International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Investigating the Potential of Blockchain for Secure Voting Systems

Disha Sharma[1]
[0000-0002-9011-789]
Chandigarh University,
Punjab, India
disha.e13241@cuchd.com

Ashish Kumar[2]
[0009-0004-4361-6056]
Chandigarh University,
Punjab, India
sauravashish.0000@gmail.com

Nandan Raj[3]
[0009-0007-2554-6762]
Chandigarh University,
Punjab, India
nandansharma712@gmail.com

Ankit Singh[4]
[0009-0005-0046-1741]
Chandigarh University,
Punjab, India
superakt2003@gmail.com

Shashank Kumar[5]
[0009-0001-6173-3887]
Chandigarh University,
Punjab, India shashankkumar2160@gmail.com

Abstract – Electronic voting systems open opportunities for better accessibility and improved efficiency of the electorate, but simultaneously Electronic vote face several issues of security, transparency and voters' privacy. Therefore, this paper looks at how or to what extent blockchain may solve some of these problems and develop better, safer, and more accurate e-voting. In this paper, we categorize the basic advantages and disadvantages of using blockchain technology in voting by surveys of the literature and some proposed implementations of blockchain voting. Despite the potential of the current blockchain applications for voting in terms of increase of transparency, immutability and decentralization, there is still a long way to go to design suitable, scalable and real-life blockchain-based voting systems that could offer the same or even better security and anonymity level of the current paper- based ballots. We review different technical solutions, describe case studies of the pilot implementations, and define further research directions. Combined, blockchain has future possibilities for developing electronic voting, though research and an actual implementation are required before committing to deploying it to foundational election technology.

Keywords: Blockchain, E-voting, Secure voting systems, Voter authentication, Cryptography, Accessibility, User experience, Transparency,.

1. INTRODUCTION

E-voting is widely regarded as essential to election management and administration, as a means of addressing challenges and 'modernizing' the process. Paper based ballots involve spending a lot of time and involves human errors, while electronic based systems are efficient, quick to implement and easily accessible. Nevertheless, e-voting has several main problems, the principal of which are: cybersecurity risks, fraud, and a lack of visible transparency that weakens public confidence in the democratic outcome.

Blockchain herein comes out as a possible remedy to these problems. Given that blockchain provides a distributed, tamper- proof, and shared database, it provides the opportunity to redefine e-voting by enhancing the security, auditable nature and overall, public confidence in the process. Current concerns with electronic voting are discussed in this paper because this methodology is currently debated, although its efficiency seems to be undisputed, and the relevance of blockchain to voting systems is investigated to see how e-voting based

on blockchain can overcome serious problems and meet new opportunities for organizing free, honest, open, and reliable elections.

2 .BACKGROUND

2.1 Traditional Electronic Voting Systems

E-voting systems are implemented to act as a substitute for or in lieu of paper-based voting. The most common types of e-voting systems include:

Direct Recording Electronic (DRE) systems: Such systems use electronic interactive surfaces such as touch screen on which voters make their decisions. The machine records the total votes cast directly into its digital storage and often prints a voter's verified record. Full-paper DREs are threatened by cyber-security attack, viruses, and possible intervention from insiders and therefore raising questions over the authenticity of votes.

Optical Scanning systems: People write on paper ballots which are then captured by electronic means. This hybrid approach does retain a paper record while at the same the electronic and computerized system is used for the tallying of the votes. However, this system although is considered to be a little more secure than the DREs because of physical records, this system is also capable to manipulate and the counting process may involve original human mistakes or mechanical frauds.

