IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

Secure online voting system using Block Chain

N. Nagoor Meeravali[1], Devasani Anjili[2], V. Venkata Rao[3], Pogula Praveen Kumar[4], Delhi Divya Sri[5]

[1]Assistant Professor, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

[2,3,4,5] Students, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

Email id: meeravali587@gmail.com[1], anjilidevasani@gmail.com[2], venkataraovipparla1@gmail.com[3], praveenkumarm4pro@gmail.com[4], dehildivyasri@gmail.com[5]

Abstract:

The evolution of democratic systems has emphasized the critical importance of secure and fair elections, a practice deeply rooted in history since ancient Greece. Traditional voting methods, typically requiring physical presence at a polling station, face challenges such as tampering and security vulnerabilities. To address these issues, we propose a secure online voting system based on Blockchain technology, incorporating homomorphic encryption and hashing techniques to ensure the integrity and privacy of each vote. The system employs smart contracts, which activate when an election is scheduled, ensuring an efficient, tamper-resistant voting process. With an ever-growing voter base, modernizing voting infrastructure to enhance security and maintain fairness has become essential. Our approach decentralizes e-voting platform management across blockchains, leveraging a multi-winner approval voting system called Aqua on the Ethereum blockchain. This solution was rigorously tested and compared on public and private blockchains, demonstrating reliable performance at a relatively low speed while ensuring complete data privacy through homomorphic encryption.

Keywords: Python full-stack project, blockchain-based voting, homomorphic encryption, secure online voting, smart contracts, multi-winner approval voting, decentralized e-voting platform, election integrity, voter privacy

1.Introduction

An "online voting system," also known as "Internet voting," is a software platform that allows groups to securely conduct votes remotely and elections. Voters cast their votes with the aid of a computer during an election. High-level Online voting systems balance the overall ballot security and ensure the accessibility and tamper-proof behavior of recorded data. Ballot casting, recording, and tabulation are routinely done with computers, even in voting systems that are not strictly electronic. In the strict sense, electronic voting is a system followed nowadays in elections, where

the first step, ballot composition (or choosing), is done with the aid of a computer. Because of security and access concerns, most large-scale electronic voting is currently held in designated precincts using special-purpose machines. This type of voting mechanism is referred to as e-voting. There are two major types of e-voting equipment: direct recording electronic (DRE) machines and optical scanning machines. A typical DRE is composed of a touch screen connected to a computer. Ballots are presented to the voters on the touch screen, where they make their choices and cast their ballots. The touch-screen display can assist the voter in various ways, including displaying large fonts and high contrast for those with limited vision, alerting the voter to under votes, and preventing overvotes.

A DRE is a secure process that directly records the cast ballots and stores the data in its memory. Thus, a single machine is used for the composition, casting, and recording of votes. The third step, recording the cast ballot in a memory device, is invisible to the voter. Assurance that the vote is recorded as cast relies on testing the machine's hardware and software before the election and confidence that the software running during the election is the same as the one tested before the election. Both of these are subjects of much controversy. In other optical scanning systems, voters compose their votes on a computer screen. Once a ballot is completed, the computer prints an optical scanning ballot. The voter verifies the ballot and then inserts it into another device that scans and tabulates the vote. Both of these systems are considered electronic voting systems.

2.Related works

As an effective means of making democratic decisions, elections have long been a social concern. As the number of votes cast in real life increases, citizens are becoming more aware of the significance of the electoral system [1,2]. The voting system is the method through which judges judge who will represent in political and corporate governance. Democracy is a system of voters to elect representatives by voting [3,4]. The efficacy of such a procedure is determined mainly by the level of faith that people have in the election process. The creation of legislative institutions to represent the desire of the people is a well-known tendency. Such political bodies differ from student unions to constituencies. Over the years, the vote has become the primary resource to express the will of the citizens by selecting from the choices they made [2]. The traditional or paper-based polling method served to increase people's confidence in the selection by majority voting. It has helped make the democratic process and the electoral system worthwhile for electing constituencies and governments more democratized. There are 167 nations with democracy in 2018, out of approximately 200, which are either wholly flawed or hybrid [5,6]. The secret voting model has been used to enhance trust in democratic systems since the beginning of the voting system. It is essential to ensure that assurance in voting does not diminish. A recent study revealed that the traditional voting process was not wholly hygienic, posing several questions, including fairness, equality, and people's will, was not adequately [7] quantified and understood in the form of government [2,8]. Engineers across the globe have created new voting techniques that offer some anticorruption protection while still ensuring that the voting process should be correct.

