A Project report on

Blockchain Empowered Device based voting system

A Dissertation submitted to JNTU Hyderabad in partial fulfillment of the academic requirements for the award of the degree

Bachelor of Technology

in

Computer Science and Engineering

Submitted by

GALLA NITIN
(20H51A05N6)

LOKINI NAVYA
(20H51A05E6)

KALAPALA NITHYA SRI
(20H51A05N9)

Under the esteemed guidance of

Ch. Raja Kishore Babu
(Associate Professor)

Department of Computer Science and Engineering

CMR COLLEGE OF ENGINEERING & TECHNOLOGY

(UGC Autonomous)

*Approved by AICTE *Affiliated to JNTUH *NAAC Accredited with A^+ Grade

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD - 501401.

2020- 2024

CMR COLLEGE OF ENGINEERING & TECHNOLOGY

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD – 501401

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Major Project Phase I report entitled **"Blockchain Empowered Device based Voting System"** being submitted by Galla Nitin (20H51A05N6), Lokini Navya (20H51A05E6), Kalapala Nithya Sri (20H51A05N9) in partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering** is a record of bonafide work carried out his/her under my guidance and supervision.

The results embodies in this project report have not been submitted to any other University or Institute for the award of any Degree.

Ch. Raja Kishor Babu
Associate Professor
Dept. of CSE

Dr. Siva Skandha Sanagala
Associate Professor and HOD
Dept. of CSE

ACKNOWLEDGEMENT

With great pleasure we want to take this opportunity to express our heartfelt gratitude to all the people who helped in making this project work a grand success.

We are grateful to **Ch. Raja Kishor Babu**, Associate Professor , Department of Computer Science and Engineering for his valuable technical suggestions and guidance during the execution of this project work.

We would like to thank **Dr. Siva Skandha Sanagala,** Head of the Department of Computer Science and Engineering, CMR College of Engineering and Technology, who is the major driving forces to complete my project work successfully.

We are very grateful to **Dr. Vijaya Kumar Koppula**, Dean-Academics, CMR College of Engineering and Technology, for his constant support and motivation in carrying out the project work successfully.

We are highly indebted to **Major Dr. V A Narayana,** Principal, CMR College of Engineering and Technology, for giving permission to carry out this project in a successful and fruitful way.

We would like to thank the **Teaching & Non- teaching** staff of Department of Computer Science and Engineering for their co-operation

We express our sincere thanks to **Shri. Ch. Gopal Reddy**, Secretary, CMR Group of Institutions, for his continuous care.

Finally, We extend thanks to our parents who stood behind us at different stages of this Project. We sincerely acknowledge and thank all those who gave support directly and indirectly in completion of this project work.

Galla Nitin 20H51A05N6
Lokini Navya 20H51A05E6
Kalapala Nithya Sri 20H51A05N9

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Blockchain Empowered Device Based Voting introduces a safer way to vote using new technologies using one's own device from their home. We all know voting is important, but sometimes it's not as secure as we'd like. Our approach leverages both **fingerprint** and blockchain technology for enhanced security and accountability. **Blockchain acts like an unbreakable digital vault for votes.** Each vote is locked in, impossible to alter. But we didn't stop there. We have incorporated an additional layer of safeguarding through fingerprint authentication. Just like unlocking your phone, only you can cast your vote, making the process ultra-secure.

We aim to create a user-friendly **web application/app** that effortlessly adapts to different devices, ensuring a seamless and intuitive experience. Upon casting your vote, **your fingerprint is authenticated,** and **your vote is saved in the blockchain infrastructure**. This makes sure your vote is private and free from tampering and manipulation. This project makes voting better and safer. By using these new ideas, we're making sure that voting is honest and fair for everyone.

CHAPTER 1
INTRODUCTION

CHAPTER 1

INTRODUCTION

1.1. Problem Statement

The conventional voting process faces several challenges, including security vulnerabilities and accessibility issues. Traditional methods often fall short in ensuring the integrity and privacy of votes, leaving room for manipulation and fraud. Additionally, the need for physical presence at polling stations can be a barrier to participation for many individuals, particularly those with mobility limitations or those residing in remote areas. To address these critical issues, the Blockchain Empowered Device Based Voting project aims to introduce a secure and user-friendly voting solution that leverages the power of blockchain technology and fingerprint authentication. By doing so, it seeks to revolutionize the voting experience, making it not only safer and more transparent but also more inclusive by allowing voters to cast their ballots conveniently from their own devices. This project is dedicated to enhancing the trustworthiness and accessibility of the electoral process, ensuring that voting remains a cornerstone of democratic societies.

