



Smart Contracts Based Decentralized Digital Voting System Using Blockchain Technology

Mohammed Abdul Waheed¹, Tabassum Mahenaaz², Zohara Begum³

¹ Professor, Department of Computer Science and Engineering, VTU, CPGS, Kalaburagi, Karnataka, India

² Student, Department of Computer Science and Engineering, VTU, CPGS, Kalaburagi, Karnataka, India

³ Assistant Professor, Department of Electronics & Communication Engineering, VTU, CPGS, Kalaburagi, Karnataka, India

Email: ¹ dr.mawaheed@gmail.com, ² tabbunaaz5@gmail.com, ³ zohra1@kbn.university

Abstract

The fundamental objective of this project is creating blockchain-based electronic voting system which is transparent and safer. Wider adoption has challenges, notably in terms of resilience. Elections using conventional centralized systems have security and transparency problems, including a lack of database control and susceptibility to meddling. With blockchain technology, numerous users can access the same database through a decentralized system. As a result, a network structure with built-in security measures is produced, utilizing the principles of consensus, decentralization, and encryption to guarantee transaction confidence. Every member of the network has a set of private keys that function as a unique digital signature for each transaction. This intends to make voting secure, transparent, and accessible to everyone, wherever they may be.

Keywords: Blockchain, voting, cryptographic foundations, digital signature, voter, planet, encryption.

1. Introduction

Blockchain technology emerged with the rise of Bitcoin and has gained significant attention in the software industry [2]. It is an open distributed ledger composed of interconnected digital blocks. Initially designed for digital currency transactions, blockchain has expanded to include various applications [4]. Several types of blockchains exist based on their purpose and characteristics, such as public, private, and consortium blockchains. The key motivation for utilizing blockchain is its features of decentralization, transparency, and immutability. It efficiently stores digital transactions between parties in a distributed ledger. Transactions are organized into blocks, forming an unchangeable chain that can be endlessly verified. Modifying blocks requires consensus from over half of the network's users. The first block, known as the 'Genesis block,' is unique as it does not reference prior blocks and is typically hardcoded into the software [5]. Subsequent blocks are attached with Genesis block, with every block containing section for transaction information. Every transaction copies are hashed & paired until a single hash, the Merkle root, remains. In Blockchain 1.0, a block comprises header & body. Header includes fields like block version, Merkle root hash, timestamp, nBits (minimum valid block hash size), nonce (mathematical value for hash

calculation), and parent block hash. The body stores transactions and transaction counters. The block's capacity for storing transactions is deliberated by its size & each transaction size. Hashing is employed to protect data integrity, generating a unique fixed-sized value for each input. Hash functions are one-way, preventing the derivation of original data from the output. This secure method ensures data integrity protection [17].

2. Related Work

Prof. Mrunal Pathak, et.al (2021) [1], Developing a reliable voting system that allows for complete anonymity of voters and content while also producing accurate results has proven difficult. Electronic voting is a modern method that uses a safe and tamper-proof mechanism to cast votes. Since blockchain is a distributed ledger and its users collectively control the system, it may serve as the foundation for a trustworthy voting infrastructure.

Abishek Yadav, Ashish Uttamrao, Yash Urade [2], July-2020. In all democracies, voting by paper ballot or electronic voting machine is a very significant and serious event. This article presents development and testing of a simple electronic voting application written in Solidity programming language & deployed upon Ethereum blockchain. To prevent users from casting duplicate votes, a finite supply of tokens (gas) is issued to each wallet and consumed whenever user casts a vote. This article presents a realistic system by displaying a webapp for voting & its limits, as well as discussing the benefits and drawbacks of employing blockchain technology.

Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson [3] (2019) There has been a long-standing need for safe Electronic Voting Machine (EVM) which retains impartiality & privacy of existing voting schemes while also taking use of transparency & adaptability of electronic systems. This draft paper aims to.

3. Proposed System

By using blockchain technology, we can make the voting process more trustworthy, safe, transparent, & immutable. How the system functions: Let's say you're a registered voter who just went to the polls to use an EVM [6]. Nonetheless, it is still circuit, so if microchip is tampered with, you might never know whether or not your vote was counted for candidate you intended.