Technology introduced the new electronic voting techniques and methods [9], which are essential and have posed significant challenges to the democratic system. Electronic voting increases election reliability when compared to manual polling. In contrast to the conventional voting method, it has enhanced both the efficiency and the integrity of the process [10]. Because of its flexibility, simplicity of use, and cheap cost compared to general elections, electronic voting is widely utilized in various decisions [11]. Despite this, existing electronic voting methods run the danger of over-authority and manipulated details, limiting fundamental fairness, privacy, secrecy, anonymity, and transparency in the voting process. Most procedures are now centralized, licensed by the critical authority, controlled, measured, and monitored in an electronic voting system, which is a problem for a transparent voting process in and of itself. On the other hand, the electronic voting protocols have a single controller that oversees the whole voting process [12]. This technique leads to erroneous selections due to the central authority's dishonesty (election commission), which is difficult to rectify using existing methods. The decentralized network may be used as a modern electronic voting technique to circumvent the central authority.

3.Methodology

Blockchain technology fixed shortcomings in today's method in elections made the polling mechanism clear and accessible, stopped illegal voting, strengthened the data protection, and checked the outcome of the polling. The implementation of the electronic voting method in blockchain is very significant However, electronic voting carries significant risks such as if an electronic voting system is compromised, all cast votes can probably be manipulated and misused. Electronic voting has thus not yet been adopted on chain technology. In Figure 4, one can see the main difference between both of the systems. In traditional voting systems, we have a central authority to cast a vote. If someone wants to modify or change the record, they can do it quickly; no one knows how to verify that record. One does not have the central authority; the data are stored in multiple nodes. It is not possible to hack all nodes and change the data. Thus, in this way, one cannot destroy the votes and efficiently verify the votes by tally with other nodes. a national scale, considering all its possible advantages. Today, there is a viable solution to overcome the risks and electronic voting, which is blockchain technology. In Figure 4, one can see the main difference between both of the systems. In traditional voting systems, we have a central authority to cast a vote. If someone wants to modify or change the record, they can do it quickly; no one knows how to verify that record. One does not have the central authority; the data are stored in multiple nodes. It is not possible to hack all nodes and change the data.

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

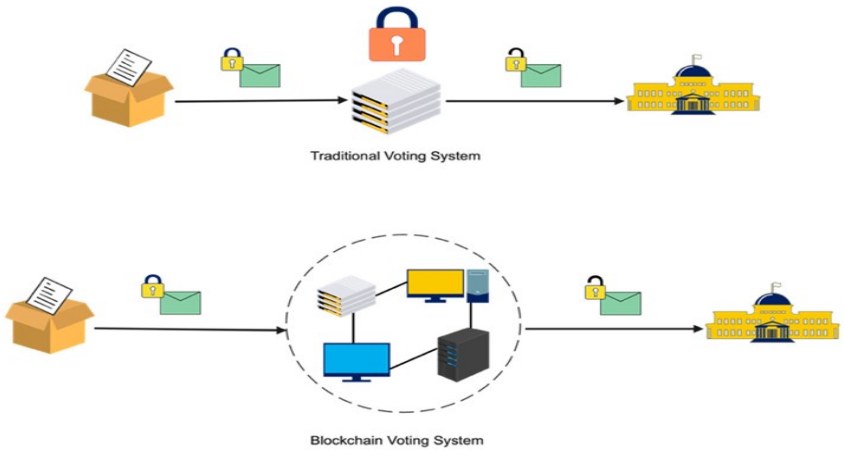


Figure: Traditional vs. blockchain voting system

The technology is used correctly, the blockchain is a digital, decentralized, encrypted, transparent ledger that can withstand manipulation and fraud. Because of the distributed structure of the blockchain, a Bitcoin electronic voting system reduces the risks involved with electronic voting and allows for a tamper-proof for the voting system. A blockchain-based electronic voting system requires a wholly distributed voting infrastructure. Electronic voting based on blockchain will only work where the online voting system.

