

E-Voting Using Blockchain Technology

**Prof. Jyoti Nandimath¹, Dhairyasheel Bhosale²,
Vaibhav Shankar Khiste³, Shubham Krushna Solanke⁴,
Smit Sanjay Vachhani⁵**

^{1,2,3,4,5}Information Technology Dept. MIT ADT UNIVERSITY, Pune

Abstract:

Voting in a democratic manner is extremely important in all countries. However, there are problems with transparency, low voter turnout, and security with conventional voting techniques such as ballot papers and electronic voting machines. The adoption of digital voting systems depends on security, which guarantees defense against data breaches and cyberattacks, particularly during crucial decision-making processes. A viable solution is provided by blockchain technology, which delivers unmatched security and transparency. Voter trust may be increased and votes can be protected from tampering thanks to its decentralized structure and encryption protocols. Through the utilization of blockchain technology, countries can bring their voting procedures up to date, promoting openness and integrity in democratic elections while resolving long-standing issues with security.

Keywords: E-voting, Smart-contracts, Blockchain, Ethereum

INTRODUCTION

Since the emergence of Bitcoin as the first widely accepted cryptocurrency in daily life, blockchain technology has shone like a star and gained immense popularity in the software industry today. The roots of blockchain technology can be traced back to the fundamental architectural design of Bitcoin, which was first made public on the internet. With its high degree of system transparency, blockchain technology has quickly gained popularity and is being actively researched for its possible applications in other fields.

The world can be clearly and momentarily followed. In this peer-to-peer (P2P) system, no central authority is required for approval or system completion.

This decentralized chain may safely store many kinds of structured data together with financial transactions by using cryptographic techniques. With the right modifications, a variety of data categories, such as assets, marriage licenses, bank records, and medical data, can all be safely maintained. Ethereum presents Ether, a cryptocurrency with flexible development parameters, in line with Bitcoin. Ethereum sets itself apart by demonstrating how blockchain technology may make the development of data management tools easier. Smart contracts make sure that unauthorized changes are blocked once these software programs are registered on the blockchain, making them unchangeable.

Blockchain is a series of blocks, which are realized "point-to-point" completion or "distributed" transactions. Once completed, the blocks are added to the blockchain in a chronological, linear order.

"Block 0" or "Genesis block" refers to the first block in a blockchain. The genesis block is different

from other blocks because it is usually hardcoded into the software and does not make reference to any previous blocks. After the genesis block is created, "Block 1" is generated and added to it when it's finished. There is a part of each block devoted to transaction data. Each transaction's copies are hashed, and the hashes are repeatedly paired and hashed. This procedure continues until there is only one hash left, which is called the Merkle root.

To maintain transaction immutability, the Merkle root is contained in the block header, and each block stores the header of the one before it. Modifying data requires changing the chain as a whole, highlighting how unchangeable the blockchain is. Blockchain access is made possible by peer-to-peer networks, in which nodes trade blocks and transactions. Peers quickly spread information about other peers as they join the network, promoting decentralized peer discovery. New nodes download their first block before starting the validation process, allowing network nodes to verify newly mined blocks and unconfirmed transactions. The validation procedure starts with this first block download.

After downloading and validating every block from block 1 to the most recent blockchain, the new node is said to have synchronized.

For initiatives involving electronic voting, blockchain offers a viable alternative. A lot of work is being done on e-voting, and many of the solutions are being tested and put into temporary use. Only a small number of these solutions, nevertheless, show the dependability required to support continued use. Even while online surveys and polls are widely used, corporations' and governments' online elections do not enjoy the same degree of confidence. The primary cause of this discrepancy is the essential function that official elections and democratic government perform in contemporary cultures.

Furthermore, a transparent and private electoral process is highly prized in democratic cultures. People (and members of organizations) make a lot of decisions these days[2].

Many questions are raised about the transparency and dependability of the current voting method. There are concerns about the system's integrity, the potential for vote tampering before the count, and strategies for maintaining openness. This study investigates and recommends a web application that uses blockchain technology and is installed on the Ethereum server via smart contracts in order to respond to such questions. The study is divided into two sections: the first explores the use of electronic voting systems as they exist now, and the second part looks closely at the limits of those systems.

