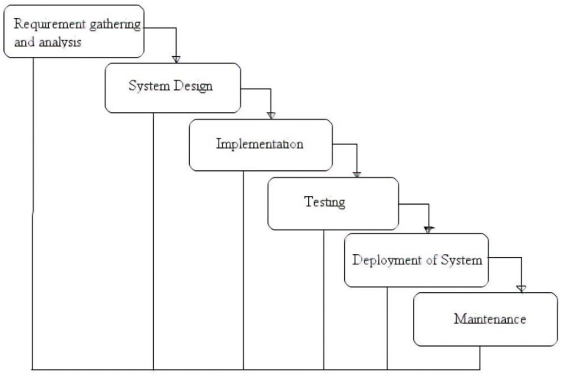

Fig.3. Waterfall Model.

Here in this Project we are going to use the Waterfall model. The Waterfall Model was the first Process Model to be introduced. It is also referred to as a linear-sequential life cycle model. It is very simple to understand and use. In a waterfall model, each phase must be completed before the next phase can begin and there is no overlapping in the phases. The Waterfall model is the earliest SDLC approach that was used for software development.

The waterfall Model illustrates the software development process in a linear sequential flow. This means that any phase in the development process begins only if the previous phase is complete. In this waterfall model, the phases do not overlap..

B. System Requirements

Online Voting System creates and handles information regarding polling and election so one can permit all citizens to solidify their vote through a web-based platform. Through Metamask Login which include information and details of the residents and applicants who are eligible to vote are maintained by way of the machine.
The software produced will be an online voting system. The main objective of this software is to increase the overall voting %. It will maintain the database of all the eligible citizens and candidates. It will manage all the account details of the voters such as citizen name, date of birth, their constituency area, region, state, login id and password of the voter from one central location. The voters cast their votes using the web interface provided.
These votes are accepted by the system. The election system must be openly verifiable and transparent. Keeping the election and vote casting necessities in mind, Online Voting System may be developed with modules: administrator module, user module, View results module. Administrator has the whole authority over the system to preserve (add, update, alter and delete) information and information of all electorate and applicants. Users, alternatively, can view the list of candidates and see outcomes after the election is finished.

Functional requirements of the system is listed below:
Admin panel
Admin will manage all the facts of citizens and candidates.
User Registration
Users/ Voters will sign in themselves within the device in order to forge a vote later using Metamask.
Manage Candidates
It will manage all the applicants that are going to participate in elections.
Manage Parties
It will manage all of the political parties which might be going to participate in elections.
Cast Vote
This characteristic will permit an eligible user to cast a vote.
Tally Vote
It will be counted the entire wide variety of votes cast against each party and display
the result.
Verify Result Integrity
It will check the duplication and mistakes in balloting

User Interfaces

1. Voters - The citizens of the country who are eligible to cast a vote.
2. Register for Online Voting System – Those who already have metamask id, they will register themselves for online voting system and they will use their voter id as their username and separate password will be used for secure authentication.
3. Cast vote – The citizens will cast their votes for their favorite candidates online through a secure system.
4. View own details – The voters will view their own details which they filled up at the time of their registration.

Metamask
MetaMask is a popular cryptocurrency wallet and browser extension that allows users to interact with decentralized applications (dApps) on the Ethereum blockchain. It acts as a bridge between your web browser and the Ethereum network, enabling you to securely store, send, and receive Ethereum and other ERC-20 tokens. MetaMask provides a user-friendly interface for managing digital assets, accessing decentralized exchanges, participating in token sales, and interacting with blockchain-based applications.

Visual Studio Code is a source-code editor that can be used with a variety of programming languages, including Java, JavaScript, Go, Node.js, Python, C++, C. Supports multiple programming languages. So earlier, programmers needed Web-Support: a different editor for different languages, but it has built-in multi-language support. This also means it easily detects if there's any fault or cross-language reference, it'll be able to detect it easily. Traditionally, editors used to support either Windows or Linux or Mac Systems. But Visual Studio Code is cross-platform. So it can work on all three platforms. Also, the code works on all three platforms; else, the open-source and proprietary software codes used to be different. It can detect if any snippet of code is left incomplete. Also, common variable syntaxes and variable

declarations are made automatically. Ex: If a certain variable is being used in the program and the user has forgotten to declare, intelli-sense will declare it for the user. Comes with built-in support for Web applications. So web applications can be built and supported in VSC.

