ABSTRACT

Electronic voting machines created all through the past twenty years with the aid of authorities- owned corporations are really totally used to conduct elections in India. These machines, called EVMs in India, have received praise for their straightforward construction, usability, and dependability; despite the fact that, in recent times, they have additionally come below the fireplace in response to several reviews of election fraud. Notwithstanding this criticism, the machines have now not passed through a thorough, independent safety examination, and many aspects in their layout have in no way been made publicly available. vote casting is an vital factor of democratic regimes as it allows individuals of a society to specific their opinions. Voter turnout has declined these days, whilst issues approximately the reliability, protection, and accessibility of the present balloting technologies have grown. E-voting was created to overcome those issues, but it's miles are still highly-priced and desire complete oversight from a centralised authority. New possibilities to create new forms of digital services are being supplied with the aid of a blockchain even though the sphere of examination is reasonably younger. To increase a brand-new digital voting gadget that is probably utilised in municipal or national elections, we will make use of the open supply Blockchain era. The Blockchain-based total machine could be secure, reliable, and nameless, and it will make a contribution to an upward thrust in voter turnout and public self-assurance in their governments. Blockchain, a decentralised and immutable ledger, presents a disbursed and transparent platform for recording and verifying transactions. by making use of blockchain to e-voting, a comfy and obvious environment is created, enabling the electorate to forge their ballots with confidence even as keeping the integrity of the election consequences. Each vote is recorded as a transaction at the blockchain, forming a series of blocks that are cryptographically related and time-stamped.

Keywords: EVM, Blockchain, E-voting

S.NO. TABLE OF CONTENTS PAGE NO.

LIST OF FIGURES

CHAPTER - 1
INTRODUCTION

The Internet is the greatest thing invented by humanity. But there are some flaws on the internet. Consider a situation where you are depositing money or casting a vote, there is a single point of authority, and we are supposed to believe him/her with our data/money/vote. The limitation of the present system is a single point of control/failure. The Authority may or may not be telling the truth or corrupted. The solution to this is to employ a decentralised and distributed system where the consensus of the users/peers is used to evaluate the transactions/votes/data. We are creating a web portal for casting a vote online. But our work is not over, Securing the casted vote is a challenging one. Many fraudsters try to manipulate the data in their favour. In our case, It doesn't occur because we created it with the help of blockchain technology.

1.1 EVM MACHINE AND IT'S WORKING:

The 1982 Assembly elections in Kerala's Paravur constituency saw the first deployment of electronic voting machines (EVMs) made by two government-owned firms, Electronics Corporation of India (ECIL) and Bharat Electronics Limited (BEL), in 50 polling places. Section 61A of the Act and Regulations, which adopted the use of EVMs for the elections, was added by Parliament in 1992. The Control Unit, which is primarily used by the polling officer to open the ballot for voting, is on the left of the EVM and is connected to the Ballot Unit, which is on the right, by a 5-metre cable. The Ballot Unit contains the list of candidates, symbols, and a button next to their names for the voters to vote. The control unit is the major part of the EVM that stores the total number of votes cast. The control unit's lower portion has a seal with a result button that may be

used to view the total number of votes cast in the machine during the counting of ballots. The list of candidates is listed in alphabetical order in the Ballot unit.

Figure 1.1 EVM machine

A ballot unit can have up to 16 candidates on it. A second ballot unit is attached to the initial ballot unit if the number of candidates is greater than 16. The Voter Verifiable Paper Audit Trail (VVPAT), another independent element that is crucial to voting, prints a slip with the name, symbol, and a serial number of the candidate for whom the voter has cast their ballot so that they may confirm their vote. This slip will be seen for seven seconds before it is placed in the locked drop box.

When a voter arrives to cast their ballot, the poll worker checks their identification, takes their signature and thumbprint, and inks their finger. The officer then opens the ballot for voting, requiring their fingerprint to be on the Control unit. The ballot is now available for voting, and the voter selects their preferred candidate by pressing the button on the ballot unit next to their name and symbol. The presence of the button is shown by a red Light nearby. The candidate's name, symbol, and serial number are now printed on the VVPAT slip for the voter to confirm.

1.2 PROBLEM IN EVM MACHINE:

The EVM was examined for any weaknesses, and in 1990, a committee discovered two potential issues: the system could be switched out for a fake one

to alter the results, and a device could be inserted into the cable linking the Ballot unit and the Control unit to alter the EVM's results. The coding underlying the EVM was not examined in this study; rather, it solely examined how the machine operated and functioned. A second investigation conducted by an IIT team in 2006 didn't verify the coding portion either. Instead, it recommended adding dynamic key coding to timestamp button presses and informing users when several buttons are hit.

Figure 1.2 Voter ID

Voter verification is one of the main issues with the electoral process. Voting with false identification, impersonation, a corrupt verification officer, and allowing the casting of bogus votes are a few examples. Another widespread problem was that when a voter touches any button, their vote is only going to one candidate. This can be the result of replacing the machine with a phone or altering the machine's program. Or paying the engineers to modify the machinery so that it works for the Candidate’s benefit. Moreover, cheating in calculations is possible, as many have just become aware of.