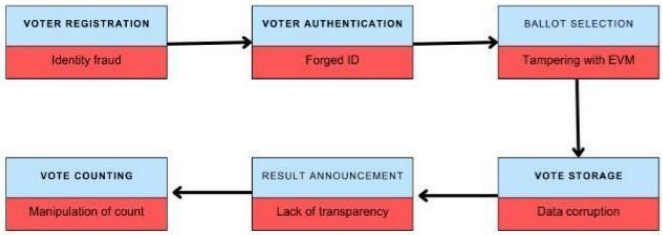

Fig 1. Problems in traditional voting system

2.2 Current Challenges and Vulnerabilities

Despite the rise of e-voting, many concerns remain:

Security vulnerabilities: Some of the e-voting systems cannot be said to have strict security measures against cyber threats. DREs together with other optical scanning systems are most exposed to hacking, software flaws, and intruder interference that may alter the entire vote count secretly.

Lack of transparency: Many voters cannot ascertain or be sure that their vote has been correctly recorded and counted. In some systems, voters have to rely on their vote being cast right on the machine with no possibility the voting system may not be accurate.

Centralized control: Most e-voting systems have centralized databases meaning a compromise in that particular point will affect the whole election. There is also the challenge to internal control, as the central processes place the finances in the hands of some miscreants.

4.Voter trust: These both technical and security concerns create a factor that hinders the credibility of electronic voting systems. When there are no rational ways of independently verifying the electoral processes, the faith of the electorate in democratic process may diminish.

3 LITERATURE REVIEW

3.1 Blockchain Technology

Originally, blockchain technology was designed essentially as support layer for implementing crypto-currency like Bitcoin; however, the increasing number of potential uses of this technology enables one to believe in multiple applications across industries. In simple terms, a blockchain could be described as a distributed traditional ledger for recording transactions with all the transactions stored in a network of computers. Key features of blockchain technology include:

- **Decentralization:** Unlike other systems, traditional or corporate databases in block chain systems are distributed across a networked computers with no central hub or hardware failure. A copy of the blockchain is stored in every node in the network to ensure that nobody has the ability to corrupt or produce a individual data and software in absence of consensus of the network.

- **Immutability:** What makes blockchain unique is that data added to the block cannot be changed or removed. This makes blockchain well suited for use in applications whereby there is need for an immutable record such as in voting applications.

- **Transparency and auditability:** The record produced by the Blockchain is seen by all the section members, so it can be audited and checked by participants. Within the sphere of voting this can go a long way towards fostering trust and guarantee that an election process was legitimate.

3.2 Relevance to Voting System

The nature of blockchain makes it well fit for use in e-voting systems among other systems. As a result, the use of blockchain can help overcome many of the security and trust concerns involved in e-voting systems. Voters and election authority can easily cross-check on the result s obtained and thus make sure that the votes cast are adequately recorded and counted as per the desires of the people. Furthermore, decentralization of blockchain makes centralized fraud or manipulation of the voting process unlikely as well so votes are more genuine and credible.

3.3 Blockchain Based Voting Systems

Case Studies

Several blockchain-based voting platforms have been deployed or tested in real-world elections:

- *Voatz mobile voting app***:** Voatz has also been employed in local elections here in the United States where a voter can vote from the comfort of his/her smartphone. Although critics find these issues as security threat, the application shows that blockchain voting can actually improve accessibility and convenience especially for military and absentee voters.

- *Follow My Vote platform:* A blockchain based electronic voting platform that is open source and thus dubbed Follow My Vote seeks to ensure the election is credible. It also allows the voters to ensure that they have voted correctly and their choices have been recorded correctly and at the same time voters exercise their rights anonymously.

- *Votem's CastIron platform:* Votem provides end-to-end encrypted voting systems based on the distributed ledger technology ideal for use in mass voting processes. In

guaranteeing election integrity, CastIron makes use of blockchain for voting while providing records and trackers for audits.

3.4 Security Considerations

Advantages:

Blockchain-based voting systems offer several security advantages:

- *Resistance to tampering and fraud:* This is because most of the control is shifted from a central authority and the voting is instead secured by cryptography on the blockchain network.

- Also, if an attacker manages to gain control of a single node, then he cannot change the whole election record.

