BLOCKCHAIN TECHNOLOGY BASED E-VOTING SYSTEM

TECHNICAL REPORT

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF

BACHELOR OF TECHNOLOGY

(Computer Science and Engineering)

Submitted By:	Submitted To.:
Bhumi	Er. Satinderpal Singh
(URN: 2302500)	

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GURU NANAK DEV ENGINEERING COLLEGE

LUDHIANA, 141006

August, 2024

Abstract

The employment of blockchain technology in electronic voting (e-voting) systems is attracting significant attention due to its ability to enhance transparency, security, and integrity in digital voting. This study presents an extensive review of the existing research on e-voting systems that rely on blockchain technology. The study investigates a range of key research concerns, including the benefits, challenges, and impacts of such systems, together with technologies and implementations, and an identification of future directions of research in this domain. We use a hybrid review approach, applying systematic literature review principles to select and categorize scientific papers and reviewing the technology used in these in terms of the above key concerns. The electronic voting has emerged over time as a replacement to the paper-based voting to reduce the redundancies and inconsistencies. The historical perspective presented in the last two decades suggests that it has not been so successful due to the security and privacy flaws observed over time. In order to guarantee the security of the framework proposed in this paper, efficient hashing techniques information. This paper introduces the notion of block creation and block sealing. The introduction of the blockchain can be adjusted to meet polling needs thanks to the block sealing concept. procedure. The use of consortium blockchain is suggested, which ensures that the blockchain is owned by a governing body (e.g., election commission), and no unauthorized access can be made from outside. The framework proposed in this paper discusses the effectiveness of the polling process, hashing algorithms' utility, block creation and sealing, data accumulation, and result declaration by using the adjustable blockchain method.

ACKNOWLEDGEMENT

I am highly grateful to the Dr. Sehijpal Singh, Principal, Guru Nanak Dev Engineering College (GNDEC), Ludhiana, for providing this opportunity to carry out the technical report at **Blockchain technology based e-voting system**.

The constant guidance and encouragement received from Dr. Kiran Jyoti H.O.D. CSE Department, GNDEC Ludhiana has been of great help in carrying out the technical report and is acknowledged with reverential thanks.

We would like to express a deep sense of gratitude and thanks profusely to Er. Satinderpal Singh, without his/her wise counsel and able guidance, it would have been impossible to complete the technical report in this manner.

We express gratitude to other faculty members of computer science and engineering department of GNDEC for their intellectual support throughout the course of this work.

Finally, we are indebted to all whosoever have contributed in this report work.

Bhumi

TABLE OF CONTENTS

Contents	Page No.

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Voting has always been an important part of expressing one’s views in a democratic society. Will of the people is a well-respected phenomenon for representation of opinion in formation of electoral bodies. These electoral bodies vary from the college unions to the parliaments. Over the years, `vote' has emerged as a tool for representing the will of the people when a selection is to be made among the available choices. The voting tool has helped improving the trust of people over the selection they make by a vote of majority. In order to make the voting process more effective the institutions like `Election Commission' came into existence in different parliamentary democracies. The institutions, along with setting up the process and legislation for conducting the elections, formed the voting districts, electoral process, and the balloting systems to help in conduct of transparent, free, and fair elections. The concept of secret voting was introduced since the beginning of the voting system.

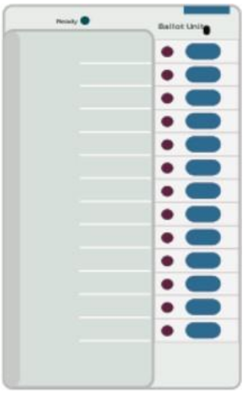

Fig 1: EVM machine

The use of EVMs and electronic voting was developed and tested by the state-owned Electronics Corporation of India and Bharat Electronics in the 1990s. They were introduced in Indian elections between 1998 and 2001, in a phased manner. Prior to the introduction of electronic voting, India used paper ballots and manual counting. The paper ballots method was widely criticized because of fraudulent voting and booth capturing, where party loyalists captured booths and stuffed them with pre-filled fake ballots. Embedded EVM features such as electronically limiting the rate of casting votes to five per minute.