1.3 BLOCKCHAIN:

A blockchain is a collection of blocks connected by means of cryptographic chains. One of the technologies, blockchain, has strong cryptographic underpinnings that allow apps to take advantage of these capabilities to provide sturdy safety solutions. Here, the information is broken up into blocks and related

via hyperlinks. every block includes a completely unique hash cost that serves as an illustration of the block. The relationship between each block is created through incorporating the preceding block's hash into the cutting-cutting modern block. A block is made of the statistics segment, hash, phase, hash, and prior hash, to summarise the chain of blocks that had been fashioned not gets saved in a single device. every user of the blockchain, additionally referred to as the allotted Current, has their replica. whilst someone attempts to adjust the information, the hash cost is altered, the hyperlink is damaged, and the hash cost is altered. The attacker must adjust and recalculate the hashes of succeeding blocks for the assault to be triumphant. customers curate each block as soon as it's miles made relying on their consensus, and every block can either be conventional or rejected. As a result, protection, immutability, and transparency are supplied through blockchains. Public, personal, and consortium blockchains are the 3 essential kinds of blockchains now in use.

1.4 THREE PARTS OF BLOCKCHAIN TECHNOLOGY:

Seeing a blockchain as a database, A blockchain can be regarded as a distributed database with many users. every consumer obtained admission to the essential. The fundamental conditions for a blockchain are peer-to-peer networking, asymmetric peer-to-peer networking, uneven cryptography, hashing, and uneven cryptography. Decentralised, open-source Ethereum is a blockchain that helps clever contracts. The platform's local cryptocurrency is known as Ether (ETH). After Bitcoin, it has the second one-biggest marketplace capitalization among cryptocurrencies. The blockchain with the best usage is Ethereum. Programmer Vitalik Buterin got here with the idea for Ethereum in 2013. Crowdfunding for the assignment started in 2014, and on July 30, 2015, the community went live with 72 million pre-mined coins. Turing-complete code may be run on the Ethereum virtual device (EVM), which can also run decentralised programs. Ethereum has been used for server initial coin services and is used for

decentralised financing. A piece of code referred to as a smart contract is used to make choices and behaviour transactions. Ethereum's smart Contracts are created using the Solidity programming language.

1.5 OBJECTIVES:

Voters who are Non-Residential Indians and physically challenged can vote from anywhere in the world until they possess citizenship of the country. The voter percentage should be clean as there will be no involvement of proxy or face votes. We can increase the healthiest vote percentage in every constituency. We can verify the data so that there will be less chance of mistakes counting. Hacking and manipulating the voters is not possible because of blockchain.

1.6 PROPOSED METHOD:

We have advised remodelling the present day on line vote casting device such that it includes Blockchain generation. via the usage of two awesome units of modules, we have worked on the subsequent principles: election commission and voter (s). Elections are created by using the Election commission, which additionally adds registered candidates and parties to contest them. The information is displayed at the voter's front end for voting the use of an election's rest API housed on Ethereum's Blockchain. The Election commission then retrieves the vote from our blockchain infrastructure after the vote has been solid. The disadvantage of not using the conventional method of clever contracts is that the blockchain framework we created cannot run on the primary network as it needs to be hosted and distinct web3 providers have to be used to engage with it. in addition, the shortage of a public API for voter identity consequences within the loss of vote authentication. The objectives of our project leveraging Blockchain technology to enhance the current online voting method. To lessen the work involved in putting up an election station and holding physical elections. Voting is entirely online, so non-resident Indians can participate.

CHAPTER 2

LITERATURE SURVEY

Ahmed Ben Ayed et al have been thinking of Conceptual secure Conceptual comfy blockchain based electronic balloting machine. New opportunities to create new sorts of digital offerings are being supplied by blockchain. Despite the fact that having a look at the issue remains in its early stages, it has in large part focused on the technological and criminal problems in place of utilising this revolutionary idea and growing stepped forward digital offerings. In this paper, we will endorse a concept for a brand-new digital voting system that is probably used in municipal or county wide elections with the aid of utilising the open source Blockchain era. The Blockchain-based system could be secure, reliable, and nameless, and it will make a contribution to a rise in voter turnout and public self-belief in their governments.

Hari K. Prasad Arun Kankipati Sai Krishna Sakhamuri et al have been taught security analysis of electronic voting machines electronic voting machines created during the past 20 years by two government-owned enterprises are virtually solely used to conduct elections in India. These machines, known as EVMs in India, have received praise for their straightforward construction, usability, and dependability; nevertheless, in recent times, they have also come under fire in response to several reports of election fraud. Despite this criticism, many aspects of the machines' design have never been made available to the public, and they haven't gone through a thorough, impartial security assessment. In this work, we analyse the security of an actual Indian EVM that we got from an unnamed source.

We go into great detail about the machine's construction and operation and assess its security in light of applicable election protocols.

Subhash Bahadur Thapa, Suraj B have been taught that voting using blockchain voting is a crucial aspect of democratic regimes due to the fact it permits individuals of a community to express their evaluations. Voter turnout has declined these days, even as concerns about the reliability, protection, and accessibility of the cutting-edge vote casting technology have grown. voting became created to conquer those troubles, but it is nonetheless high-priced and desires entire oversight from a centralised authority. a brand new, decentralised, and dispensed era referred to as the blockchain has the capacity to improve several industries' various facets. components are required for the blockchain- primarily based vote casting task to feature and integrate as an entire. one in every of them will be the Election fee, that is in charge of putting in place elections and including registered parties and candidates who're strolling for office using clever contracts. The voter's module might be on the opposite side, where every person can forge a ballot for their personal assembly Constituency. The ballot could be recorded at the blockchain to make it tamper evidence.