1.2. Research Objective

The primary objective of this research is to embark on a comprehensive exploration to gain a deep and thorough understanding of the feasibility and efficacy of the groundbreaking Blockchain Empowered Device Voting system. Our aim is to revolutionize the voting process by enhancing its security and accessibility. Through a meticulous process of analysis and rigorous testing, we are dedicated to evaluating the integrity and reliability of blockchain technology in safeguarding every individual's valuable votes. In addition, we will assess the usability and potential of fingerprint authentication to ensure the utmost authenticity of voters.

Furthermore, we are committed to the design and implementation of a cutting-edge, user-friendly web application/app that seamlessly adapts to a wide array of devices, ensuring a convenient and intuitive experience for voters across the spectrum. Our ultimate goal is to provide valuable and actionable insights into the potential of this innovative voting solution to effectively address the longstanding challenges related to security and accessibility within the electoral system. In doing so, we aspire to contribute significantly to equitable elections and, in turn, foster greater civic engagement among the populace.

1.3. Project Scope and Limitations

Our main goal in this project is to improve the voting process's security and accessibility through the design, development, and evaluation of a Blockchain-powered device-based voting system. Our aim is to develop an application that is easy to use and adaptable to multiple devices. We will prioritize features like security, integrity, and convenience of use. In-depth testing will be done as part of this research to determine how well fingerprint authentication and blockchain technology work together to secure votes and confirm voter identity. The review method will include both technical and user experience components, with the goal of offering in-depth insights into the system's ability to improve the voting process.

However, limitations within the scope of this research project must be acknowledged. Our research focuses solely on the technological feasibility and security features of the system, rather than on the broader political, legal, or behavioral issues that might arise from the acceptance of such a voting solution. Second, even though we are dedicated to developing a safe and easy-to-use application, the limitations of our resources and project schedules might make it challenging for us to complete the work and have a finished production-ready product. Finally, we acknowledge that the system's acceptance and real-world implementation may face a variety of logistical, legal, and adoption obstacles that go beyond the purview of this study. However, these restrictions are essential to the project's specified objective.

CHAPTER 2
BACKGROUND WORK

CHAPTER 2

BACKGROUND WORK

2.1. DVTChain : A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system

2.1.1. Introduction

Democracy is defined as the right of people to choose their leaders. Voting is a critical process that enables people to elect their government leader. The electoral system should be democratic, independent, and impartial. As a result, it must be a transparent and secure procedure that allows everyone to share their viewpoint freely. Many people in the world do not keep faith in the election system. Conventional voting is controlled and full of mediators. Furthermore, people are dealing with a variety of issues, such as booth capture, dummy voting and the problem of proper monitoring (Rajendran, 2018), a massive line of people in front of the polling booths, false voting, pre-vote casting, redundant vote, lack of law enforcement and audits, political instability, lack of awareness, polling booths are located a long distance away from the house. Older people face significant challenges that lower the number of votes.

The Electronic Voting Machine(EVM) is the alternative to the issues with the old voting system. Nevertheless, because EVM(Electronic Voting Machine) does not fix any security concerns, it also suffers from universal approval problems. The main difficulty with EVM(Electronic Voting Machine) is that it is simple to inject any malware into the device that will mess with the server to tamper with the votes.

Since a voting system has to fulfill some security properties such as authentication, transparency, anonymity, integrity, security, privacy, mobility, fairness, and verifiability to achieve a fair and transparent result, the cost is a big issue in the case of the implementation of Ethereum-based application. We have attempted to minimize the system's computing and storage costs while maintaining its essential security properties. We explain the implementation using Ganache, a local blockchain platform integrated into Truffle, and analyze the costs associated with generic elections. We also compare the performance of the current proposal to that of prior proposals.

2.1.2. Merits, Demerits & Challenges

Merits:

1. Improved Security: The use of blockchain technology can enhance the security of the voting process. Blockchain's decentralized and immutable nature can make it difficult for malicious actors to tamper with or manipulate voting data.

2. Privacy: The abstract mentions the use of blockchain for voter anonymity by storing voter information as a hash in the blockchain. This ensures that individual votes remain private, addressing concerns about voter privacy.

3. Verifiability: The system allows voters to verify their cast votes after the election has ended. This transparency and verifiability can help build trust in the electoral process.

4. Fairness: The use of blockchain to keep casted votes encrypted until the end of the election ensures fairness, as it prevents early access to vote tallies, which could influence the outcome.