React is a declarative, efficient, and flexible JavaScript library for building user interfaces. ReactJS is an open-source, component-based front end library responsible only for the view layer of the application. It is maintained by Facebook. React uses a declarative paradigm that makes it easier to reason about your application and aims to be both efficient and flexible. It designs simple views for each state in your application, and React will efficiently update and render just the right component when your data changes. The declarative view makes your code more predictable and easier to debug. A React application is made of multiple components, each responsible for rendering a small, reusable piece of HTML. Components can be nested within other components to allow complex applications to be built out of simple building blocks. A component may also maintain an internal state – for example, a TabList component may store a variable corresponding to the currently open tab.

Remix IDE, is a no-setup tool with a GUI for developing smart contracts. Used by experts and beginners alike, Remix will get you going in double time. Remix plays well with other tools, and allows for a simple deployment process to the chain of your choice. Remix is famous for its visual debugger.

Ganache is a development tool and personal Ethereum blockchain that allows developers to create and test decentralized applications (dApps) in a local environment. It provides a simulated blockchain network with a set of predefined accounts, enabling developers to interact with the blockchain without the need for real Ether or connecting to the main Ethereum network.

C. Mathematical Formulation

Models describe our beliefs about how the world functions. In mathematical modeling, we translate those beliefs into the language of mathematics as follows:

Let S be the Blockchain Voting System.

$$S = \{I,O,P,F\}$$

Here,
I = set of all inputs to the system.
I = {I1, I2, I3,I4}
where,
I1 = voter credentials
I2 = Admin credentials
I3 = cast vote
I4 = start or stop election
O = set of all outputs
O = {O1, O2, O3, O4}
where
O1 = voter logs in successfully or fails to login
O2 = Admin logs in successfully or fails to login
O3 = vote increment
O4 = declare result
P = set of all functions
P = {P1, P2, P3, P4}
where
P1 = registers the voter
⇒ if(I1.age > 18) → O1
P2 = verifies the Admin
⇒ f(I2) → O2
P3 = counts the vote
⇒ f(I3) → O3
P4 = declares the result
⇒ if(I4 == stop)→ O4
F = set of the possible failures
F = {F1, F2 }
where
F1 = server timeout failure
F2 = Database failure

V. Results And Discussion

Our E-voting systems present all of the elements of a secure E-voting system including four main parameters [15] such as i) Anonymity, ii) Authentication, iii) Accuracy, iv) Verifiability. The E-Voting system should allow anonymity during and after the election and only listed users can cast their votes. After that vote must be accurate, no duplicate and redundant vote cannot be counted. The main reliability and flexibility of this system is verifiable.

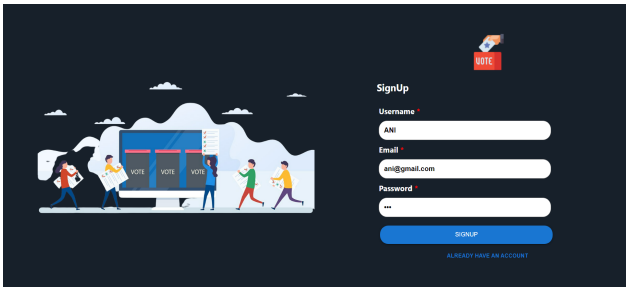

Fig.4. Voters can Login to cast their votes

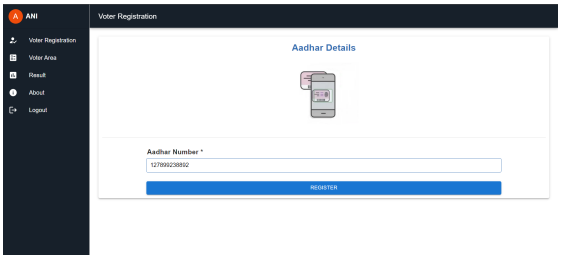

Fig.5. Voters need to register with their Adhar No.