- *End-to-end verifiability:* Indeed, in a blockchain technology, the votes are verified from the time they are cast to the time they are tallied. The voters were able to confirm their votes were taken while the independent auditors can check the general tally of the election.

- *Anonymity and vote secrecy:* Another strand asserts that blockchain methods can preserve the anonymity of the voter. While the block-chain transactions are public and may be easily seen by everyone in the network the votes themselves are encrypted and the identity of the voter cannot be ascertained.

Challenges and Vulnerabilities:

Despite its potential, blockchain voting faces significant challenges:

- *Potential for hacking or manipulation:* While the blockchain is very secure, the application remains insecure, and identity cards, voter devices are at risk. For example, a virus on a voter's smartphone would change their vote before it gets written to the blockchain. This challenge can only be addressed with serious security measures that are not a part of the blockchain network.

- *Privacy concerns:* Privacy of voters and at the same time serve the purpose of electoral transparency is a daunting task. While the blockchain solutions preserve the voting agency anonymity, the use of further cryptographic measures that include zero knowledge proofs could possibly eradicate these issues.

- *Scalability and performance issues:* It is noteworthy that, for example, proof-of-work based blockchains and their transaction processing can be slow, and require a great amount of power. Such challenges threaten to reduce the

- applications of blockchain voting systems especially at the national level with millions of voters.

Ethical and Social Implications:

The implementation of blockchain-based voting systems raises several ethical and social questions:

- *Impact on voter trust and confidence:* Unfortunately, for blockchain to gain mainstream use, the general public needs to understand how it functions because its primary features include transparency and checkability. Some people might have a misconception or lack accurate information on the blockchain technology and will instill some form of resistance while implementing the system. They have not implemented any practice all need to start and build a workable relationship Confidence building will be key in implementation.

- *Digital divide and accessibility concerns:* While using the blockchain for voting is convenient for techie voters, it may also widen the gap between those connected to the internet. Only some voters especially those living in rural areas or those with limited physical access to technological devices may feel challenged in their ability to participate.

4. METHODOLOGY

4.1 System Design and Implementation

Ease Of Use and Accessibility

One more limitation found is that the user experience and access to blockchain application in the context of voting systems should be easily extended to as many users as possible and be as comprehensive as possible to accommodate as many people as possible within society. This section summarizes general considerations for the layout of a voting interface as well as principal concerns for interface accessibility.

Special Consideration for the Targeted Groups

The voting interface should be tailored for different age bracket including young adults as well as the aged persons. Accessibility is critical for a design that follows layouts that are straightforward, instructive, and whose text is easy to read. The system should particularly be developed to accommodate mobile and tablet interfaces in addition to the standard PCs. Final groups of voters with different age, gender, marital status, etc. should go through user testing to adjust interface.

Accessibility Features

In addressing the needs of the disabled voters the system must incorporate the following categories. Website accessibility features that are particularly important to visually impaired voters include compatibility with assistive technology such as the screen reader as well as providing an audio feedback and voice control of the voting process. Refreshed color contrast combined with the resizable texts enhances the content's readability; the keyboard's control ensures that the motor-disabled will have easy access to the site's interfaces. Keyboard adaptations should also include additional ways of voting as well as sip-and-puff or eye-gaze control systems for voters with disabilities

Multilingualism: Supporting and Translating

The voting system needed to have a capacity to support different languages since the world is full of different linguistic groups. It is crucial to maintain the current progress in the voting process and the ability for switching languages in real time. Candidate information and ballot measures not only have to be translated, but also have to be translated accurately. Support for right-to-left orientation where necessary and overriding concerns as regards cultural sensitiveness with respect to design cues and icons necessary in creating a universal voting platform.

4.2 Technical Implementation

It remains crucial to consider several essential technical issues in order to construct the sufficient and effective system of blockchain- based voting. There are several stages that make secure and reliable.