Blockchain technology has been acknowledged as a possible remedy for transparent and safe electronic voting systems. By utilizing blockchain technology's decentralization, immutability, and transparency, electronic voting systems can enhance voter anonymity, thwart fraud and manipulation, and boost public confidence in the democratic process. Furthermore, e-voting systems built on blockchain technology can save time and money compared to conventional voting methods.

Conventional voting methods frequently depend on centralized organizations, which opens the door to vulnerabilities like electoral fraud or result tampering. Blockchain technology can be used to build an open, transparent, and impenetrable platform for electronic voting. Blockchain-based electronic voting systems combine consensus protocols and cryptographic techniques to offer safe, verifiable, and auditable voting processes. The growing interest in blockchain-based e-voting systems indicates the importance of a comprehensive and systematic evaluation of the current knowledge in this domain. One of the aims of this review is to identify the main benefits of e-voting systems based on blockchain technology through an in-depth review of the previous research. These benefits include heightened security, transparency, decentralization, and privacy.

ADVANTAGES

• ENHANCED SECURITY

Your data is sensitive and crucial, and blockchain can significantly change how your critical information is viewed. By creating a record that can’t be altered and is encrypted end-to-end, blockchain helps prevent fraud and unauthorized activity. Privacy issues can also be addressed on blockchain by anonymizing personal data and using permissions to prevent access.

Information is stored across a network of computers rather than a single server, making it difficult for hackers to view data.

• GREATER TRANSPERANCY

Without blockchain, each organization has to keep a separate database. Because blockchain uses a distributed ledger, transactions and data are recorded identically in multiple locations. All network participants with permissioned access see the same information at the same time, providing full transparency. All transactions are immutability recorded, and are time- and date stamped. This enables members to view the entire history of a transaction and virtually eliminates any opportunity for fraud.

• INSTANT TRACEBILITY

Blockchain creates an audit trail that documents the provenance of an asset at every step on its journey. In industries where consumers are concerned about environmental or human rights issues surrounding a product — or an industry troubled by counterfeiting and fraud — this helps provide the proof. With blockchain, it is possible to share data about provenance directly with customers. Traceability data can also expose weaknesses in any supply chain — where goods might sit on a loading dock awaiting transit.

• INCREASED EFFICIENCY AND SPEED

Traditional paper-heavy processes are time-consuming, prone to human error, and often requires third-party mediation. By streamlining these processes with blockchain, transactions can be completed faster and more efficiently. Documentation can be stored on the blockchain along with transaction details, eliminating the need to exchange paper. There's no need to 17 reconcile multiple ledgers, so clearing and settlement can be much faster.

• AUTOMATION

Transactions can even be automated with “smart contracts,” which increase your efficiency and speed the process even further. Once pre-specified conditions are met, the next step in transaction or process is automatically triggered. Smart contracts reduce human intervention as well as reliance on third parties to verify that terms of a contract have been met. In insurance, for example, once a customer has provided all necessary documentation to file a claim, the claim can automatically be settled and paid.

APPLICATIONS

• Cryptocurrency exchange

• Voting mechanism

• Secure sharing of medical data

• NFT marketplaces

• Music royalties tracking

• Cross-border payments

• Real-time IoT operating systems

• Personal identity security

• Anti-money laundering tracking system

• Supply chain and logistics monitoring

• Advertising insights

• Original content creation

• Real estate processing platform

CHAPTER 2

LITERATURE REVIEW

To enhance trust, the simplest step to take in this area is to implement electronic voting systems that rely on biometric identification. This approach could address a significant portion of the issues encountered by numerous nations during their electoral processes. Electronic voting systems have been employed by a select few countries, such as Estonia, Ireland, and Norway, while others have chosen to discontinue their use to avoid audit-related complications.

Blockchain technology is rapidly emerging as the most advanced. While the Internet has been accustomed to various peer-to-peer applications for file sharing, music streaming, and more, the concept that such networks could offer their own security and resources was introduced only in 2008. Over the past decade, blockchain has been primarily associated with the success of the technology that birthed it, bitcoin.