Below is a brief overview of the solutions for satisfying these properties in online voting systems

Eligibility: The solution to the issue of eligibility is rather apparent. To take part in online voting, voters need to identify themselves using a recognized identification system. The identifiers of all legitimate voters need to be added to the list of participants. But there are threats: Firstly, all modifications made to the participation list need to be checked so that no illegitimate voters can be added, and secondly, the identification system should be both trusted and secure so that a voter's account cannot be stolen or used by an intruder. Building such an identification system is a complex task in itself.

Un reusability

At first, glance, implementing un reusability may seem straightforward when a voter casts their vote, all that needs to be done is to place a mark in the participation list and not allow them to vote a second time. But privacy needs to be taken into consideration; thus, providing both un reusability and voter anonymity is tricky. Moreover, it may be necessary to allow the voter to re-vote, making the task even more complex.

Privacy:

Privacy in the context of online voting means that no one except the voter knows how a participant has voted. Achieving this property mainly relies on one (or more) of the following techniques:

blind signatures, homomorphic encryption, and mix-networks Blind signature is a method of signing data when the signer does not know what they are signing. It is achieved by using a blinding function so that blinding and signing functions are commutative–Blind (Sign(message)) = Sign (Blind(message)). The requester blinds (applies blinding function to) their message and sends it for signing.

Security Requirements for Voting System

Suitable electronic voting systems should meet the following electronic voting requirements. Figure shows the main security requirements for electronic voting systems.

Anonymity: Throughout the polling process, the voting turnout must be secured from external interpretation. Any correlation between registered votes and voter identities inside the electoral structure shall be unknown.

Figure: Security requirements for electronic voting system

Electronic Voting on Blockchain

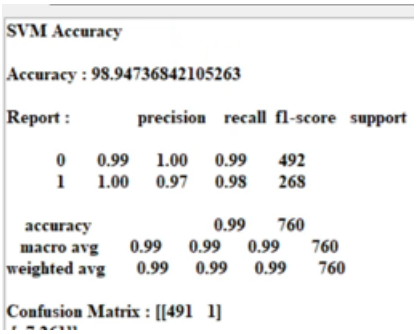
This section provides some background information on electronic voting methods. Electronic voting is a voting technique in which votes are recorded or counted using electronic equipment. Electronic voting is usually defined as voting that is supported by some electronic hardware and software. Such regularities should be competent in supporting/implementing various functions, ranging from election setup through vote storage. Kiosks at election offices, laptops, and, more recently, mobile devices are all examples of system types. Voter registration, authentication, voting, and tallying must be incorporated in the electronic voting systems Figure One of the areas where blockchain may have a significant impact is electronic voting. The level of risk is so great that electronic voting alone is not a viable option. If an electronic voting system is hacked, the

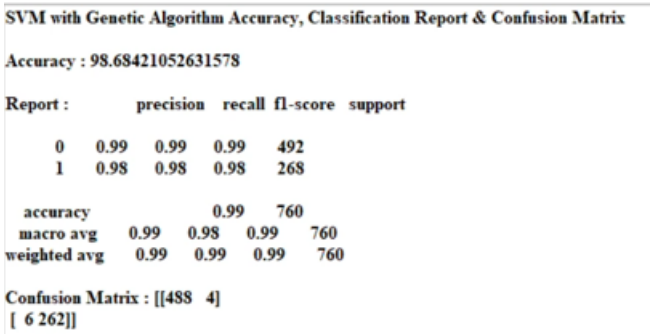
International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