Kshetri, N. (2017) This paper provides an overview of how blockchain technology can enhance the security and transparency of voting systems. It discusses various aspects such as immutability, decentralisation, and cryptographic techniques employed in blockchain-based e-voting systems.

Zohren, S., et al. (2020) This survey paper explores different blockchain-based e-voting systems proposed in literature. It discusses the advantages

and challenges associated with implementing such systems, including scalability, anonymity, and resilience to attacks.

Yavuz, A. A., & Polat, H. (2018) This paper presents a detailed design and implementation of an e-voting system using blockchain technology. It covers various technical aspects such as smart contracts, encryption techniques, and user authentication mechanisms.

Huh, J. H., & Cho, S. W. (2017) The authors describe the implementation and evaluation of a blockchain-based e-voting system. They discuss the system architecture, security features, and performance evaluation metrics such as throughput and latency.

Fatima, M., et al. (2020) This paper proposes a secure e-voting system architecture leveraging blockchain technology. It emphasises the importance of cryptographic techniques and decentralised consensus mechanisms in ensuring the integrity and confidentiality of votes.

White, S. J., & Ruoti, S. (2018) The paper examines the potential impact of blockchain-based e-voting systems on election transparency and voter confidence. It discusses how blockchain technology can address concerns such as vote manipulation and tampering.

CHAPTER 3

OBJECTIVES AND METHODOLOGY

3.1 OBJECTIVES:

The objective of an E-voting system using blockchain is to create a secure and transparent platform for conducting fair and democratic voting processes. This system utilises blockchain technology to ensure the accuracy and security of the voting process by providing an immutable and decentralised ledger of all transactions.

3.2 METHODOLOGY:

The working methodology of an E-voting system using blockchain can be summarised in the following steps:

3.2.1 Identity verification

Voters are required to register and provide their identity information to be verified before being able to vote. The identity verification process is conducted by a trusted third-party organisation. Identity verification is an essential aspect of an online polling system using blockchain technology. The goal of identity verification is to ensure that the person casting the vote is authorised to do so and that the voting process is conducted fairly and securely. The process of identity verification involves several steps, including collecting personal information from the voter, verifying the identity of the voter, and ensuring that the voter is eligible to vote.

Blockchain technology provides a secure and transparent platform for identity verification. The blockchain ledger can be used to store and verify identity information, which ensures the accuracy and security of the voting

process. The blockchain ledger is decentralised, which means that there is no central authority or control, and the risk of fraud is significantly reduced.

The identity verification process starts with the collection of personal information from the voter, such as name, address, and date of birth. This information is stored on the blockchain network, where it can be accessed and verified by the network participants. Once the personal information is collected, the identity of the voter is verified using various methods, such as facial recognition or biometric authentication. This ensures that the person casting the vote is the same person whose identity has been verified.

Ultimately, the voter's eligibility to vote is checked, which includes their citizenship or age. that is additionally tested the usage of the facts saved at the blockchain community. It's far a critical aspect of an online polling machine, the use of blockchain generation. The use of the blockchain era affords a comfortable and obvious platform for verifying voter identification, ensuring the accuracy and safety of the vote casting procedure. The decentralised nature of the blockchain network considerably reduces the chance of fraud and guarantees that the voting system is performed fairly and securely.

3.2.2 Creation of a digital ballot:

A digital ballot is created, and candidates or propositions are listed. The creation of a digital ballot is an essential aspect of an online polling system using blockchain technology. The digital ballot is a list of candidates or propositions that voters can choose from when casting their vote. The goal of creating a digital ballot is to ensure that the voting process is fair and

transparent, and that all eligible voters have an equal opportunity to cast their vote.

To create a digital ballot, the blockchain network first collects all the candidates or propositions that will be included in the ballot. This information is then verified to ensure that it meets the eligibility criteria for inclusion in the ballot. Once the information is verified, it is added to the blockchain network, and a digital ballot is created.

The digital ballot is designed to be user-friendly and accessible to all eligible voters. It may include information about each candidate or proposition, such as their name, party affiliation, and a brief description of their platform. The digital ballot may also include instructions on how to cast a vote and how to verify that the vote has been successfully recorded on the blockchain network.

The usage of the blockchain era within the creation of a virtual ballot affords numerous benefits. The decentralised nature of the blockchain community ensures that the vote casting procedure is transparent and comfy, as there may be no valuable authority controlling the system. Moreover, the blockchain ledger offers an immutable file of all transactions, which guarantees that the integrity of the voting manner is maintained.

The digital ballot is designed to be user-friendly, transparent, and secure, ensuring that all eligible voters have an equal opportunity to cast their vote. The use of blockchain technology provides a decentralised and immutable ledger, which ensures that the voting process is conducted fairly and transparently, without the risk of fraud or manipulation.