Demerits & Challenges:

1. Regulatory and Legal Challenges: The use of blockchain in voting may raise legal and regulatory questions. Ensuring the system complies with existing laws and regulationscan be a challenge.

2. Technical Challenges: Implementing a secure blockchain-based voting system can be technically complex. It requires a deep understanding of blockchain technology, smart contract development, and cybersecurity.

3. Adoption Hurdles: Convincing governments and election authorities to adopt blockchain-based voting can be challenging. Traditional paper-based voting systems are deeply entrenched in many democracies, and transitioning to a new system may face resistance.

4. Voter Education: Introducing a new voting system, especially one based on blockchain, would require extensive voter education to ensure that people understand how to use the technology securely.

5. Scalability: Blockchain systems, including Ethereum, can face scalability issues when handling a large number of transactions in a short period, which is a critical requirement during elections.

2.1.3. Implementation

The Ethereum blockchain technology is a promising option for computerized voting applications. The Ethereum blockchain provides the ability to design smart contracts. The term ”smart contract” refers to a computer program or transaction protocol designed to automatically perform appropriate activities according to the conditions of the agreement. Smart contracts have many objectives, including the elimination of trusted intermediaries, the reduction of arbitration and enforcement costs, the reduction of fraud losses, and the elimination of intentional and inadvertent exceptions. There are two kinds of accounts supported by Ethereum. An externally owned account (also known as a user-controlled account) is controlled by a user. These accounts are denoted by the letters EOA. A contract account is managed by the smart contract that is running on the computer. A contract account is denoted by the letter CA. Both kinds of accounts are capable of storing the Ethereum cryptocurrency, or ether. Ethereum does not execute operations (computations) in a smart contract without user input. As a result, before its functions may be performed, a CA must be enabled by an EOA. The EOA must buy ’gas’ in order to carry out its operations, and this must be done using the ether currency.

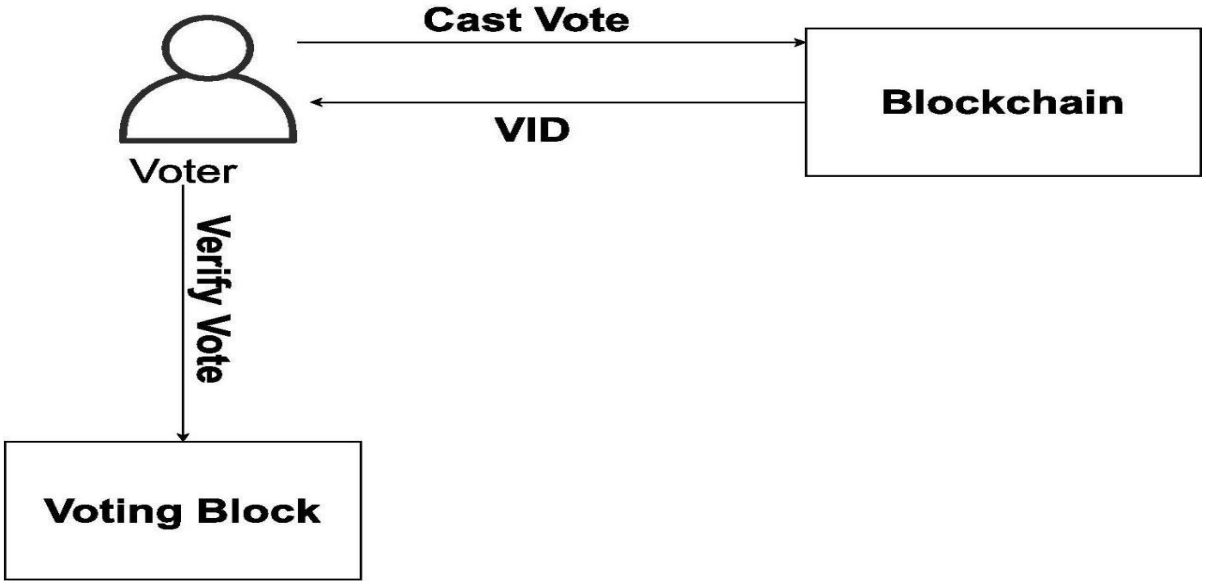

Fig. No. 2.1 Verifiability

On the server side, the proposed blockchain-based voting system employs several key components and tools to facilitate its operation. Truffle, a development tool based on the Solidity programming language, manages the network and handles smart contract development, offering features such as testing, network management, and contract administration. Solidity, as a contract-oriented high-level programming language, is used to create the smart contracts that underpin the system's functionality, and its code is compiled into bytecode for execution on the Ethereum Virtual Machine (EVM). Ganache serves as a local Ethereum RPC server, integrating with Truffle to enable local testing and simulation of blockchain networks, making it an essential tool for development. Lastly, a Node server acts as a cryptographic server, storing public and private keys essential for encrypting and decrypting casted votes, enhancing the security and privacy of the voting process. These components collectively contribute to the development, testing, and security of the blockchain-based voting system.