Lately, it has quickly emerged as a leading figure in its own right. As the global favourite cryptocurrency gained popularity, so did the understanding of its enigmatic and distinctive technology. Developers who saw the worth in blockchain are now in a hurry to innovate with it and bring their concepts to life.

A lot of people are discovering that blockchain's main benefit is its capacity to enhance existing systems. Forward-thinking individuals recognized the technology's potential early on, as bitcoin provided a more secure and transparent solution for payments and banking than what was currently available. Over the past few years, these same individuals have utilized blockchain to transform sectors across the globe, including cloud computing, smart contracts, crowdfunding, and healthcare. Yet, one of the most significant issues that blockchain's decentralized power can address is voter fraud.

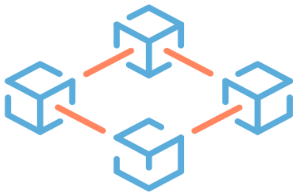

Fig 2: Blockchain Illustration

2.1 Blockchain Serves the Voters

In its most basic form, blockchain is a digital ledger. The technology draws its power from the peers or nodes on its network to verify, process, and record all transactions across the system. This ledger is never stored, but rather exists on the “chain” supported by millions of nodes simultaneously. Thanks to encryption and decentralization, blockchain’s database of transactions is incorruptible, and each record is easily verifiable. Blockchain can solve the many problems discovered in these early attempts at online voting. A blockchain-based voting application does not concern itself with the security of its Internet connection, because any hacker with access to the terminal will not be able to affect other nodes. Voters can effectively submit their vote without revealing their identity or political preferences to the public. Officials can count votes with absolute certainty, knowing that each ID can be attributed to one vote, no fakes can be created, and that tampering is impossible.

2.2 A True Democracy

A True Democracy Blockchain is paving the way for a direct democracy, where people can decide the course of policy themselves, rather than rely on representatives to do it for them. While the rules of a political election may have to be changed to make way for such a transparent system, blockchain is also ideal for informing business decisions, guiding general meetings, polling, censuses, and more. The use cases for blockchain voting software are many and diverse. Its ability to engage and manage a constituency is crucial to the future of society, not just to produce a transparent outcome but to encourage all people to participate in their communities. Currently, the technology is still in its infancy, but it matures alongside the young voters it will one day help, and looks to be a key part of our collective future.

CHAPTER 3

OBJECTIVES

Thus, the voting system that is hereby conceived must satisfy the following requirements:

1. The election system must be openly verifiable and transparent.

2. The election system must ensure that the vote cast by the voter has been recorded.

3. Only eligible voters must be allowed to vote.

Using a Blockchain, the most important requirements are satisfied:

• Authentication: Only registered voters will be allowed to vote.

• Anonymity: The system prevents any interaction between the votes casted by the voters and their identities.

• Accuracy: Votes once cast are permanently recorded and cannot be modified or changed under any circumstances.

• Verifiability: The system will be verifiable such that the number of votes is accounted for.

CHAPTER 4

METHODOLOGY

1. Modelling of entire e-voting process.

The system modelling helps in drawing the entire system on paper to develop a deep understanding of the system and to identify errors and flaws that can be observed before the system can be implemented.

2. Determination of the suitable technology platform to ensure anonymity, privacy ,and security .

The e-voting process requires the features like privacy, security, anonymity, and verifiability as the core function of this solution, it is important that the choice of the underlying technology is consistent to meet these challenges. It has been identified that the Blockchain technology sufficiently deals with all such challenges.

3. Development & technology integration with the perceived e-voting model .

Based on the system model, the system will be developed and will be integrated with the baseline technology. Blockchain consists of three important concepts: blocks, nodes and miners.