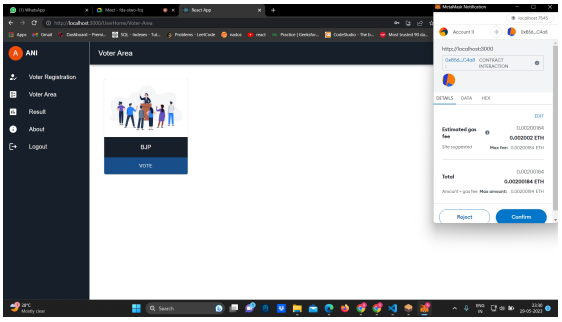

Fig.6. Voters can cast their vote

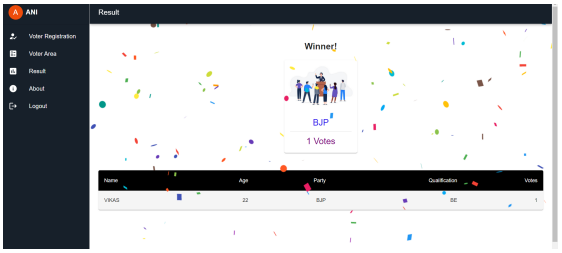

Fig.7. Voters can cast their vote

Figure 7 shows the vote count with who won the voting with their number of votes to the voter.

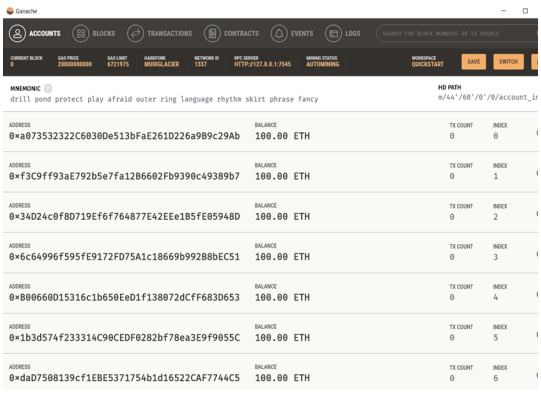

Fig.8. Test accounts of voters in Ganache

We used the test accounts in our application to simulate voters. Import the private keys or configure your development environment to interact with these accounts and perform voting-related operations.

Now, we'll take a look at the administrative side of the application.

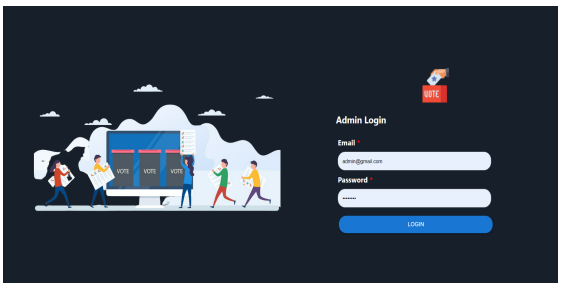

Fig.9. Admins can login

In Figure 9 we can see the page from where Admins can login or register themselves if they have not done it already.

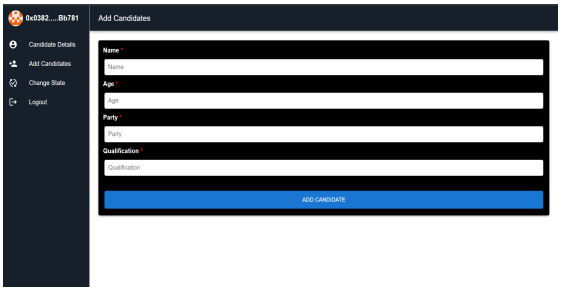

Fig.10. Add candidate module

Figure 10 shows from where the admin can add candidates to the elections

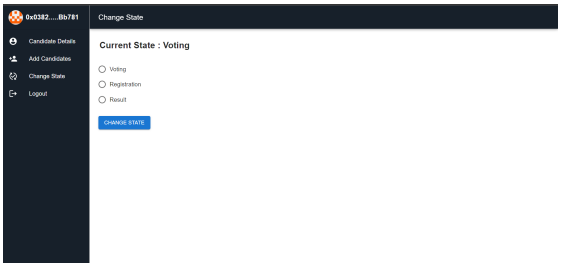

Fig.11. Add candidate module

Figure 11 shows the module from where we can change the state of the election. Our application has three states. Namely:-