MOTIVATION AND RELATED WORKS

Our main objective in this project is to provide a safe space for voting and demonstrate the practicality of a trustworthy electronic voting system that makes use of blockchain technology. By providing ubiquitous access to electronic voting through everyday devices like computers and smartphones, we hope to enable everyone to participate in administrative decision-making procedures. This improved accessibility has the potential to promote true direct democracy in addition to increasing the transparency of public opinions and making them easier for administrators and policymakers to obtain. This endeavor is especially important because elections are susceptible to fraud, especially in smaller towns and areas where corruption is prevalent. Election integrity is a severe concern, even in bigger urban areas within such situations. Moreover, traditional elections, particularly on a large scale with numerous geographically dispersed voting centers and millions of voters, incur substantial long-term costs. Additionally, voter turnout at traditional voting centers

is often low due to logistical challenges such as individuals being away from their registered address or engaged in other commitments. E-voting has the potential to address these issues if implemented with careful consideration. It is noteworthy that while the concept of e-voting predates blockchain technology, previous implementations have predominantly relied on centralized computation and storage models.

Under the leadership of its government, Estonia has been a leader in the construction of a sophisticated electronic voting system. Early talks about the voyage started in 2001, and in 2003 national officials formally implemented it. Ever since, Estonia's electronic voting system has experienced constant improvement, making it a stable and dependable platform today. Smart digital ID cards and personal card readers, which the government provides for safe individual verification, are essential to its operation. Anyone with a computer, internet connection, and ID card can conveniently participate in elections by accessing candidate listings and casting their ballots through a specialized web portal and desktop program.

Through rahvaalgatus.ee, citizens in Estonia have the ability to digitally propose laws and support petitions using smart ID cards. Proposals are debated in parliament after they receive a certain number of signatures, strengthening democratic procedures. Even though approximately 30% of voters participated, there are still restrictions. Data integrity is at risk because to the centralized system's susceptibility to hacking, denial-of-service assaults, and possible abuse by administrators. Scalability issues surface, which may make adaptation more difficult in bigger populations. Furthermore, certain voters may find it difficult to get voting materials due to the manufacture and distribution costs associated with ID card use.

Known for its strong democratic principles, Switzerland was one of the first countries to use computerized voting. Every Swiss citizen who turns 18 can take part in elections on a variety of themes, either actively or passively, provided they pledge to be inclusive. The nation has formally started working on creating remote voting technologies. Notably, Swiss company Agora was given the task of tallying votes in two districts during the general election held in Sierra Leone in March 2018. This demonstrates Switzerland's forward-thinking embrace of technical innovations to improve democratic processes and demonstrates its commitment to guaranteeing broad participation and openness in elections.

Accredited observers manually entered about 400,000 votes onto Agora's blockchain system after the voting process. Votes were validated using blockchain technology, but it was not the only source of authority in this instance. The method, which reflects a cautious incorporation of technology into voting procedures, combines the verification dependability of blockchain technology with manual input. It represents a stage of transition towards utilizing blockchain's transparency and integrity possibilities for voting processes. This emphasizes how crucial it is to accept new technology gradually and with steps to foster confidence. Since December 2017, great progress has been achieved in integrating blockchain technology for voting purposes under Moscow's Active Citizen program. The public auditability and transparency of the voting results have improved as a result of this change. By utilizing blockchain technology, every topic that is debated by the community and put to a vote is easily incorporated into the electronic voting system. The voting process's outcomes are then recorded on a ledger, which also acts as a repository for all earlier surveys [10].

On the other hand, websites such as <http://www.strawpoll.me/> provide an easy-to-use interface and convenient ways for users to create and join polls. Nevertheless, they mostly rely on user confidence

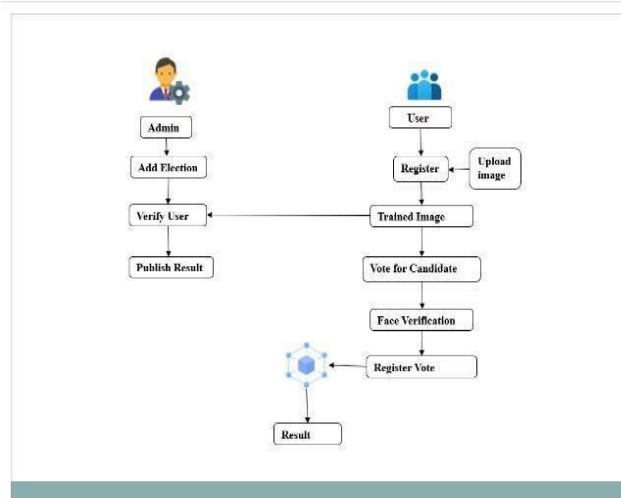
and lack strong security safeguards. As a result, because of their limitations, these platforms might not be appropriate for important decision-making procedures, including choosing department chairs.