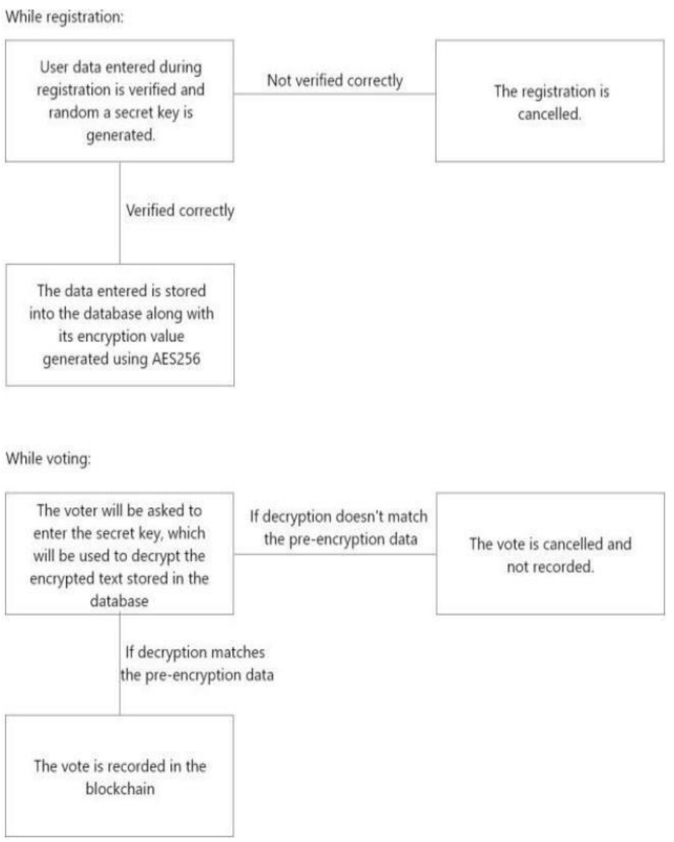

Fig 3: Flowchart for identity verification

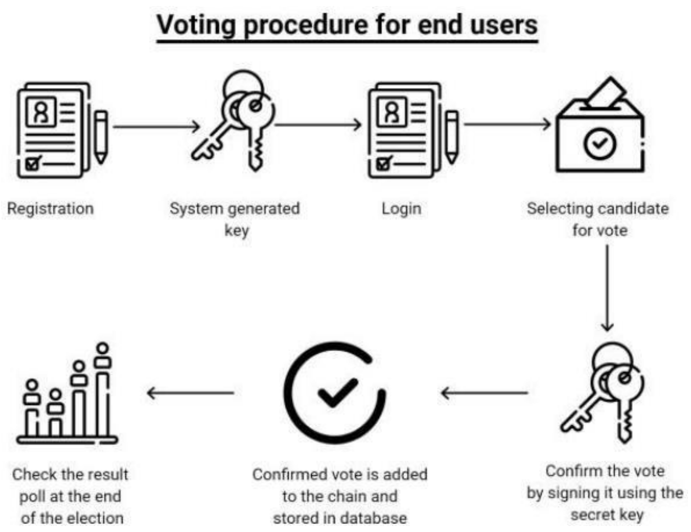

Fig 4: Voting procedure

4.1 Blocks

Every chain consists of multiple blocks and each block has three basic elements:

The data in the block.

A 32-bit whole number called a nonce. The nonce is randomly generated when a block is created, which then generates a block header hash. The hash is a 256-bit number wedded to the nonce. It must start with a huge number of zeroes (i.e., be extremely small). When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

Miners

Miners create new blocks on the chain through a process called mining. In a blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains.

Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found. When that happens, miners are said to have found the "golden nonce" and their block is added to the chain.

Making a change to any block earlier in the chain requires re-mining not just the block with the change, but all of the blocks that come after. This is why it's extremely difficult to manipulate blockchain technology. Think of it is as "safety in math" since finding golden nonces requires an enormous amount of time and computing power.

When a block is successfully mined, the change is accepted by all of the nodes on the network and the miner is rewarded financially

Nodes

One of the most important concepts in blockchain technology is decentralization. No one computer or organization can own the chain. Instead, it is a distributed ledger via the nodes connected to the chain. Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning.

Every node has its own copy of the blockchain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified. Since blockchains are transparent, every action in the ledger can be easily checked and viewed. Each participant is given a unique alphanumeric identification number that shows their transactions.