3.2.3 Encryption of Votes:

Voters cast their votes anonymously, and the vote is encrypted using advanced cryptography. Encryption of votes is an vital element of an online polling gadget the use of the blockchain era. The purpose of encrypting votes is to make certain that the votes are nameless, comfortable, and can not be manipulated or tampered with. Encryption is performed through the usage of superior cryptographic algorithms, which make certain that the votes are securely saved at the blockchain network. Once a voter has solid their vote, the vote is encrypted using superior cryptographic algorithms. This ensures that the vote is anonymous and can not be traced back to the voter who solidified it. The encrypted vote is then delivered to the blockchain network, in which it can be validated and counted. Using blockchain generation in the encryption of votes affords numerous advantages. The decentralised nature of the blockchain network ensures that the vote casting method is obvious and comfortable, as there's no critical authority controlling the system. In addition, the usage of cryptography ensures that the votes are cosy and cannot be manipulated or tampered with.

To ensure that the encryption of votes is secure, the cryptographic algorithms used are constantly updated and reviewed. This ensures that the voting process remains secure and that the risk of fraud or manipulation is minimised. The use of advanced cryptographic algorithms ensures that the votes are anonymous, secure, and cannot be manipulated or tampered with. The decentralised nature of the blockchain network ensures that the voting process is transparent and secure, providing voters with confidence in the integrity of the voting process. The use of cryptography is constantly reviewed and updated, ensuring that the voting process remains secure and that the risk of fraud or manipulation is minimised.

3.2.4 Distribution of the encrypted votes:

The encrypted votes are distributed across the blockchain network, which consists of multiple nodes, each of which has a copy of the ledger.The distribution of encrypted votes is a crucial aspect of an online polling system using blockchain technology. Once the votes have been validated and counted, the next step is to distribute the encrypted votes to authorised participants who have access to the decryption key. This distribution process ensures that the authorised participants can decrypt the votes and tally them up. The distribution of encrypted votes is carried out through a process known as key management. The decryption key is generated by the blockchain network, and only authorised participants have access to it. These participants use the key to decrypt the encrypted votes, tally them up, and record the results on the blockchain ledger. The decentralised nature of the blockchain network ensures that the distribution process is transparent and secure, as there is no central authority controlling the process. The use of blockchain technology in the distribution of encrypted votes provides several benefits. The decentralised nature of the blockchain network ensures that the distribution process is transparent and secure, providing voters with confidence in the integrity of the voting process. Additionally, the use of key management ensures that only authorised participants have access to the decryption key, minimising the risk of fraud or manipulation.

To ensure that the distribution of encrypted votes is secure, the key management process used is constantly updated and reviewed. This ensures that the voting process remains secure and that the risk of fraud or manipulation is minimised. The key management ensures that only authorised participants have access to the decryption key, minimising the risk of fraud or manipulation. The decentralised nature of the blockchain

network ensures that the distribution process is transparent and secure, providing voters with confidence in the integrity of the voting process. The use of key management is constantly reviewed and updated, ensuring that the voting process remains secure and that the risk of fraud or manipulation is minimised.

3.2.5 Validation of votes:

The blockchain network validates the encrypted votes to ensure their authenticity and accuracy. Validation of votes is an essential aspect of an online polling system using blockchain technology. The goal of validating votes is to ensure that only authorised votes are counted, and the vote process is fair and transparent. Validation of votes is achieved by using consensus algorithms, which ensure that all nodes on the blockchain network agree on the validity of a vote.

Once a vote has been cast, it is added to the blockchain network, where it is verified and validated by the nodes on the network. The consensus algorithm ensures that all nodes on the network agree on the validity of the vote before it is recorded on the blockchain ledger. This process ensures that only authorised votes are counted, and the voting process is fair and transparent. The use of blockchain technology in the validation of votes provides several benefits. The decentralised nature of the blockchain network ensures that the voting process is transparent and secure, as there are no central authority controls. Additionally, the use of consensus algorithms ensures that the voting process is fair and that all authorised votes are counted. To ensure that the validation of votes is secure, the consensus algorithms used are constantly updated and reviewed. This

ensures that the voting process remains secure and that the risk of fraud or manipulation is minimised.

The use of consensus algorithms ensures that all authorised votes are counted, and the voting process is fair and transparent. The decentralised nature of the blockchain network ensures that the voting process is transparent and secure, providing voters with confidence in the integrity of the voting process. The use of consensus algorithms is constantly reviewed and updated, ensuring that the voting process remains secure and that the risk of fraud or manipulation is minimised.

3.2.6 Counting of votes:

Once the validation is complete, the votes are counted, and the results are posted on the blockchain network for public verification. Counting votes is a crucial step in the online polling system using blockchain technology. Once the votes have been cast and validated, the next step is to count them accurately. Counting votes on the blockchain network involves using cryptographic algorithms to decrypt the encrypted votes and tally. The counting process is carried out by authorised participants who have access to the decryption key. These participants decrypt the encrypted votes, tally them up, and record the results on the blockchain ledger. The decentralised nature of the blockchain network ensures that the counting process is transparent and secure, as there are no central authority controls.

The use of blockchain technology in the counting of votes provides several benefits. The decentralised nature of the blockchain network ensures that the counting process is transparent and secure, providing voters with confidence in the integrity of the voting process. Additionally, the use of

cryptography ensures that the votes are secure and cannot be manipulated or tampered with. To ensure that the counting of votes is accurate, the cryptographic algorithms used are constantly updated and reviewed. This ensures that the voting process remains secure and that the risk of fraud or manipulation is minimised. Counting votes is a critical aspect of an online polling system using blockchain technology. The use of cryptographic algorithms ensures that the votes are decrypted securely and accurately tallied up. The decentralised nature of the blockchain network ensures that the counting process is transparent and secure, providing voters with confidence in the integrity of the voting process. The use of cryptography is constantly reviewed and updated, ensuring that the voting process remains secure and that the risk of fraud or manipulation is minimised.