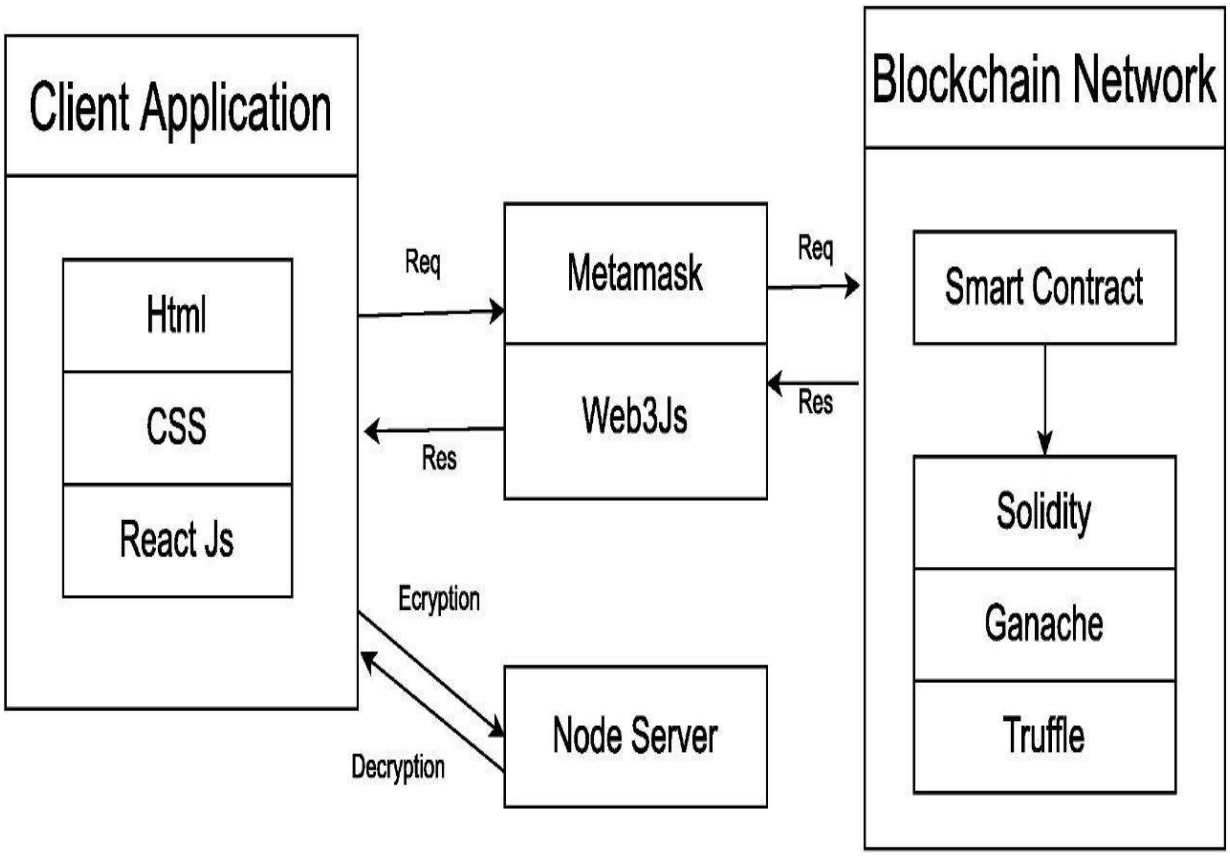

Fig. No. 2.2 Flow of implementation

2.2. Blockchain for Electronic Voting System

2.2.1. Introduction

Electoral integrity is essential not just for democratic nations but also for state voter's trust and liability. Political voting methods are crucial in this respect. From a government standpoint, electronic voting technologies can boost voter participation and confidence and rekindle interest in the voting system. 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. The voting system is the method through which judges judge who will represent in political and corporate governance.

Democracy is a system in which voters elect representatives by voting. The efficacy of such a procedure is determined mainly by the level of faith that people have in the election process.