Combining public information with a system of checks-and-balances helps the blockchain maintain integrity and creates trust among users. Essentially, blockchains can be thought of as the scalability of trust via technology.

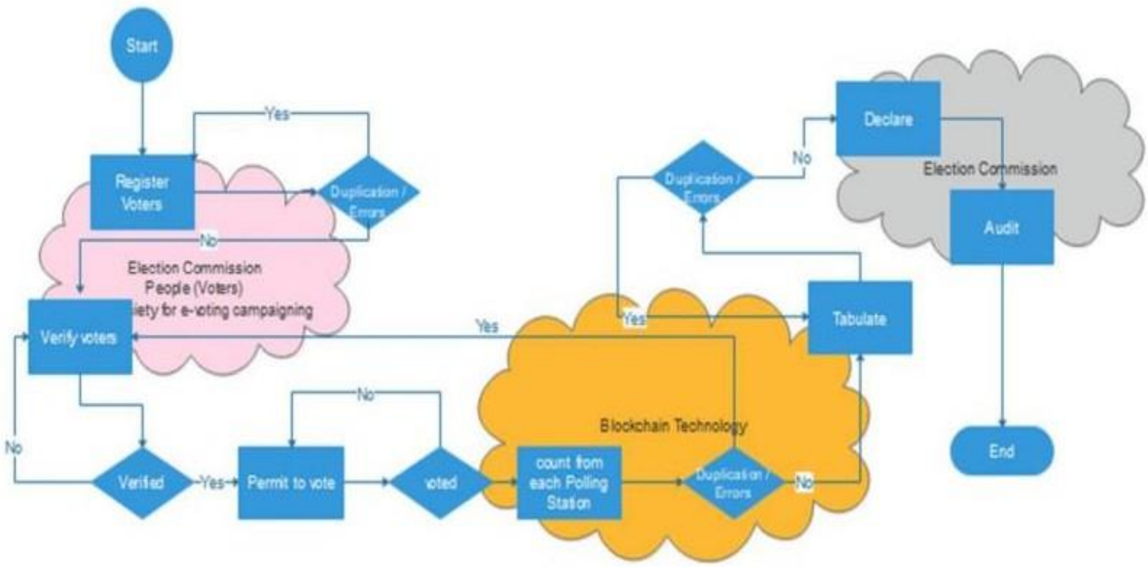

Fig 5: Voting process flowchart

Blockchain has three different types, i.e., public blockchain, private blockchain, and consortium blockchain. Bitcoin and Ethereum are the examples of public blockchain, anyone and from anywhere can join them and can get relieved at the time of his will. This is proofed by the complex mathematical functions. The private blockchain is the internal-public ledger of the company and the joining on that blockchain is granted by the company owning that blockchain.

The block construction and mining speed is far better in the private blockchain as compared to public blockchain due to the limited nodes. The consortium blockchain however exists among the companies or group of companies and instead of the consensus the principles of memberships are designated to govern the blockchain transactions more effectively. This research uses consortium blockchain as the blockchain is to be governed by a national authority in the country.

CHAPTER 5

RESULTS AND DISCUSSION

A viewpoint on the electronic voting process is presented in the report. This comprises, but is not restricted to choosing the appropriate hash algorithm, determining the polling procedure, and choosing the adjustments the voting data management procedure in the blockchain, as well as the security and authentication of the specifically the voting process are discussed.

This report's discussion of polling techniques draws inspiration from the real voting procedure utilized on the voting day, which comprises the voter's data and physical and rational verification, but just by utilizing voter lists, etc. Voters' verifiability is ensured by the electronic voting process. by its tangible documentation, such as the national identity card, and additionally verifiable through biometric verification.