1. Voting
2. Registration
3. Result

This system possesses certain limitations as it can be susceptible to malicious attacks, wherein attackers may install harmful software on the voting device. Additionally, voters are restricted to casting their vote only once and are unable to retract it. To summarize, we have emphasized the research trends and challenges associated with the Blockchain-based E-voting system. Presently, we are in the process of developing a real-time application that enables individuals to cast their votes conveniently from any location worldwide.

VI. CONCLUSION

Blockchain technology is relatively a new field and there is a lot exploring remaining to be done to fully grasp its functionalities and capabilities. People associate blockchain with bitcoin and fail to recognise the fact that bitcoin is just an application of the former.

Blockchain can be used in many diverse applications other than just crypto-currencies and improve their functionality. The purpose of this project is to build trust between all parties involved in the voting process. Blockchain based voting will make the process transparent and trustworthy. Large amount of money is spent every election to support the infrastructure, protect its integrity and logistics. Whereas the proposed system achieves the same in a cheaper manner. We are implementing a method to conduct voting on blockchain because it has characteristics like immutability and tamper-proof nature. This research has proposed a framework based on the adjustable blockchain that can apprehend the problems in the polling process, selection of the suitable hash algorithm, selection of adjustments in the blockchain, process of voting data management, and the security and authentication of the voting process. The power of blockchain has been used adjustably to fit into the dynamics of the electronic voting process.

APPENDIX

i) List of Abbreviations

Abbreviations	Description
HTML	Hyper-text Markup Language
CSS	Cascading Style Sheets
GPU	Graphics Processing Unit
SLDC	Software development life cycle
DAP	Decentralized Application

Table1. Abbreviations

REFERENCES

[1] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, ‘‘On the design and implementation of a blockchain enabled E-Voting application within IoToriented smart cities,’’ IEEE Access, vol. 9, pp. 34165–34176, 2021, doi: 10.1109/ACCESS.2021.3061411.

[2]L. V. Thuy, K. Cao-Minh, C. Dang-Le-Bao and T. A. Nguyen, "Votereum: An Ethereum-Based E-Voting System," 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF), 2019, pp.1-6, doi: 10.1109/RIVF.2019.8713661

[3] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora, ‘‘E-voting 40 scantegrity: End-to-end voter verifiable optical-scan voting,’’ IEEE Secur. Privacy, vol. 6, no. 3, pp. 40–46, May 2008. Accessed: Feb. 14, 2021. [Online]. Available: https://www.computer.org/security/

[4] D. L. Chaum and D. L., ―Untraceable electronic mail, return addresses, and digital pseudonyms,‖ Commun. ACM, vol. 24, no. 2, pp. 84–90, Feb. 1981.

[5] P. McCorry, S. Shahandashti, and F. Hao, ‘‘A smart contract for boardroom voting with maximum voter privacy,’’ in Financial Cryptography and Data Security. Sliema, Malta: Springer, 2017, pp. 357–375, doi: 10.1007/978-3-319-70972-7_20.

[6] Vairam T1,Sarathambekai S2, Balaji R3 “Blockchain based Voting system in Local Network”,2021 7th International Conference on Advanced Computing & Communication Systems (ICACCS)

[7] Divya Rathore ,Virender Ranga “Secure Remote E-Voting using Blockchain” Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021) IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2

[8] F. P. Hjálmarsson, G. K. Hreiòarsson, M. Hamdaqa, and G. Hjálmtýsson, ‘‘Blockchain-based E-Voting system,’’ in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 983–986.

[9] S K Geetha,” A Secure Digital E-Voting Using Blockchain Technology”, 2021 J. Phys.: Conf. Ser. 1916 012197

[10] Mukammad Shoaib Farooq, Usman Iftikhar, Adel Khelifi “A Framework to Make Voting System Transparent Using Blockchain Technology”, date of publication June 3, 2022