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. The secret voting model has been used to enhance trust in democratic systems since the beginning of the voting system.

Blockchain technology offers a decentralized node for online voting or electronic voting Recently distributed ledger technologies such as blockchain were used to produce electronic voting systems mainly because of their end-to-end verification advantages. Blockchain is an appealing alternative to conventional electronic voting systems with features such as decentralization, non-repudiation, and security protection. It is used to hold both the boardroom and public voting. A blockchain, initially a chain of blocks, is a growing list of blocks combined with cryptographic connections. Each block contains a hash, timestamp, and transaction data from the previous block. The blockchain was created to be data-resistant.

Voting is a new phase of blockchain technology; in this area, researchers are trying to leverage benefits such as transparency, secrecy, and non-repudiation that are essential for voting applications.

2.2.2. Merits, Demerits and Challenges

Merits:

1. Decentralization: Blockchain technology provides a decentralized network for online voting, reducing reliance on a central authority and enhancing the system's resilience.

2. End-to-end Verification: Distributed ledger technologies, like blockchain, offer end-to-end verification advantages, ensuring the integrity of the voting process.

3. Non-Repudiation: Blockchain introduces non-repudiation features, meaning participants cannot deny their involvement in the voting process, enhancing accountability.

4. Security Protection: The use of blockchain in electronic voting systems enhances security, protecting against tampering or unauthorized access to voting data.

5. Blockchain Structure: A blockchain consists of a chain of blocks, each containing a hash, timestamp, and transaction data from the previous block, creating a tamper-resistant record.

Demerits & Challenges:

1. Scalability Concerns: Blockchain systems may face scalability challenges when handling a large number of transactions simultaneously, potentially slowing down the voting process.

2. Complexity in Implementation: Integrating blockchain into existing voting systems can be complex, requiring significant technical expertise and resources.

3. User Accessibility: The use of blockchain in voting might pose challenges for less tech-savvy individuals, potentially excluding certain demographics from the voting process.

4. Vulnerability to Cyber Attacks: While blockchain is known for its security features, no system is entirely immune to cyber threats. A targeted attack could compromise the integrity of the voting process.

2.2.3. Implementation

Whether talking about traditional paper-based voting, voting via digital voting machines, or an online voting system, several conditions need to be satisfied:

• Eligibility: Only legitimate voters should be able to take part in voting;

• Unreusability: Each voter can vote only once;

• Privacy: No one except the voter can obtain information about the voter's choice;

• Fairness: No one can obtain intermediate voting results;

• Soundness: Invalid ballots should be detected and not taken into account.

• Completeness: All valid ballots should be tallied correctly.

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. However, because this sort of system is necessary for a wide range of other contexts, especially those related to digital government services, researchers believe it is best to use an existing identification system, and the question of creating one is beyond the scope of work.

Unreusability: At first, glance, implementing unreusability 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 unreusability and voter anonymity is tricky. Moreover, it may be necessary to allow the voter to re-vote, making the task even more complex. A brief overview of unreusability techniques will be provided below in conjunction with the outline on implementing privacy.

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)).

Homomorphic encryption is a form of encryption that allows mathematical operations to be performed on encrypted data without decryption, for example, the addition Enc(a) + Enc(b) = Enc(a + b); or multiplication Enc(a) × Enc(b) = Enc(a × b). In the context of online voting, additive homomorphic encryption allows us to calculate the sum of all the voters' choices before decryption. It is worth mentioning here that multiplicative homomorphic encryption can generally be used as an additive. For example, if we have choices x and y and multiplicative homomorphic encryption, we can select a value g and encrypt exponentiation: Enc(gx) × Enc(gy) = Enc(g(x + y)).

Fairness: Fairness in terms of no one obtaining intermediate results is achieved straightforwardly: Voters encrypt their choices before sending, and those choices are decrypted at the end of the voting process. The critical thing to remember here is that if someone owns a decryption key with access to encrypted decisions, they can obtain intermediate results. This problem is solved by distributing the key among several stakeholders. A system where all the key holders are required for decryption is unreliable one of the key holders does not participate, decryption cannot be performed. Therefore, threshold schemes are used whereby a specific number of key holders are required to perform decryption. There are two main approaches for distributing the key: secret sharing, where a trusted dealer divides the generated key into parts and distributes them among key holders (e.g., Shamir's Secret Sharing protocol); and distributed key generation, where no trusted dealer is needed, and all parties contribute to the calculation of the key (for example, Pedersen's Distributed Key Generation protocol).