This paper presents a novel system that incorporates the blockchain paradigm into the e-voting process, resulting in a practical and versatile e-voting protocol devoid of a Trusted Third Party (TTP). Our proposed protocol offers a secure and adaptable voting mechanism that meets nearly all essential criteria for an e-voting system, thereby enhancing the efficacy of organized elections.

IMPLEMENTATION AND DISCUSSION

We outline the application's design and operation phases in this section. Visitors begin their interaction with the platform by visiting the online application that is housed on our system. From there, they register and transparently cast their votes in a secure manner.

1. **Registration Phase:** The voter initiates the process by providing unique identity details such as name, roll number, and cellphone number, which are subsequently recorded in the database.
2. **Login:** The voter uses their password to log in after finishing the registration process. The voter goes through authentication after successfully logging in, which includes OTP verification to improve real-time security.
3. **Blockchain Technology:** The security features of blockchain technology are what make it most useful. By encrypting voter messages (cast votes) using asymmetric encryption methods, it ensures a safe and open environment. In this model, the host holds onto the private key, and the blockchain provides a public key for verification.
4. **Database:** User information, which includes attributes like name, gender, and unique ID, is kept in the database. The database management system selected to meet this need is MySQL, which is advised.
5. **Ethereum Network:** The foundation for creating and storing blockchain data is the Ethereum network. Every block in this network is made up of encrypted data that is dispersed among nodes to increase fault tolerance.
6. **Result Phase:** The votes are processed and totaled during this stage. The result is then produced and shown on the website, allowing users to utilize their unique public keys to verify the validity of their votes. The voting system's transparency is ensured by this procedure.



The application adheres to the Model-View-Controller (MVC) architectural pattern, a widely adopted and structured approach. This architectural design divides the application into three primary logical

components: the model, the view, and the controller.

- The view serves as the interface via which end users interact with the application; it is located at the top layer of the application architecture. It offers customers a number of features, including the ability to click buttons, enter data, access the camera, choose radio buttons, upload music, and more. The main duty of this layer is to show the user the data, in full or in part, as needed by the functionality of the program. Additionally, the view facilitates easy communication and interaction by acting as a bridge between the user and the application. It guarantees that users can carry out required tasks, get feedback when needed, and traverse the program with ease. By offering a responsive and user-friendly interface, the view layer significantly contributes to improving user pleasure and experience.
- The controller is the layer in the application architecture that sits in the middle and contains the program's basic functionality and business logic. It processes user interactions and arranges the proper replies, serving as a bridge between the view layer and the underlying data model. This layer is in charge of all background operations, including managing vote-casting and login processes. For example, when a user starts the login process, the controller checks and authenticates the user, granting access to the relevant resources according to their permissions. Comparably, the controller supervises the verification of user inputs, guarantees the reliability of the voting system, and safely records the votes throughout the voting process. The application achieves modularity through the centralization of the business logic within the controller.
- Model: The model layer is tasked with managing and storing user data. In this architecture, the relational database MySQL is employed to store and organize user information.

In our application, users must possess an account with a wallet address and a certain amount of Ether, which is Ethereum's cryptocurrency, to cast their vote.

In order to cast a vote on the blockchain, users must pay a small transaction charge known as "gas" when they join the network. Network miners are paid with this charge in exchange for handling the transaction. Candidate lists are accessible for free, however voting costs Ether. This is due to the fact that while retrieving data is free, putting data to the blockchain—such as casting votes—requires processing resources and is therefore subject to costs. The distinction is indicative of the blockchain's business model, which charges users for acts that entail writing data but usually doesn't charge for accessing already-written data. This pricing mechanism rewards miners and discourages pointless transactions, which promotes network security and sustainability.

We use the Ethereum Virtual Machine (EVM) on the Ethereum blockchain to create our application, which allows for direct code execution via smart contracts. The foundation for reading and publishing data to the blockchain and carrying out essential logic is provided by smart contracts. Solidity, the preferred programming language for Ethereum smart contracts, is used to create these contracts. In essence, we think of the blockchain's public ledger as the database layer, and smart contracts as the user interface for accessing and manipulating data. Our programme provides a decentralised and immutable database architecture by using smart contracts and Solidity, which guarantees security, trust, and transparency in data transactions on the blockchain.

Without a doubt, smart contracts serve as the main hub for all business logic interacting with data held on blockchains. These contracts serve as a legally binding covenant within our program, ensuring the validity of every user's vote, avoiding duplicate votes, and selecting the winner based on the candidate who receives the most votes. The fairness and integrity of our system's voting procedure are protected by this agreement.