Since votes can't be traced back to an individual. However, the blockchain records everything as transaction, and thus it offers you receipt for your vote (as transaction ID) that you can utilise for verifying your ballot was properly tallied [7-9].

Scenario 2: Someone attempts to hack or spy on digital voting system (website/app) established to digitalize process & finds out as all private data is saved upon single admin server/machine, at which point the vote total for candidate A may be changed from 2 to 22. If a hacker secretly installs malware on your device, clickjacks your browser, or assaults the central server, you may never find out.

By using blockchain technology, unique trait called as immutability which protects system against this. Think about standard database management systems like SQL and PHP. Votes may be added, changed, or removed. Data on a blockchain, however, can only be added to; it cannot be altered or removed [11-13]. So, everything you put remains permanently and cannot be changed. Denote this record as the immutable ledger. However, just creating a blockchain system is insufficient. It must be decentralized so that if one server is down or node is compromised, the rest of the network can continue to operate properly.

Advantages of blockchain based voting are as follows:

- Voters could participate anytime and from anywhere, especially in events epidemics like COVID-19 when physical elections are challenging.
- The use of blockchain ensures a secure voting process, reducing the risk of fraud or tampering.
- Once recorded on the blockchain, votes are immutable, providing a permanent and transparent record.
- Faster and more efficient vote counting and result verification.
- Transparency in the voting process, allowing participants to verify and audit the results.

4. System Architecture

To cast a ballot, a voter must provide the information shown in the above diagram. After then, everything is encrypted and filed away as a deal. Every node in network receives copy of this transaction & verifies it. If the network consents to the transaction, it will be included in the next available block on the ledger [16]. It is important to remember that a block can never be modified after it has been put to the chain. Users may now see outcomes and audit past transactions if they so want. Considering the security concerns of today's voters, it is imperative that a new voting system be developed that improves upon the existing ones in these respects [10]. So, Blockchain technology is used in voting systems to increase security, make voting more convenient (people may cast their ballots at any time, from any location), and cheaper.

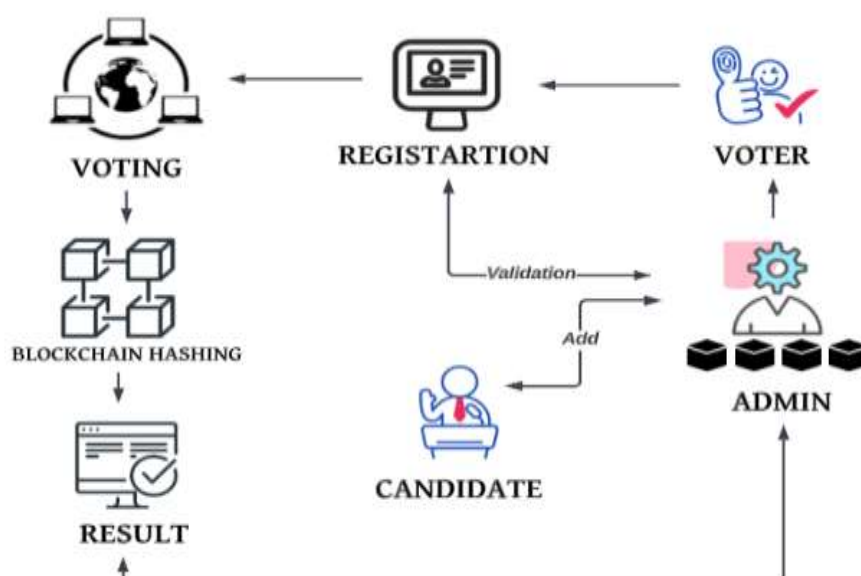
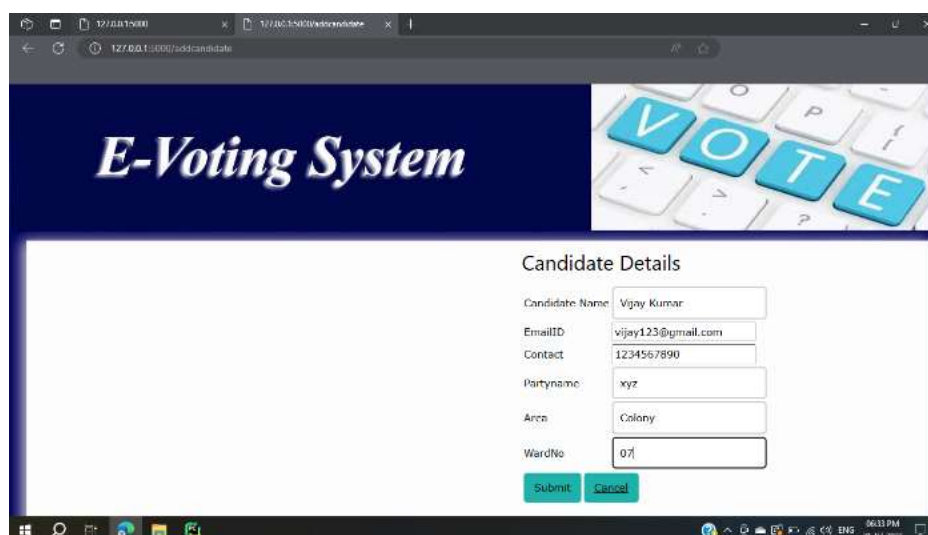