2.3 Securing e-voting based on blockchain in P2P network

2.3.1. Introduction

Voting is a method to make a collective decision or express an opinion among a group or a meeting or electorates. Voting is usually following debates, discussions, and election campaigns. During voting, the person to be elected is the candidate of an election, and the person who casts a ballot for their chosen candidate is the voter. Usually, the voter can vote under the list of candidates or vote for any other person he/she prefers. Voting ballots must be unsigned and marked by the voters in private booths so that no one else can find out for whom a citizen is voting. Since the 17th century, voting has been the usual mechanism by which modern representative democracy has operated.

Voting is also used in many other private organizations and groups, such as clubs, corporations, and voluntary associations. With the rapid development of the Internet and information technologies, many conventional offline services such as voting, mail, and payment, are migrating to online ones. The online voting is known as electronic voting (e-voting). It is an electronic means for casting and counting votes. Users of e-voting are voters and election authorities. The voter can submit his/her or her votes electronically to the election authorities from any location via e-voting. The election authorities are responsible for collecting votes from voters. E-voting can save time and effort with high efficiency and flexibility, which is getting more and more attention instead of traditional voting. With the development of the Internet, e-voting has become an important means for many organizations. Proposed an efficient E2E verifiable e-voting system without setup assumptions and proposed a certificate deniably authenticated encryption and its application to the e-voting systems. proposed a blockchain-enabled e-voting system.

With the advent of the internet and technological advancements, electronic voting (e-voting) has emerged as a promising alternative to traditional voting methods, offering increased efficiency and accessibility. Moreover, recent innovations, such as blockchain-enabled e-voting systems, aim to further enhance the transparency and security of the electoral process.

2.3.2. Merits, Demerits and Challenges:

Merits:

1. **Security Enhancement:** The use of blockchain technology in e-voting offers a significant improvement in security. It helps prevent the forgery of votes through a synchronized model of voting records, ensuring the integrity of the electoral process.
2. **Authentication and Non-Repudiation:** The user credential model based on elliptic curve cryptography (ECC) adds an additional layer of security by providing authentication and non-repudiation, ensuring that each vote is cast by an authorized voter and cannot be denied.
3. **Vote Withdrawal Option:** The inclusion of a withdrawal model that allows voters to change their votes before a preset deadline enhances voter flexibility and ensures that voters are not locked into their choices prematurely.
4. **Decentralized and Transparent:** Blockchain's decentralized nature makes the e-voting system more resilient to tampering or hacking, and the use of distributed ledger technology (DLT) provides transparency and accountability.
5. **Practical Implementation:** The successful implementation of the blockchain-based e-voting system on Linux platforms demonstrates its practicality and ability to solve the problem of vote forgery, providing a viable solution for secure e-voting.

Demerits and Challenges:

1. Accessibility: Some individuals may not have access to the necessary technology or internet connectivity to participate in e-voting, potentially disenfranchising certain segments of the population.

2. Regulatory and Legal Challenges: Adapting existing electoral laws and regulations to accommodate blockchain-based e-voting may be complex, and ensuring compliance with legal standards is crucial.

3. Public Trust: Building public trust in blockchain-based e-voting is a significant challenge. Convincing voters that their votes are secure and private is crucial for widespread adoption.

4. Technical Infrastructure: E-voting requires a reliable technical infrastructure, including internet access and devices. Ensuring that all eligible voters have access to this infrastructure can be a challenge in some regions.

5. Privacy Concerns: While the use of blockchain enhances the privacy of votes, there may still be concerns about the potential for voter data to be mishandled or misused.

2.3.3.Implementations

The study of this paper originates from a need to design a more secure and practical e-voting system since it has become a popular topic in the area of industry and information security. Blockchain is based on DLT and was invented by Satoshi Nakamoto in 2008. Blockchain is a growing list of blocks. Each block except the first block stores its previous block's hash value. It synchronizes the ledgers replicated among multiple nodes by using community validation, which is adapted to serve as the public transaction ledger of the cryptocurrency Bitcoin.

Compared with the original blockchain, the improvements are as follows: (1) We design a synchronized model of voting records based on DLT to avoid forgery of votes. (2) We design a user credential model based on ECC to provide authentication and non- repudiation. (3) We design a withdrawal model that allows voters to change their vote before a preset deadline. By integrating the above designs, we propose a blockchain-based e-voting scheme, which meets the essential requirements of the e-voting process. We illustrate the blockchain-based e-voting scheme as follows: (1) The blockchain-based e-voting scheme is public, distributed, and decentralized. It can record votes from voters across many mobile devices and computers. (2) The blockchain-based e-voting scheme allows the voters to audit and verify the votes inexpensively. (3) The database of votes is managed autonomously and uses a distributed server of timestamps on a peer-to-peer network. (4) Voting on blockchain is a workflow where voters' regarding data security is marginal, which removes the characteristic of infinite reproducibility from e-voting.