The availability of the verification system on the polling time is extremely essential and the process can't be completed without the completely available system. The threats to the verification process can be extremely high if either the system is not available or the system is not in a state to be used effectively for the purpose of the voter's verification. It is the responsibility of the election commission and allied institutions to ensure that the equipment, tools, and technologies are available to make / keep the proceedings on track. The process can only be successfully completed if all the stakeholders perform their duties with extreme coherency and consistency.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

CONCLUSION

Election-related mistrust is a widespread occurrence, even in developed nations. The electronic voting, on the other hand, has become a viable substitute but is still not widely used. Although there is hope for a bright future for electronic voting, its history is not particularly impressive. In certain countries, electronic voting is not permitted, and others are working to remove the security, verifiability, and worries about anonymity. Certain matters demand extremely careful thought on the part of the legislatures, people, civil society, and technologists. This study has put forth a framework based on utilizing the configurable blockchain to detect issues with the voting procedure, choosing the appropriate hash algorithm, choosing changes for the blockchain, and data voting procedure management, as well as the voting process's security and authenticity. The power of blockchain has been used adjustably to fit into the dynamics of the electronic voting process.

FUTURE WORK

1. Blockchain is not a Distributed Computing System

   Blockchain is a network that relies on nodes to function properly. The quality of the nodes determines the quality of the blockchain. For example, Bitcoin's blockchain is strong and incentivizes the nodes to participate in the network. However, the same cannot be true for a blockchain network that does not incentivize the nodes.

2. Scalability Is an Issue

   Blockchains are not scalable as their counterpart centralized system. If you have used the Bitcoin network, then you would know that the transactions are completed depending on the network congestion. This problem is related to scalability issues with blockchain networks. In simple words, the more people or nodes join the network, the chances of slowing down is more.

3. Some Blockchain Solutions Consume Too Much Energy

   Blockchain technology got introduced with Bitcoin. It uses the Proof-of-Work consensus algorithm that relied on the miners to do the hard work. The high energy consumption is what makes these complex mathematical problems not so ideal for the real-world.

4. Blockchain Cannot Go Back — Data is Immutable

   Data immutability has always been one of the biggest disadvantages of the blockchain. It is clear that multiple systems benefit from it including supply chain, financial systems, and so on. However, if you take how networks work, you should understand that this immutability can only be present if the network nodes are distributed fairly.

5. Blockchains are Sometimes Inefficient

   Right now, there are multiple blockchain technologies out there. If you pick up the most popular ones including the blockchain technology used by Bitcoin, you will find a lot of inefficiencies within the system. This is one of the big disadvantages of blockchain.

REFERENCES

[1] EIU Democracy Index 2017. Accessed: Aug. 3, 2018. [Online]. Available: https://infographics.economist.com/2018/DemocracyIndex/

[2] ScienceDirect. Democracy Online: An Assessment of New Zealand Government Web Sites.

Accessed:Aug.1,2018.[Online].Available:https://www.sciencedirect.com/science/article/pii/S074062 4X00000332

[3] M. Volkamer, O. Spycher, and E. Dubuis, ``Measures to establish trust in Internet voting,'' in Proc. 5th Int. Conf. Theory Pract. Electron. Governance, 2011, pp. 1 6.

[4] É. Bélanger and R. Nadeau, ``Political trust and the vote in multiparty elections: The Canadian case,'' Eur. J. Political Res., vol. 44, no. 1, pp. 121 146, 2005.

[5] T. Kunioka and G. M. Woller, ``In (a) democracy we trust: Social and economic determinants of support for democratic procedures in Central and Eastern Europe,'' J. Socio-Econ., vol. 28, no. 5, pp. 577 596, 1999.

[6] T. van der Meer, ``In what we trust? A multi-level study into trust in parliament as an evaluation of state characteristics,'' Int. Rev. Administ. Sci., vol. 76, no. 3, pp. 517 536, 2010.

[7] D. Basin, H. Gersbach, A. Mamageishvili, L. Schmid, and O. Tejada, ``Election security and economics: It's all about eve,'' in Proc. Int. Joint Conf. Electron. Voting, 2017, pp. 1 28.

[8] P. Bevelander and R. Pendakur, ``Electoral participation as a measure of social inclusion for natives, immigrants and descendants in Sweden,'' Tech. Rep., 2008, p. 33.

[9] S. Wolchok et al., ``Security analysis of India's electronic voting machines,'' in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 1 14.

[10] R. L. Rivest, ``The threeballot voting system,'' Tech. Rep., 2006, p. 15.