Installing all necessary dependencies is the initial step in developing our application. Next, we write our contract and successfully launch it onto the blockchain. First, the contract must be declared using the "contract" keyword, and then the selected contract name must be specified. Next, we create a state variable that will eventually carry the candidate's name. We can reliably record data onto the blockchain thanks to these state variables. Moreover, the constructor function is called each time the contract is deployed.

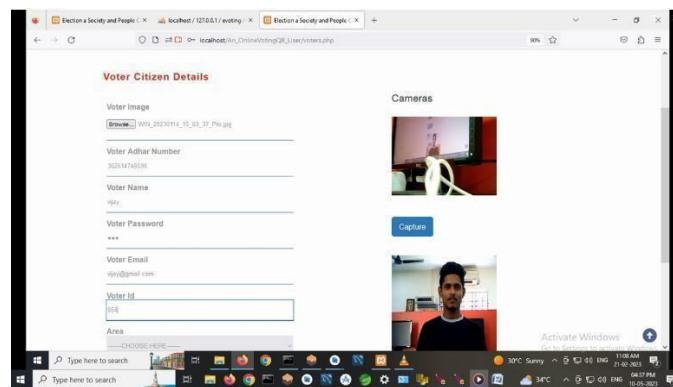
We have defined the struct "candidate" with attributes including an id of unsigned integer type, a name of string type, and a vote count of unsigned integer type. To store instances of these structs, we utilize Solidity mapping, which functions akin to an associative array or hash, establishing associations between key-value pairs.

```
Mapping(unit => Candidate) public candidates;
```

In this case, the value relates to the Candidate structure type, and the mapping's primary is an unsigned integer. The mapping's visibility is set to public so that a getter function can access it. Throughout the contract code, there is a mapping in addition to a method for adding candidates, which are all contained in a smart contract called "contract election".

We developed the client-side application that communicates with our smart contract after setting up the server-side application. JavaScript and HTML were used in the front end's construction. In addition to the conventional unique ID and password authentication technique, we included a new unique feature—the One-Time Password (OTP) feature—to strengthen system security. After entering their cellphone number, users will receive an OTP for verification. After that, the OTP verification method is used by the system to authenticate the user.

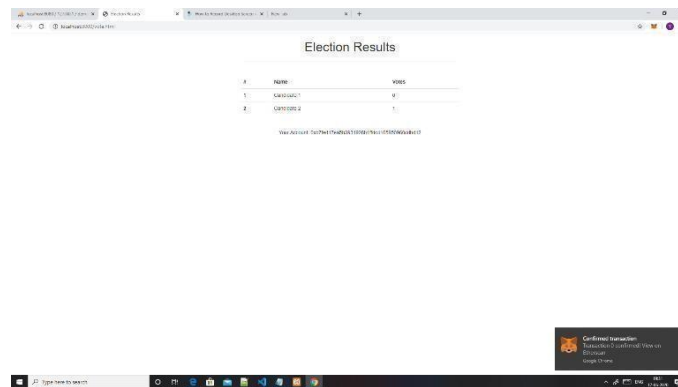
Logging into the blockchain is the next step after creating the webpage. We import one of the accounts from Ganache, a dependency that gives us ten accounts with their account addresses and simulated ethers, into MetaMask in order to connect to the blockchain. In order to use the Ethereum blockchain, you must install a specialised browser extension, like MetaMask. With the help of this plugin, we can communicate with the Ethereum blockchain easily. After a successful connection, we may communicate with our smart contract and access account and contract data.



In the next stage of development, we included the ability to vote in the elections through the use of a smart contract. We defined a mapping in the smart contract called "voters" to keep track of the accounts that have cast ballots. We also included a 'vote' function that takes in one input, which is the ID of the candidate. This function completes a number of crucial duties, including confirming that the user has never voted before, confirming the legitimacy of the candidate, logging the user's vote, and updating the vote total for the relevant candidate. The code snippet and mapping used to cast votes are shown in Figure 9. This method guarantees integrity and transparency in the blockchain platform's voting

procedure.

When a user votes, they pay a transaction fee in gas, which is then given to the miner or node that handles the transaction's processing and recording on the blockchain. As soon as votes are cast successfully, the outcomes are shown. The election process is essentially over when the candidate with the most votes is proclaimed the victor. This method guarantees the election process's immutability, security, and transparency because all voting activities and outcomes are kept on the blockchain and made available to all parties involved.



#	NAME	VOTES
1.	CANDIDATE 1	97
2.	CANDIDATE 2	1

Screenshot of an Election results

After votes are cast successfully, it displays the election results. It also displays the vote-casting transaction's entry into the blockchain, including information such as the transaction hash, the number of blocks generated up to that point, the contract address, the timestamp, the related account, the transaction block number, the amount of gas used, and the total amount spent during voting process.