Based on the illustration above, Fig. 1 is designed as follows: (1) Voting blockchain: it is a growing list of voting blocks. (2) Voters: the person who casts a ballot for his chosen candidate is a voter. The voter can vote or withdraw a vote. (3) Voting office: it is the organization of voting.It can query the public key of the voter, and verify the votes votes.

(4) Public key infrastructure (PKI): it is a set of procedures that manage public-key encryption. (5) Vote database: it is a database according to the statistics of votes that are updated by the voting office. (6) Miners: the responsibility of miners is to deal with accepted votes and add them to the public voting blockchain.

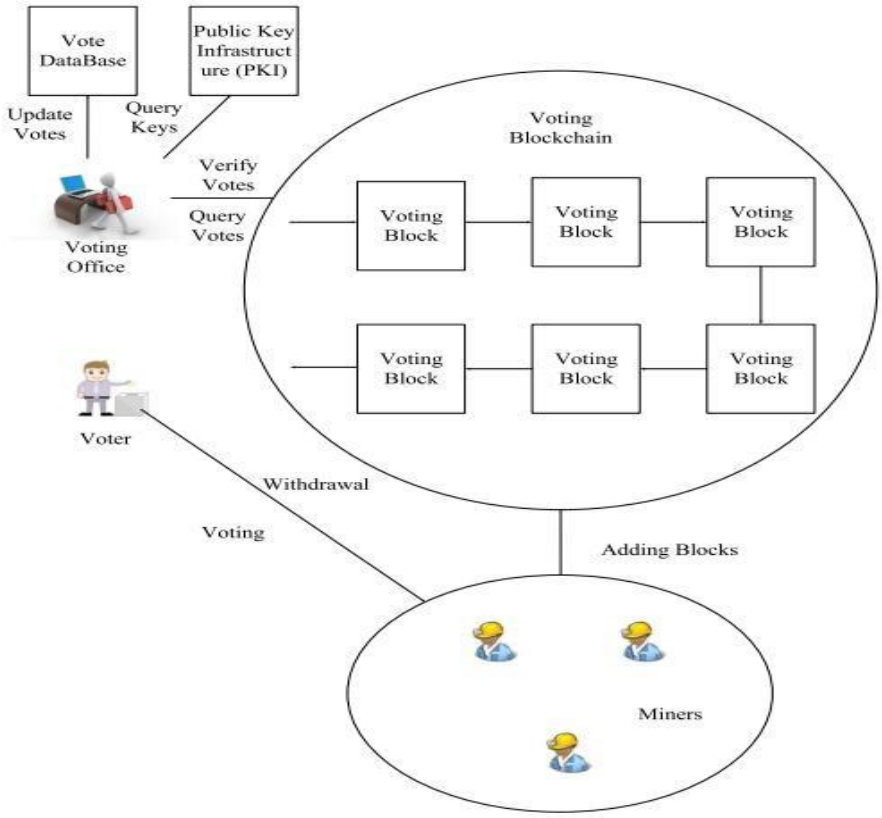

Fig. No. 2.3 Blockchain-based e-voting scheme

We design a blockchain-based scheme for secure e-voting. First, a synchronized model of voting records based on DLT is designed to avoid the forgery of votes. Second, a user credential model based on ECC is designed to provide authentication and non-repudiation. Third, a withdrawal model is designed that allows voters to change their vote before a preset deadline. We introduce the block definition, user credential based on ECC, computing the hash value based on SHA-256, and mining and generation of voting blocks in the following.

CHAPTER 3
RESULTS AND DISCUSSION

CHAPTER 3

RESULTS AND DISCUSSION

The results and discussions are apparently about the background work we had done, that is, how the existing solutions are helpful or informative about the solution we are making. Let's discuss how this is happening:

1) DVTChain: A blockchain-based decentralized mechanism to ensure the security ofdigital voting system voting system

It is evident that the proposed DVTChain, a blockchain-based decentralized mechanism for securing digital voting systems, holds several notable merits. These include significantly enhanced security through the immutability and decentralization of blockchain technology, ensuring the integrity of the voting process. Furthermore, the system addresses concerns about voter privacy by anonymizing voter information through hashing and allows voters to verify their cast votes post-election, enhancing transparency and trust in the electoral process. The approach also ensures fairness by preventing early access to vote tallies. However, it's crucial to acknowledge the challenges and demerits associated with implementing such a system. Regulatory and legal hurdles, technical complexities, adoption resistance, the need for extensive voter education, and potential scalability issues are significant considerations.