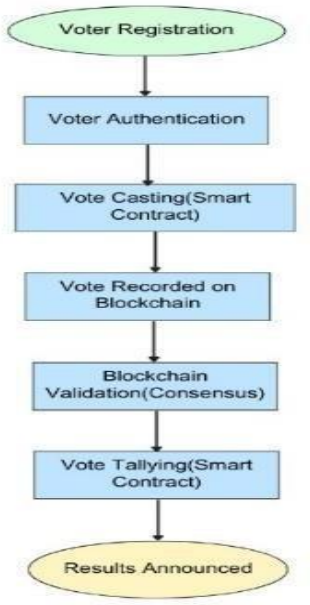

Fig 2. Voter Registration Process

1. Voter authentication and eligibility verification: With regard to the issue of voters, there is a need to guarantee only the voters who are legally supposed to vote to exercise that right and do it accordingly. By so doing, each of the blockchain systems tries to employ sound procedures for voter verification to prevent fraudulent activities during the election. These procedures may include:

- Employing licenses that are extracted from the online voter registration lists
- The use of biometrics identification such as fingerprint or face scan
- Employing cryptographic keys that referred to each voter only

But for the purpose of increasing security, a combination of two or more of those methods can be used, this is known as two-factor authentication. Further, the use of zero-knowledge proof so as to confirm the eligibility of the voters as a means of avoiding disclosure of the voters personal details. A particular vote can be coded to check the qualifications of the voter before approving ones vote, even with the use of smart contracts on the blockchain.

2. Vote casting and recording on the blockchain: As soon as a voter is authenticated, voting is conducted simplistically through a graphical user interface. The voting process in a blockchain- based system involves several key steps:

- The vote is encrypted with the help of homomorphic encryption and other such technologies.
- The encrypted vote is used in a transaction on the blockchain.
- More importantly the vote once recorded cannot be altered or deleted affording the vote high levels of immutability.
- The vote will therefore remain anonymous throughout, with the use of taxonomical particulars such as ring signatures or mixnets to conceal the link of the voter to the encrypted vote they cast.

Additional Considerations:

- It should also accommodate political accessibility for voters with disabilities and support multilingual for the disabled as well as those voters who do not understand English.
- In addition, the blockchain platform used needs to be scalable during the increased voting traffic at the voting period to ensure that all the votes made during this period are recorded appropriately and immediately.

3. Vote tallying and result verification: A single genetic and structural characteristic in a blockchain-based voting system is the high level of vote count information protection. The following features ensure accurate and verifiable results:

- The vote counts are stored on the blockchain and can be changed once the data has been input into the system.
- Homomorphic encryption enables transfer of votes and their counting in such a way that each ballot does not have to be decrypted.
- The system allows independent confirmation of the result by electoral commissions and candidates and the general public without compromising identities of the voters.
- Smart contracts can also be employed in tallying to eliminate errors that may be occasioned by tallying.
- The voting records can be audited by anyone by furnishing a public blockchain explorer.
- Proximity proofs can be created for proving vote inclusions, or for proving correctness of the final tally.

The process of vote casting, vote counting and result verification being so transparent makes the various stakeholders place their trust on the election result.

4. System Security and Auditing: To ensure the overall integrity of the blockchain-based voting system, comprehensive security measures and auditing processes must be implemented:

- A series of routine security assessments and, at least, vulnerability probing should be implemented and performed.
- Proper DDoS protection methods have to be employed in order to guarantee system availability during the course of the election
- There should be end to end verification so that a voter should be able to verify her votes without violating the privacy of her ballot.
- There are ways that risk limiting audits can be conducted that will have the goal of confirming the accuracy of the published results of the elections.
- Failed systems need to be backed up to recover data and therefore proper disaster recovery mechanisms must be developed.
- The use of transparent code review as well as the open-source approach will create confidence in the system's security.