The use of blockchain technology provides several advantages, including transparency, security, and immutability. Because the ledger is decentralised, there is no central authority, and the risk of fraud is significantly reduced. Additionally, since the blockchain is immutable, the integrity of the voting process is maintained, and the results can be verified at any time. In conclusion, a polling system using blockchain provides a secure, transparent, and trustworthy platform for conducting fair and democratic elections.

CHAPTER 4

PROPOSED METHODOLOGY

Designing an e-voting system using blockchain technology involves several key modules to ensure security, transparency, and user accessibility.

4.1 USER AUTHENTICATION MODULE:

MetaMask, a popular browser extension for managing Ethereum-based assets, will be integrated for user authentication. MetaMask's secure and decentralised nature ensures a trustworthy authentication process. Users will log in securely using their MetaMask credentials, adding an additional layer of protection against unauthorised access.

4.2 VOTER REGISTRATION MODULE:

Implement a user-friendly voter registration process. Validate and store voter information securely on the blockchain using smart contracts. Link MetaMask wallet addresses to individual voter profiles for seamless authentication during the voting process.

Develop a verification mechanism to ensure the validity of voter registrations. Utilise blockchain's transparency to allow stakeholders to audit the voter registration process. Implement additional security measures to prevent fraudulent registrations.

4.3 BLOCKCHAIN INTEGRATION MODULE:

Choose a suitable blockchain platform, such as Ethereum, for recording and storing votes securely. Utilise smart contracts to define the rules and logic of the election, ensuring transparency and immutability.

Develop smart contracts that handle the voting process, ensuring one vote per eligible voter. Include logic for vote counting, result determination, and other election-related processes. Implement robust error handling to address any unforeseen issues during the voting period.

4.4 VOTING MODULE:

Enable users to cast their votes securely using MetaMask. Implement a user-friendly interface that guides voters through the voting process. Ensure that each voter can only cast one vote to maintain the integrity of the election.

Design the voting process to maintain voter anonymity. Use cryptographic techniques to encrypt and protect voter data, preventing the identification of individual votes. Leverage blockchain's decentralised nature to enhance the privacy of the voting process.

4.5 VERIFICATION MODULE:

Provide a transparent verification process for voters to confirm that their votes have been recorded accurately. Enable users to access a public ledger containing encrypted vote details without compromising individual voter identities. Implement mechanisms for voters to report any discrepancies or issues with their votes.

Ensure that the blockchain is tamper-resistant, preventing any unauthorised alterations to the recorded votes. Implement regular audits to verify the integrity of the voting data stored on the blockchain. Utilise cryptographic hashing to secure the immutability of the vote records.

4.6 RESULT MODULE:

Design a module for counting and presenting election results in a clear and understandable format. Implement visualisation tools to display results graphically, aiding stakeholders in interpreting the outcome. Ensure that results are accessible to all stakeholders in a transparent manner.

Implement measures to prevent tampering with election results. Leverage blockchain's consensus mechanisms to validate and confirm the accuracy of the results. Provide stakeholders with tools to independently verify the results for increased transparency.

4.7 SECURITY MODULE:

Implement robust access control measures to prevent unauthorised access to the e-voting system. Utilise role-based access controls to ensure that only authorised personnel can modify system configurations or access sensitive data. Utilise advanced encryption techniques to secure voter data and communication channels. Implement end-to-end encryption for all user interactions within the system. Regularly update encryption protocols to address emerging security threats.

Conduct normal protection audits and vulnerability checks to perceive and cope with capability weaknesses within the gadget. establish a protocol for right away addressing and patching security vulnerabilities. Collaborate with security experts to stay knowledgeable about cutting-edge threats and mitigation techniques. Incorporating these detailed modules and considerations will contribute to the development of a robust, secure, and transparent e-voting system using blockchain technology.

ARCHITURE OF SYSTEM:

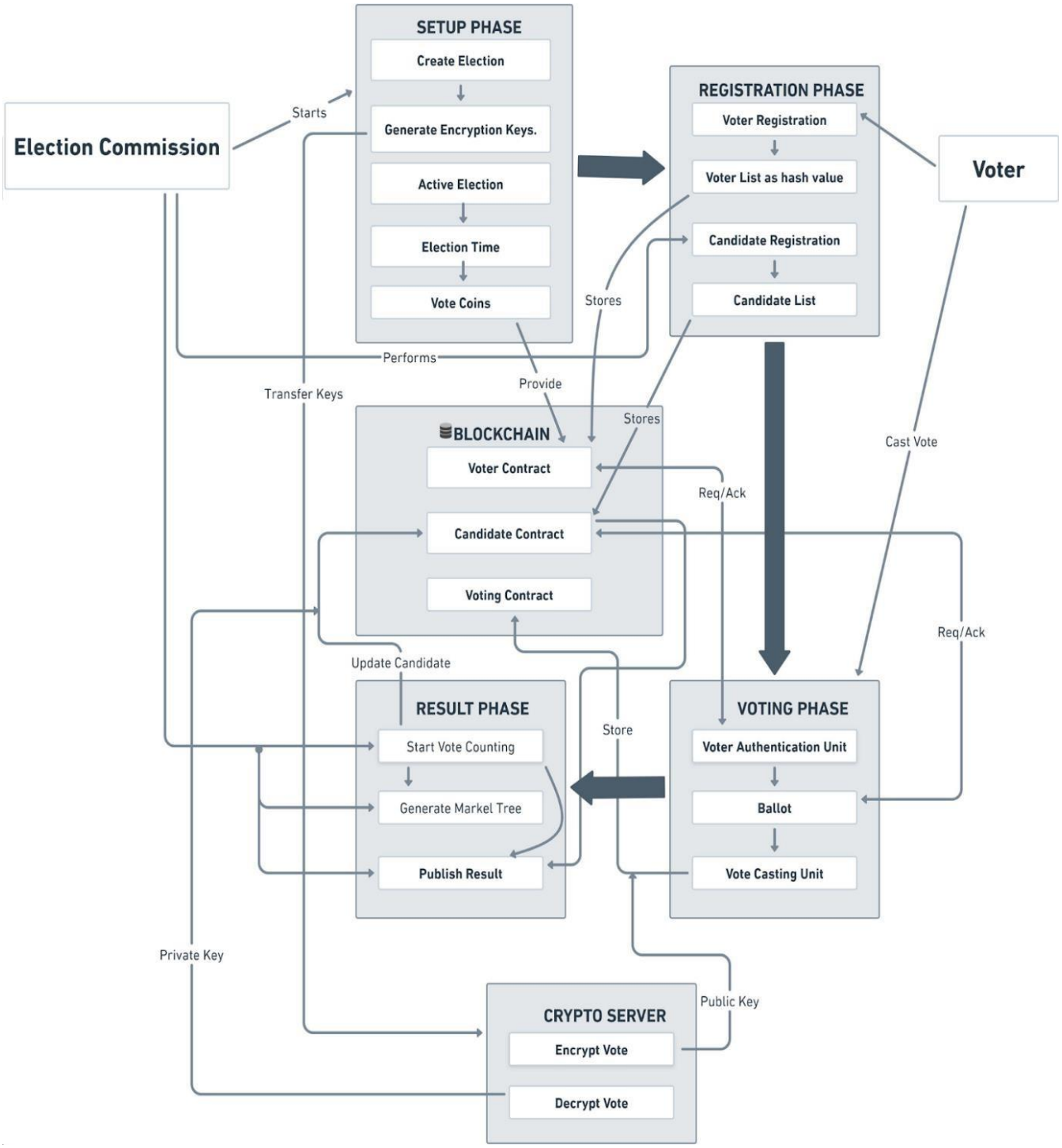

Fig 4.1 ARCHITECTURE OF THE PROJECT

PHASE ONE FLOW DIAGRAM:

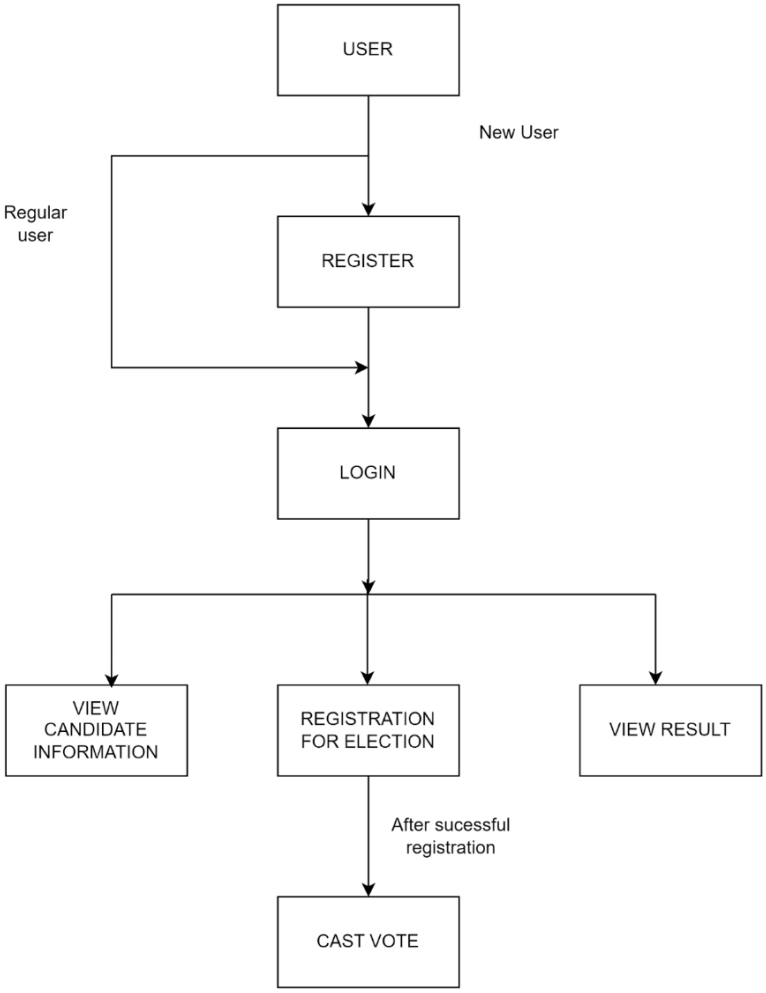

FIG 4.2 USER FLOW DIAGRAM

PHASE TWO FLOW DIAGRAM:

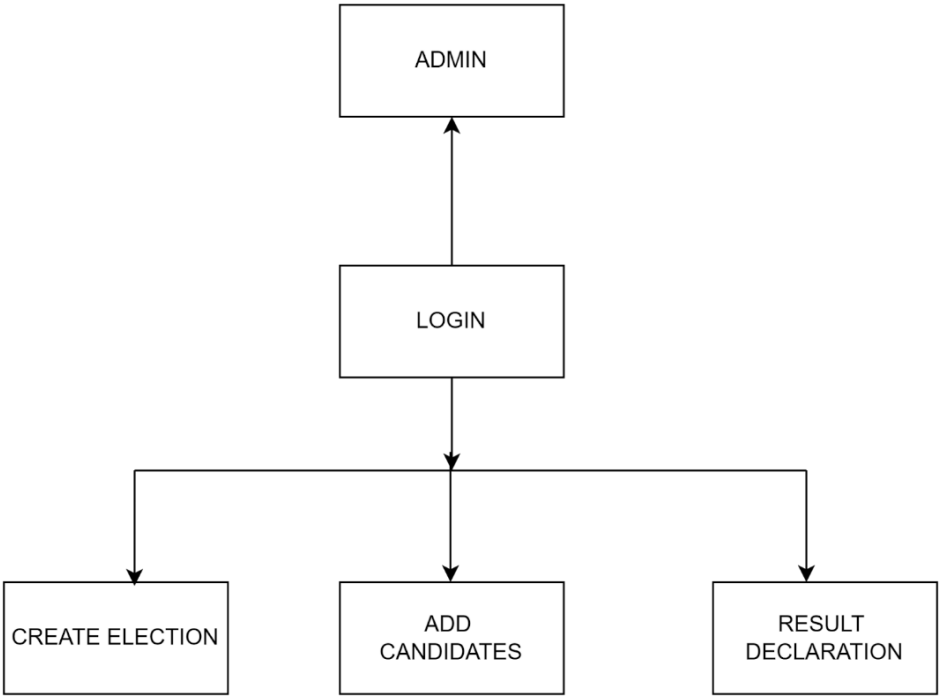

FIG 4.3 ADMIN FLOW DIAGRAM

CHAPTER - 5

RESULTS AND DISCUSSIONS

5.1 RESULTS:

Online polling systems that employ blockchain technology gain a number of advantages, such as improved performance, protection, and transparency. Online polling systems that utilise the blockchain era can provide a secure, transparent, and impervious to fraud and manipulation voting process by capitalising on the decentralised and immutable characteristics of the platform.

Blockchain-powered online polling platforms have produced encouraging results. They have been effectively used in a number of contexts, such as community surveys, corporate shareholder voting, and governmental elections. The adoption of blockchain technology has lowered expenses related to conventional voting procedures, enhanced security and transparency, and raised voter turnout. I am able to provide you a broad rundown of the many performance and outcome types that are used.

5.2 DISCUSSIONS:

Voter Authentication:

Voters would need to authenticate themselves using their Metamask wallets. Through a browser extension, Metamask offers users a safe method to interact with decentralised applications (DApps) and manage their Ethereum accounts.

Metamask Integration:

The online polling platform would integrate with the well-known Ethereum wallet browser addon Metamask. With Metamask, users may sign transactions and safely store their Ethereum accounts. Additionally, users can communicate with decentralised apps (DApps) straight from their browser by using Metamask.

Wallet Address Verification:

When a voter accesses the online poling platform, they would be prompted to connect their Metamask wallet. The platform would request access to the voter's Ethereum address to verify their identity. The wallet address serves as a unique identifier for the voter within the blockchain network.

Privacy Protection:

Throughout the authentication process, the online polling platform should prioritise the privacy of the voter. While the platform verifies the user's identity, it should not collect or store any personally identifiable information beyond the Ethereum address. This ensures that the voting process remains anonymous and confidential.

Submitting Votes:

Once authenticated, to prevent potential fraud or misuse, the authentication token issued to the voter's Metamask wallet should be single-use and valid only for the current voting session. Voters can submit their votes through the online polling platform. Each vote is encrypted and recorded on the blockchain as a transaction. The vote is transparent and verifiable, but the voter's name is kept anonymous.

Blockchain Consensus:

One blockchain network is used to record the votes. It might be a permissioned blockchain with designated validators or a public blockchain like Ethereum, depending on how the system is designed. The consensus mechanism ensures that all transactions (i.e., votes) are valid and agreed upon by the network.

Immutable Record:

Votes on the blockchain are unchangeable once they are registered, thus they cannot be manipulated or changed. Due to their transparency and impossibility of manipulation after the fact, the results guarantee the integrity of the voting process.

Real-Time Results:

As votes are recorded on the blockchain, real-time information on the vote results can be obtained from the polling platform. Users can track the progress of the poll and see how their votes contribute to the overall outcome.

Verification:

Anyone with blockchain access can audit the results after the polling period has ended. Since every vote is openly recorded, the results may be independently verified. This promotes confidence in the fairness of the electoral process.

5.3 COST BENEFIT ANALYSIS:

Conducting a cost-benefit analysis for an electronic voting system that integrates blockchain technology with MetaMask involves assessing the benefits and drawbacksofimplementingthesolutions.

Expenses cover the system's original creation, implementation, and upkeep, including software development, security precautions, blockchain infrastructure setup, and continuing support. It is also important to consider user and administratortraining.