2) Blockchain for Electronic Voting System

Blockchain technology is being explored for electronic voting systems due to its decentralization, non-repudiation, and security advantages. However, its implementation presents challenges like scalability, complexity, and accessibility. Despite its security features, it remains susceptible to cyber threats. To ensure online voting requirements are met, factors like eligibility, unreusability, privacy, fairness, soundness, and completeness must be considered. This involves utilizing trusted identification systems, techniques like blind signatures and homomorphic encryption for privacy, and secure key distribution to prevent unauthorized access to intermediate results. The choice between methods like secret sharing and distributed key generation is vital for system reliability.

3) Securing e-voting based on blockchain in P2P network

In this section, we illustrate the scheme and implement the system on the Linux platform. We use Python programming language for source codes. The Linux platform for implementation is Ubuntu. Each block contains the voter's ID, vote, voter's signature, timestamp, and hash of the previous block. Blockchain-based e-voting system for multiple candidates has been designed on Linux platforms. Compared with other e-voting systems, blockchain-based e-voting system is more secure and anonymous. (1) Anonymous: each user in a blockchain-based e-voting system uses an ID instead of his real identity and the system is decentralized without a third party. Thus, the privacy of the users is protected. (2) Security: we design a synchronized model of voting records based on DLT to avoid forgery of votes. Thus, it is very difficult to forge votes. (3) Non-repudiation: we design a user credential model based on ECC to provide authentication and nonrepudiation. Thus, it is very difficult to deny a vote. (4) Withdrawable: we design a withdrawal model that allows voters to change their vote before a preset

Comparison:

The first three paragraphs explain the basics of using blockchain for secure voting systems and talk about its pros and cons, like security and technical difficulties. On the other hand, the abstract for "Blockchain Empowered Device Based Voting" focuses on a specific voting solution that's easy to use. It uses your fingerprint and blockchain to make voting secure and convenient. It also mentions some extra security measures like sending an OTP to your phone and using a system called IPFS to keep the results safe. So, the abstract tells you about a specific, user-friendly way to make voting better and safer using modern technology.

Integration:

Bringing together the big picture and a practical solution,s The first part explains the benefits and challenges of using blockchain for voting, like making it more secure and transparent. In the abstract, it gets specific, showing how you can vote securely from your own device using your fingerprint. They also mention using extra security steps like sending an OTP to your phone. So, it's like going from the idea of better voting to actually making it easier and safer for people. It's a step from talking aboutit to making it happen.

CHAPTER 4
CONCLUSION

CHAPTER 4

CONCLUSION

The goal of this research is to analyze and evaluate current research on blockchain-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

REFERENCES

1. Liu Y., Wang Q. An E-voting Protocol Based on Blockchain. IACR Cryptol. Eprint Arch.2017;2017:1043.

2. Shahzad B., Crowcroft J. Trustworthy Electronic Voting Using AdjustedBlockchainTechnology. IEEE Access. 2019;7:24477–24488. doi: 10.1109/ACCESS.2019.2895670.

3. Racsko P. Blockchain and Democracy. Soc. Econ. 2019;41:353–369. doi:10.1556/204.2019.007.

4. Yaga D., Mell P., Roby N., Scarfone K. Blockchain technology overview.arXiv.20191906.11078

5. The Economist EIU Democracy Index. [(accessed on 18 January 2020)];

2017 Available online: https://infographics.economist.com/2018/DemocracyIndex/

6. Cullen R., Houghton C. Democracy online: An assessment of New Zealand government web sites. Gov. Inf. Q. 2000;17:243–267. doi: 10.1016/S0740-624X(00)00033-2.

7. Schinckus C. The good, the bad and the ugly: An overview of the sustainability of blockchain technology. Energy Res. Soc. Sci. 2020;69:101614. doi: 10.1016/j.erss.2020.101614.

8. Morris, David Z. (15 May 2016). "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting". Fortune .

9. Popper, Nathan (21 May 2016). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". The New York Times.

10. "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency.

11. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton, New Jersey: Princeton University Press. ISBN 978-0-691-17169-2.