Fig. 1. System Architecture

5. Methodology

A. Candidate Registration

Register the candidate with all credentials and details such as candidate name, e-mail ID, contact, party name, area, and ward number and submit as shown in the following figure.

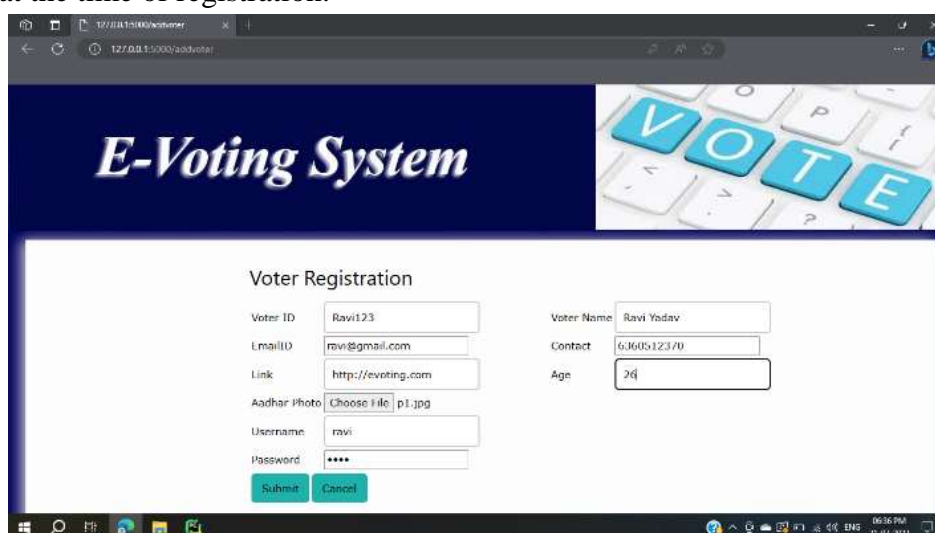


The screenshot shows a web browser window with the URL `127.0.0.1:3000/addcandidate`. The page features a dark blue header with the text "E-Voting System" in white, italicized font. To the right of the header is a keyboard graphic with the word "VOTE" highlighted in blue. Below the header is a white form titled "Candidate Details". The form contains the following fields: Candidate Name (Vijay Kumar), EmailID (vijay123@gmail.com), Contact (1234567890), Partyname (xyz), Area (Colony), and WardNo (07). At the bottom of the form are two buttons: "Submit" and "Cancel".