5 FUTURE CONSIDERATIONS

Although there are massive developmental opportunities with blockchain technology applications in voting, there are some themes that need to be researched, promoted, and tested to become more effective in large- scale elections. Here are some key areas for future exploration:

- **Scalability and Performance Improvements:** Today's blockchain technologies are mostly centralized and those based on proof-of-work, face limitations of scalability and slow transactions per second. In the context of the national elections, where the number of votes millions that should be registered in a short period, these impediments could hamper the use of blockchain. More researches are still needed to work on new consensus algorithms like proof-of- stake, or sharding, or hybrid proofs of concept which can handle high volumes of transactions needed in the conduct of large scale elections.

- **Privacy-Enhancing Technologies:** One of the key issues in blockchain-based voting is the protection of vote anonymity and at the same time, the full and open vote count. In our framework, we ensure the anonymity of the votes and only report the aggregated result without disclosing the vote choices of every voter by using cryptographic methods like zero-knowledge proofs and homomorphic encryption. There is then need for more research on these methods to make sure that privacy for any patient is not at any one time infringed and at the same time there should be more transparency in the methods used.

- **Interoperability with Existing Voting Infrastructure:** To further innovate voting systems, future systems must also immediately interface with current voting systems for easy switching to blockchain solutions. This involves interaction with systems, voter registration, identity/authenticity data bases, and conventional election audit trails. The combination of blockchain videos the use of traditional paper ballots may be the way forward during transition phase.

- **Regulatory and Legal Frameworks:** The integration process of blockchain in electoral systems requires independent legal and regulatory provisions. There are issues of legal ramifications, regulation including recognition of privacy laws say in the European Union (EU) General Data Protection Regulation (GDPR), and moments of responsibility in the event of system snafus or fraud. Creating such frameworks will be instrumental in approaching the decentralised voting systems' legitimacy in blockchain platforms.

- **Security Threats and Attack Vectors:** However, as much as blockchain incorporates massive security benefits, everything surrounding blockchain extending to the Voter devices and internet connections is hackable. Promising work on the fundamental hardware and software solutions of physical tamper-resistant storage, confidential execution and even higher-level security in a voting context is still necessary. Further constant auditing, stress testing and, simulation of genesis block and voting systems by posing different attack situations will go a long way in establishing possible risks and ensuring safety.

- **User Experience and Accessibility:** Currently, there have been increased adoption of blockchain based voting systems, and in order to for them to gain public approval, they should incorporate a voting system that any voter, including the illiterate ones can comfortably use. Especially, the overhauling of the voting system, the enhanced interface, and effective voter education shall form the core in enabling the blockchain voting systems to deliver

- **Pilot Programs and Public Trials:** Thus, the idea of applying blockchain voting means is not contrary to the implementation of voting based on this technology on a national level In order to assess the potential and applicability of blockchain technology for voting purposes, it is critical to organize pilots in a small-population-controlled environment. Still these trials are useful to adjust the technology and to define all potential practical problems that can come out during wider application. Other nations like Estonia and Switzerland have even tried mock blockchain-based voting to make it clear as to what can be achieved and what is wrong with blockchain.

- **Increased Voter Confidence through Education:** Another challenge that may affect the implementation of the blockchain voting system is the ill iterates of citizenry of such systems. Unless voters know how a blockchain works or how it makes the process more secure they may be reluctant or suspicious of the technology. To make the public, political leaders and election officials believe in the blockchain system, they will have to be educated on the advantages and processes involved in the blockchain system.

6 CONCLUSION

The application of the blockchain capability offers an opportunity to change the nature of electronic voting due to its issues of security, traceability, and credibility. Distributed and time-stamped nature of the blockchain functionality provides evidence that the vote has not been altered which improves voters expectation of the accurate tallying of the corals. Moreover, a use of the blockchain may improve the voter turnout, especially among the disenfranchised or citizens living in foreign countries due to the opportunity of remote and available voting.

Still, there are certain problems associated with the use of blockchain based voting systems. Concerns regarding the size of the problems being solved, privacy, and security, irregularities with governmental regulation must be resolved before blockchain can be utilized for national elections. Furthermore, the growing threats of hacking, voter intimidation, and the digital gap cannot be ignored under careful designing, implementing, and training.