The main advantages are greater accessibility, security, and transparency. Election results can be trusted more because blockchain technology provides tamper-proof record-keeping. Voting becomes simple and convenient with the

help of MetaMask integration, which makes blockchain engagement more approachable. Moreover, it lowers the possibility of fraud and manipulation, improving the democratic process's integrity.

Additional advantages include expediting the voting process overall, possibly lowering administrative expenses, and speeding up the tallying of ballots. Furthermore, blockchain-based electronic voting can increase voter participation especiallywithtech-savvypopulations.

In conclusion, although blockchain e-voting systems may need a sizable initial expenditure, in the long run, the advantages in terms of efficiency, security, and transparency exceed the drawbacks, hence fortifying democratic processes.

CHAPTER - 6

CONCLUSIONS AND FUTURE SCOPES

6.1 CONCLUSIONS:

Conclusively, blockchain-based online polling platforms offer a potentially effective means of providing a promising solution for improving and enhancing voting process integrity. By leveraging the security, transparency, and decentralisation inherent in blockchain, many of the issues with traditional voting systems can be resolved by using online polling platforms.

The voting process is protected against fraud, tampering, and hacking by the tamper-proof ledger of blockchain technology. The use of cryptographic techniques ensures voter anonymity while still allowing for transparent verification of voting results. Integrating with tools like Metamask provides a user-friendly interface for voter authentication, enhancing accessibility and usability.

However, implementing online polling in blockchain technology also poses challenges, such as ensuring inclusivity, protecting voter privacy, and navigating regulatory frameworks. Addressing these challenges requires careful planning, robust technological infrastructure, and collaboration with stakeholders. Finally after the results are published you are able to view and even can download it as PDF files.

Overall, blockchain-enabled online polling has the power to increase trust in democratic institutions, democratise politics, and increase voter turnout. Blockchain-based online polls can open the door to more inclusive, safe, and transparent elections in the digital era with continued innovation and improvement.

6.2 FUTURE SCOPES:

Increased Adoption:

As blockchain technology matures and gains wider acceptance, online polling systems should become more widely used by governments, organisations, and communities around the world. This adoption will drive further innovation and refinement of blockchain-based voting platforms.

Enhanced Security Features:

Future developments in blockchain technology will likely introduce even more robust security features to protect against emerging threats. This could include advancements in encryption techniques, multi-factor authentication methods, and consensus techniques to guarantee the voting process's integrity.

Scalability Solutions:

Blockchain networks still struggle with scalability, especially when it comes to managing massive online polling events with millions of participants. Online polling platforms will be able to perform better when blockchain scalability solutions like sharding, sidechains, or layer 2 protocols become more advanced.

Smart Contract Integration:

Voter registration, ballot counting, and result tabulation are just a few of the electoral procedures that smart contract self-executing contracts with the terms of the deal clearly written into code can automate. Future advancements in clever contract technology will enable more complex and sophisticated voting mechanisms to be implemented on blockchain-based platforms.

Mobile and IoT Integration:

Due to the widespread use of mobile and Internet of Things (IoT) devices, future online polling platforms may leverage these technologies to enhance accessibility and convenience for voters. Mobile voting apps and IoT-enabled voting devices could enable voters to participate in polls from anywhere, at any time, using their smartphones or connected devices.

Global Impact:

Blockchain-powered online polling has the potential to democratise the voting process on a global scale, enabling disenfranchised populations, such as refugees, expatriates, and those living in authoritarian regimes, to participate in elections and have their voices heard.

Research and Collaboration:

Research, development, and cooperation between academia and industry should continue, and government stakeholders will drive innovation in blockchain-based online polling technology. Interdisciplinary efforts involving experts in computer science, cryptography, political science, and law will be essential for addressing the technical, social, and regulatory challenges associated with online voting.

CHAPTER - 7

REFERENCES

1. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media. ISBN: 978-1491920497.

2. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. Applied Innovation Review, 2(6), 6-14.

3. Myerson, J., & Srinivasan, S. (2017). Blockchains and the Logic of Accountability: Evidence, Epistemology, and the Privacy-Security Tradeoff. Harvard Kennedy School Misinformation Review, 1(1), 1-19.

4. De Filippi, P., & Hassan, S. (2016). Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. First Monday, 21(12).

5. Grigg, I. (2005). Triple Entry Accounting. Ian Grigg's Bitcoin Pages.

6. Clark, J., & Essex, A. (2017). Blockchain Technologies: A Whitepaper Discussing How and Why Universities Should be Involved. Journal of Research in Leadership Education, 12(2), 1-19.

7. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin. ISBN: 978-1101980132.

8. Biswas, K., & Misra, S. (2016). Blockchain Demystified. IEEE Potentials, 35(5), 36-40.

9. OECD (2020). Blockchain Technology in Government: Benefits and Implications. OECD Publishing. ISBN: 978-9264892908.

10. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview. National Institute of Standards and Technology (NIST) Special Publication 800-207.

APPENDICES

8.1 BILL OF MATERIAL:

A Bill of Materials (BOM) is a list of all the parts, software, hardware, and materials needed to execute a project, such as "E-VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY". To run the necessary software, you'll need a computer with the right specs. A contemporary PC or laptop should work just well, though the actual requirements may differ. You might require software like ganache to run this project more efficiently and in a secured manner.