Fig. 2. Candidate registration

B. Voter Registration

The proposed system used registration website as for the users to register themselves. The website collects details like name, e-mail, phone number, Aadhar number of the voter at the time of registration. These details are collected from the user and stored in the database. After successful completion of voter registration, the user is sent a confirmation mail to the e-mail provided at the time of registration.



The screenshot shows a web browser window with the URL `127.0.0.1:3000/addvoter`. The page features a dark blue header with the text "E-Voting System" in white, italicized font. To the right of the header is a keyboard graphic with the word "VOTE" highlighted in blue. Below the header is a white form titled "Voter Registration". The form contains the following fields: Voter ID (Ravi123), Voter Name (Ravi Yadav), EmailID (ravi@gmail.com), Contact (6360512370), Link (http://evoting.com), Age (24), Aadhar Photo (Choose file p1.jpg), Username (ravi), and Password (****). At the bottom of the form are two buttons: "Submit" and "Cancel".

Fig. 3. Voter registration

C. Authentication

Once the details are collected from the user the next step is the authentication process. Aadhar verification is done either by uploading the Aadhar photocopy or the website has a provision for taking the photo at the time of registration. After successful verification, the user is provided with the blockchain account address and private key. User must keep these details intact and protected.

D. Voting Portal

The voter logs into the website using their unique Blockchain account. This page will be redirected to the vote casting page where parties are displayed, the voter will cast their vote to a specific party.