However, the implementation of blockchain solution for secure and transparent voting will not be successful unless technologists, policymakers, and election officials come on board. With regards to the future of voting, more study should be made, suitable legal mechanisms need to be established and pilot implementation needs to be made to pave the way for a new voting system that is fair, secure, and credible. Blockchain can bring, not only advancements to the election process, but also protect one of the most important human achievements – democracy.

Funding Information

Not Applicable

Author Contribution

Ankit Singh: Conceptualization, methodology, writing - original draft, project administration

Ashish Kumar: Investigation, data analysis

Nandan Raj: Methodology, validation

Er. Disha Sharma: Supervision, review and editing

Vasudha Sharma: data validation, formal analysis

Shashank Kumar: Review and editing

Data Availability Statement

The data and implementation details presented in this study are available from the corresponding author upon reasonable request. The source code and documentation will be made available following publication.

Research Involving Human and/or Animals

Not Applicable - This research is focused on blockchain technology implementation and does not involve human participants or animal subjects.

Informed Consent

Not Applicable - This study did not require informed consent as it did not involve human subjects or collection of personal data.

REFERENCES

1. Lindmark, Malin, and Asima-Asja Salihovic. "Investigating the Security of End-to-End and Blockchain-based Electronic Voting Systems: A Comparative Literature Review." (2022).
2. Pawlak, Michał, and Aneta Poniszewska- Marańda. "Trends in blockchain-based electronic voting systems." Information Processing & Management 58.4 (2021): 102595.
3. Agbesi, Samuel, and George Asante. "Electronic voting recording system based on blockchain technology." 2019 12th CMI Conference on Cybersecurity and Privacy (CMI). IEEE, 2019.
4. Preethi Kasireddy, "Fundamental challenges with public blockchains", Dec 10, 2017. Available: medium.com/@preethikasireddy/fundamental challenges-with-public-blockchains- 253c800e9428.
5. Çabuk U.C., Çavdar A., Demir E., Şenocak T., "A Financial Analysis on Realization of Elections and Votings as Online in Turkey", in Proc. of Mediterranean Natural Sciences and Engineering Congress (MENSEC), October 2017, pp.31-32.
6. Karaarslan E., Akbaş, M.F., "Blockchain based Cyber Security Systems", International Information Security Engineering Journal, 2017. doi: 10.18640/ubgmd.373297, 2017.
7. M. L. Pennetier, L. Thomas, J. Stonestreet, "France drops electronic voting for citizens abroad over cybersecurity fears", Reuters, March 6, 2017.
8. Scytl Online Voting, "Online Voting Technology", September 2015. Available: www.scytl.com/wp-content/uploads/2015/09/DIGITAL_online voting.pdf.
9. Heiberg, S., Laud, P. and Willemson, J., September. "The application of i-voting for
10. Estonian parliamentary elections of 2011", In International Conference on E-Voting and Identity (pp. 208-223). Springer, Berlin, Heidelberg, 2011.
11. White M., Killmeyer J., Chew B., "Will blockchain transform the public sector? Blockchain basics for the government", Deloitte Center for Government Insights Report, Deloitte University Press, Sep 2017.
12. Stephen Dinan, "Stunning testimony: Voting machines can be hacked without a trace of evidence", The Washington Times, September 12, 2017.
13. European Commission: CORDIS: Projects and Results, "An innovative cyber voting system for Internet terminals and mobile phones". September 9, 2000.
14. Feng Hao, Peter Y. A. Ryan, "Real-World Electronic Voting: Design, Analysis and Deployment", Chapter 7, Auerbach Publications, ISBN: 9781498714693, December 13, 2016.
15. Sebastian Kettley, "Vote online: Can you vote online in the General Election 2017?", June 8, 2017. Available: www.express.co.uk/news/politics/814685/Vote- online-election-2017-can-you-vote-online-UK- general-election.