Our primary focus in this research is on small-scale elections and polls, including college elections. Managing more extensive voting scenarios with millions of voters could provide unique difficulties. More research is necessary to determine whether the Ethereum network can scale. As a result, we refrain from promoting the use of these contracts for national elections, at least not just yet.

One issue that blockchain-based electronic voting systems frequently confront is preserving voter anonymity while guaranteeing voting process transparency in our voting application. At the moment, every transaction—including votes and financial transfers—is publicly documented in the blockchain's blocks. Voter privacy is compromised because anyone having access to the chain can examine transactions. This restriction is a major obstacle, particularly for important or official elections. Research efforts are still facing a significant issue in addressing this anonymity risk. In their work, Hao et al. suggested a method based on the Diffie-Hellman procedure, which makes use of random integers and public/private key pairs. Their strategy seeks to allow for a "two-round" referendum while maintaining some degree of ballot privacy.

CONCLUSION

In this paper, we have presented a novel electronic voting system leveraging blockchain technology and smart contracts. Our system ensures secure and cost-efficient elections while safeguarding voter privacy. In contrast to previous approaches, we have demonstrated that blockchain technology provides democratic nations with an opportunity to transition from traditional pen-and-paper election methods to a more efficient and secure electoral system. Additionally, our system enhances transparency and introduces new possibilities for electoral processes.

E-voting is still a contentious issue in scientific and political circles. While there are a few successful

examples, many attempts have failed to provide the security and privacy elements that are essential for traditional elections, while others encounter issues with scalability and usability. On the other hand, blockchain-based e-voting solutions, such as the one we've developed utilizing Ethereum and smart contracts, present viable ways to overcome most security issues, or at least potentially address them with appropriate modifications. These include maintaining vote integrity and non-repudiation, protecting voter privacy, and enhancing counting process openness. But other features, like voter authentication at the individual level (beyond account level), call for extra steps, such as adding biometric factors.

Although blockchain technology has a lot of potential, more study and development are needed to fully realize this potential at this time. Enhancing the fundamental features of blockchain technology is necessary, particularly to accommodate more complex applications. This means that in order to overcome current limitations and fully utilize blockchain technology, research and development must work together in a concerted effort.

REFERENCES

1. S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system",
2. A. K. Koç, E. Yavuz, U. C. Çabuk, G. Dalkılıç, "Towards Secure E-Voting Using Ethereum Blockchain".
3. G. Wood, "Ethereum: a secure decentralized generalized transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.
4. C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: foundations, design landscape, and research directions", Mar 2017, arXiv:1608.00771.
5. E. Maaten, "Towards remote e-voting: Estonian case", Electronic Voting in Europe-Technology, Law, Politics and Society, vol. 47, pp. 83-100, 2004.
6. U. C. Çabuk, A. Çavdar, and E. Demir, "E-Demokrasi: Yeni Nesil Doğrudan Demokrasi ve Türkiye'deki Uygulanabilirliği", [Online] Available: Democracy_The_Next_Generation_Direct_Democracy_and_Applicability_in_Turkey/links/5818a6d408-an-ee7cdc685b40b/E-Democracy-The-Next-Generation-DirectDemocracy-and-Applicability-in-Turkey.pdf.
7. "Final report: a study on eGovernment and the reduction of administrative burden (SMART 2012/0061)", 2014, [Online]. Available: <https://ec.europa.eu/digital-single-market/en/news/finalreport-study-egovernment-and-reduction-administrative-burdensmart-20120061>.
8. F. Hao and P. Y. A. Ryan, Real-World Electronic Voting: Design, Analysis and Deployment, CRC Press, pp. 143-170, 2017.
9. N. Braun, S. F. Chancellery, and B. West. "E-Voting: Switzerland's projects and their legal framework–In a European context", Electronic Voting in Europe: Technology, Law, Politics and Society. Gesellschaft für Informatik, Bonn, pp.43-52, 2004.
10. N. Kshetri, J. Voas, "Blockchain-Enabled E-Voting".
11. P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy", International Conference on Financial Cryptography and Data Security. Springer, Cham, pp. 357-375, 2017.
12. U. C. Çabuk, T. Şenocak, E. Demir, and A. Çavdar, "A Proposal on initial remote user enrollment

for IVR-based voice authentication systems”, Int. J. of Advanced Research in Computer and Communication Engineering, vol 6, pp.118-123, July 2017.

13. Y. Takabatake, D. Kotani, and Y. Okabe, “An anonymous distributed electronic voting system using Zerocoin“, IEICE Technical Report, pp. 127-131, 2016.