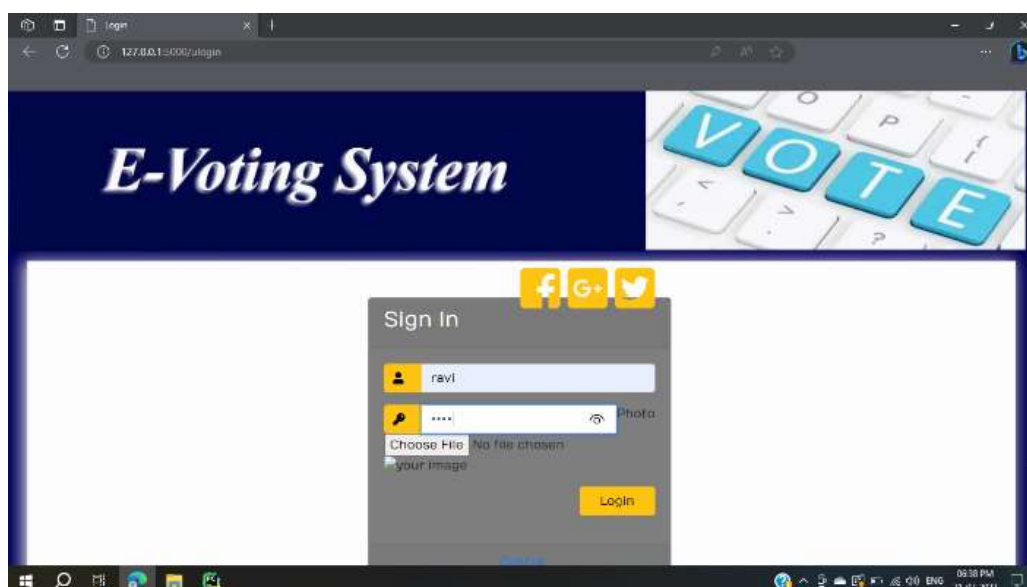


Fig. 4. Voter Sign in

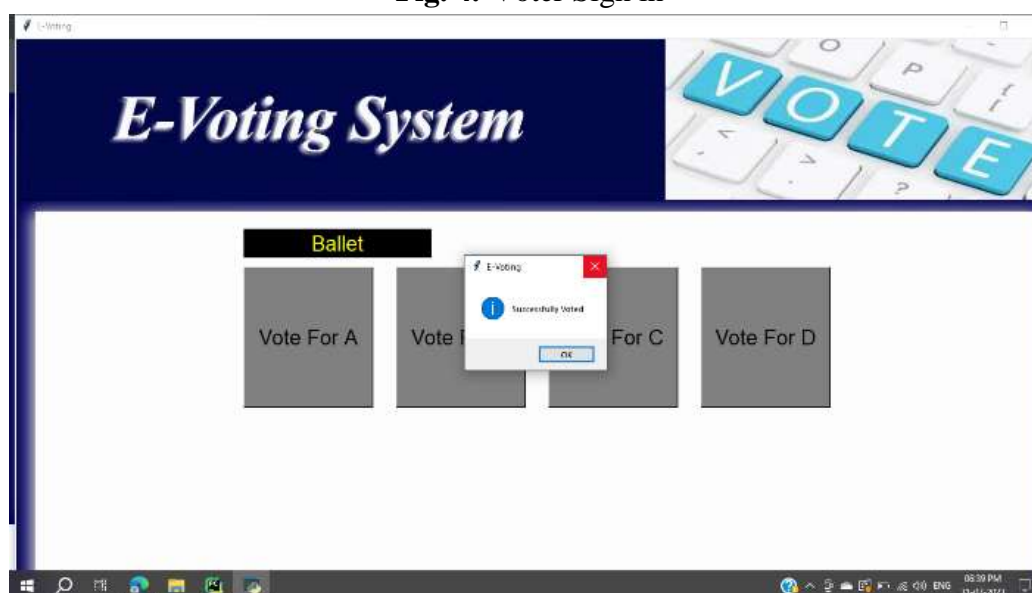


Fig. 5. Voting

E. Voting Transaction

The next step is the casting of vote by the user. The voter logs into the e-voting website by entering the login credentials, the blockchain account which was given to the user after the authentication process was complete. The home page displays the candidates and parties of the election. The voters select the party they want to cast their vote for. Once the user casts his vote the page connects to the Meta mask, a local blockchain environment where the voter can confirm their vote transaction.

F. Result Validation

The next step is the result validation process. The result is computed using JavaScript function. The vote is incrementally added to the data as it is cast. Once all the voters complete casting their vote the JavaScript function computes the overall result, and the result is displayed in the page.

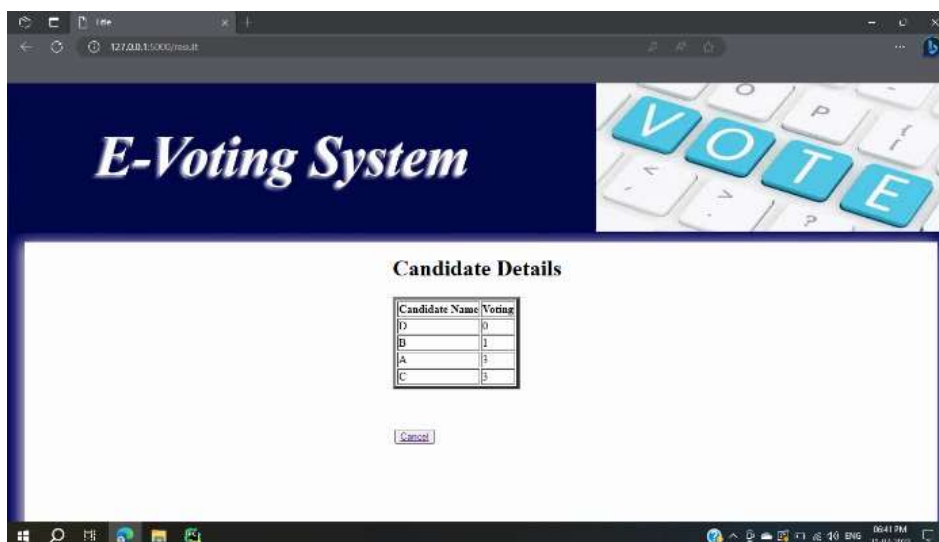


Fig. 6. Voting result

G. Result Validation

Once the voter is voted, he cannot cast his vote next time because of the blockchain transaction, there is a gas limit set for each transaction once the user finishes the gas limit, he can't cast another vote. The gas limit is set as such only one vote can be casted for one cast.