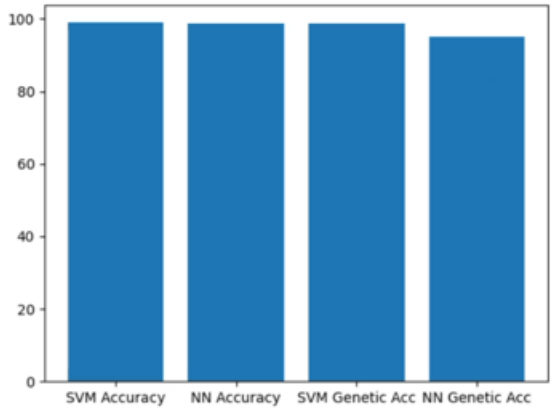
consequences will be far-reaching. Because a blockchain network is entire, centralized, open, and consensus-driven, the design of a blockchain-based network guarantees that fraud is not theoretically possible until adequately implemented As a result, the blockchain's unique characteristics must be taken into account. There is nothing inherent about blockchain technology that prevents it from being used to any other kind of cryptocurrency. The idea of utilizing blockchain technology to create a tamper-resistant electronic/online voting network is gaining momentum End users would not notice a significant difference between a blockchain-based voting system and a traditional electronic voting system.

Table: Scalability analysis of famous block chain platforms

Framework	Year Release	Generation Time	Hash Rate	Transactions Per Sec
Bitcoin	2008	9.7 min	899.624 Th/s	4.6 max 7
Ethereum	2015	10 to 19 s	168.59 Th/s	15
Hyperledger Fabric	2015	10 ms	NA	3500
Litecoin	2011	2.5 min	1.307 Th/s	56
Ripple	2012	3.5 s	NA	1500
Dogecoin	2013	1 min	1.4 Th/s	33
Peercoin	2012	10 min	693.098 Th/s	8







Conclusions

The goal of this research is to analyze and evaluate current research on block chain based electronic voting systems. The article discusses recent electronic voting research using blockchain

technology. The blockchain concept and its uses are presented first, followed by existing electronic voting systems. Then, a set of deficiencies in existing electronic voting systems are identified and addressed. The blockchain's potential is fundamental to enhance electronic voting, current solutions for blockchain-based electronic voting, and possible research paths on blockchain-based electronic voting systems. Numerous experts believe that blockchain may be a good fit for a decentralized electronic voting system. Furthermore, all voters and impartial observers may see the voting records kept in these suggested systems. On the other hand, researchers discovered that most publications on blockchain-based electronic voting identified and addressed similar issues. There have been many study gaps in electronic voting that need to be addressed in future studies. Scalability attacks, lack of transparency, reliance on untrustworthy systems, and resistance to compulsion are all potential drawbacks that must be addressed. As further research is required, we are not entirely aware of all the risks connected with the security and scalability of blockchain-based electronic voting systems.

References

1. Liu, Y.; Wang, Q. An E-voting Protocol Based on Blockchain. IACR Cryptol. Eprint Arch. 2017, 2017, 1043. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access 2019, 7, 24477–24488.
2. Racsko, P. Blockchain and Democracy. Soc. Econ. 2019, 41, 353–369.
3. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. arXiv 2019, arXiv:1906.11078. The Economist. EIU Democracy Index. 2017.
4. Cullen, R.; Houghton, C. Democracy online: An assessment of New Zealand government web sites. Gov. Inf. Q. 2000, 17, 243–267.
5. Schinckus, C. The good, the bad and the ugly: An overview of the sustainability of blockchain technology. Energy Res. Soc. Sci. 2020, 69, 101614.
6. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. IEEE Access 2019, 7, 115304–115316.
7. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, A.; Di, J.; Li, Q.; Lee, Y. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE J. Emerg. Sel. Top. Power Electron. 2020.
8. Hang,L.; Kim, D.-H. Design and implementation of an integrated iot blockchain platform for sensing data integrity. Sensors 2019, 19, 2228.
9. Chang, V.; Baudier, P.; Zhang, H.; Xu, Q.; Zhang, J.; Arami, M. How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. Technol. Forecast. Soc. Chang. 2020, 158, 120166.
10. Wang, B.; Sun, J.; He, Y.; Pang, D.; Lu, N. Large-scale election based on blockchain. Procedia Comput. Sci. 2018, 129, 234–237.
11. Ometov, A.; Bardinova, Y.; Afanasyeva, A.; Masek, P.; Zhidanov, K.; Vanurin, S.; Sayfullin, M.; Shubina, V.; Komarov, M.; Bezzateev, S. An Overview on Blockchain for

ISSN 2347–3657

Volume 13, Issue 2, 2025

Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends. IEEE Access 2020, 8, 103994–104015