6. Conclusion

This safe, low-cost, and anonymous electronic voting system is built on the Blockchain and runs on smart contracts. Blockchain technology offers democratic countries a novel opportunity to transition from traditional paper-based election systems to a more efficient and cost-effective alternative [14]. This technological advancement not only enhances security measures of existing system but also showcases potential for increased transparency. Electronic voting is still widely debated topic in both political and academic communities. Although there are several great examples—the most majority of which are still in use—many other efforts fell short in either providing security & privacy features of standard elections or in being usable and scalable enough to be widely adopted. However, blockchain-based e-voting systems, such as those that use smart contracts and the Ethereum network, solve almost all of the security concerns, including those related to voter privacy, integrity, vote verification and non-repudiation, and counting transparency [15]. However, the blockchain is not able to solve every problem; authentication, for example, has to be combined with additional techniques like biometric factors and digital signatures for use in real time. Blockchain technology offers promising applications, but much more study is required before it can be fully developed. The blockchain's basic technology needs concerted work to make it suitable for more complex uses.

References

- [1] Prof. Mrunal Pathak , Amol Suradkar , Ajinkya Kadam , Akansha Ghodeswar , Prashant Parde's "Blockchain Based EVoting System"-International Journal of Scientific Research in Science and Technology (2021).
- [2] Abishek Yadav, Ashish Uttamrao, Yash Urade "E-Voting using Blockchain Technology" International Journal of Engineering Research & Technology, July-2020.

- [3] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson “Blockchain Based E-voting System” International Journal of Scientific Research in Science and Technology (2019).
- [4] M. Swan, Blockchain, “Blueprint for a New Economy”, Sebastopol, CA, USA: O’Reilly Media, 2015.
- [5] N. Ramkumar, G. Sudhasadaswam, K. G. Saranya, “Survey on different consensus Mechanisms on Blockchain Technology” 2020 International conference on communication and Signal Processing (2020).
- [6] Nicholas Weaver. (2016). Secure the Vote Today Available at: <https://www.lawfareblog.com/secure-vote-today>.
- [7] T. M. Roopak and R. Sumathi, “Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology”, 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020.
- [8] M. Swan, Blockchain, “Blueprint for a New Economy”, Sebastopol, CA, USA: O’Reilly Media, 2015.
- [9] Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., &Guizani, M., A “Blockchain-based Self-tallying Voting Protocol in Decentralized IoT”, IEEE Transactions on Dependable and Secure Computing (2020).
- [10] LinHao Bai, LuoHui Liu, “Research on Software Defined Network Security Model Based on Blockchain”, 2021 IEEE 6th International Conference on Intelligent Computing and Signal Processing (ICSP 2021).
- [11] Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M., A “Blockchain-based Self-tallying Voting Protocol in Decentralized IoT”, IEEE Transactions on Dependable and Secure Computing (2020).
- [12] Yang Jun-ho, Jin Min-goo, Lee Kyung-hee, Co-yung-won, “Design of Electronic Voting System based on Block Chain Security Technology”, Journal of The Korean Information Science Society, 2018.
- [13] Kashif Mehboob, Junaid Arshad, Muhammad Mubashir Khan “Secure Digital Voting System based on Blockchain Technology” International Journal of Electronic Governement Research (2018).
- [14] Cosmas Krisna, Rikard Hjort, Hiroyuki Sato “A Proposal of Blockchain-based Electronic Voting System” 2018 Second World Conference on Smart Trends in System, Security and Sustainability (2018).
- [15] Bhavani Thuraisingham “Blockchain Technologies and their Applications in Data Science and Cyber Security”, 3rd International Conference on Smart BlockChain (SmartBlock) (2020).
- [16] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system”, [Online]. <https://bitcoin.org/bitcoin.pdf>
- [17] Pluralsight (Jan. 19, 2019), “Blockchain Architecture”, Pluralsight.com. Accessed: Mar. 13, 2019. [Online]. <https://www.pluralsight.com/guides/Blockchainarchitecture>.
- [18] Yash Dalvi, Shivam Jaiswal, Pawan Sharma, “E-voting using Blockchain”, International Journal of Engineering Research & Technology (IJERT), 2021.