IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Comprehensive Analysis: Security Attacks On E-Voting Systems Using Blockchain Technology

[1] **Mahvash Fatema S.A. Khan,** [2] **Dr. Mahip Bartere**,

[1] Student at GH Raisoni University Amravati, [2] Assistant Professor at GH Raisoni University Amravati

[12] Computer Science and Engineering,

[12] GH Raisoni University, Amravati, Maharashtra

Abstract : In any democratic country, Voting is a fundamental right of any citizen that enables them to choose the leaders of tomorrow. The trend of electronic voting has risen in recent years as an alternative to paper ballot elections, bringing meaningful benefits in terms of efficiency and error proneness. However, real world applications have demonstrated significant vulnerabilities and susceptibility to software errors that could be exploited by malicious entities. In fact, the difficult challenge of electronic voting lies in the need to incorporate multiple, often contradictory, properties into the system design. As a digital platform, they eliminate the need to cast your votes using paper or having to gather in person. They also protect the integrity of your vote by preventing voters from being able to vote multiple times. Electronic voting or e-voting has fundamental benefits over paper based systems such as increased efficiency and reduced errors. The electronic voting system tends to maximize user participation, by allowing them to vote from anywhere and from any device that has an internet connection. The blockchain is an emerging, decentralized, and distributed technology with strong cryptographic foundations that promises to improve different aspects of many industries. Expanding e-voting into blockchain technology could be the solution to alleviate the present concerns in e-voting. Here we propose a blockchain based voting system that will limit the voting fraud and make the voting process simple, secure and efficient.

Keywords - Blockchain, E-voting, Electronic Voting, Security Attacks, Cryptographic Vulnerabilities, Smart Contracts, Voter Privacy.

I. INTRODUCTION

Voting is one of the most fundamental processes in any democratic society, as it allows citizens to choose their representatives and express their opinions on key issues. Traditionally, voting has been carried out using paper ballots and manual counting. While such systems are relatively simple, they are vulnerable to several issues including ballot tampering, vote rigging, and human error in counting. To address these limitations, electronic voting (E-Voting) systems were introduced, offering faster tallying, improved accessibility, and easier management of large-scale elections. However, despite these advantages, E Voting systems have been criticized for their security vulnerabilities, including hacking attempts, software manipulation, insider threats, and lack of transparency.

These challenges raise questions about the trustworthiness of electronic voting and the integrity of democratic processes. The emergence of blockchain technology has opened new avenues for building secure, transparent, and tamper-resistant voting systems. With its decentralized nature, immutability, transparency, and cryptographic security, blockchain offers a promising alternative to traditional E-Voting systems. A blockchain-based E-Voting system can ensure that votes are securely cast, immutably stored, and transparently verified, thereby reducing the risks of electoral fraud. The proliferation of blockchain technology has sparked considerable interest in its application to electronic voting systems, promising to revolutionize democratic processes through enhanced security, transparency, and verifiability. Blockchain-based e-voting systems leverage the technology's inherent characteristics—decentralization, immutability, and cryptographic security—to address longstanding vulnerabilities in traditional paper-based and electronic voting mechanisms. Proponents argue that these systems can eliminate vote tampering, ensure voter anonymity, provide real-time transparency, and reduce the substantial costs associated with conventional electoral infrastructure.

However, despite the theoretical advantages and growing enthusiasm surrounding blockchain voting systems, a comprehensive analysis of security vulnerabilities reveals that these solutions introduce significant and potentially catastrophic risks to electoral integrity. Research conducted by leading cybersecurity experts and academic institutions has consistently demonstrated that blockchain technology does not solve—and in many cases exacerbates—the fundamental security problems inherent to all electronic voting systems. The decentralized nature of blockchain, while offering certain benefits, creates new attack surfaces and governance challenges that traditional centralized systems do not face.

The security landscape of blockchain-based e-voting systems encompasses a diverse spectrum of attack vectors operating at multiple layers of the electoral infrastructure. These vulnerabilities range from consensus-level attacks such as 51% attacks and Sybil attacks, to network-layer threats including denial-of-service attacks, man-in-the-middle attacks, and traffic analysis vulnerabilities. Cryptographic weaknesses pose additional concerns, particularly with the emergence of quantum computing threats that could compromise current encryption schemes, while implementation-level vulnerabilities manifest through smart contract bugs, malware infections, and inadequate key management practices. Ensuring trust in electoral processes is crucial for maintaining democratic values. A voting system that fails to provide transparency and security can lead to public distrust, manipulation of election results, and political instability. Current E-Voting systems are often centralized, meaning that a single authority controls the infrastructure. This centralization introduces the possibility of corruption, hacking, and data tampering.

Furthermore, human-factor vulnerabilities such as phishing attacks, social engineering, vote coercion, and vote buying remain largely unaddressed by blockchain solutions. The immutability characteristic of blockchain, often cited as a strength, becomes a liability when erroneous votes cannot be corrected, and the absence of voter-verified paper audit trails eliminates the most effective defense mechanism against cyberattacks. Scalability challenges compound these security concerns, as high transaction volumes lead to network congestion, elevated gas fees, and increased vulnerability to resource exhaustion attacks.

This comprehensive review paper systematically analyzes the security attacks threatening blockchain-based e-voting systems, examining both theoretical vulnerabilities and documented exploits. The analysis encompasses consensus mechanism attacks, network and infrastructure vulnerabilities, cryptographic weaknesses, smart contract security issues, privacy and coercion threats, implementation and operational risks, and scalability related security concerns. By synthesizing current research from academic literature, security audits, and real-world case studies spanning from 2020 to 2025, this review provides a critical assessment of the security posture of blockchain voting systems.

The paper contributes to the growing body of evidence suggesting that while blockchain technology offers certain advantages for specific applications, its application to high-stakes democratic elections introduces unacceptable security risks that cannot be adequately mitigated with current technological capabilities. Understanding these vulnerabilities is essential for policymakers, election officials, technology developers, and voters as they evaluate proposals to implement blockchain-based voting systems. The findings

underscore the importance of maintaining robust, auditable, and paper-based voting mechanisms that provide software independence and meaningful security guarantees against both classical and emerging cyber threats.

II. LITERATURE REVIEW

Trustworthy elections depend on three key things: keeping votes secret, making sure the final count is accurate, and allowing everyone to check that the whole process was fair. Classical electronic voting (e-voting) systems used strong encryption methods like mix-nets, homomorphic tallying, and zero-knowledge proofs to make sure elections are fully verifiable from start to finish. More recently, blockchain and smart contract platforms have been suggested as tools to help with checking elections. Some use them as just a way to record and share votes and proof of counting, while others aim to make the whole voting process fully automatic and spread out across many computers. This chapter looks at both approaches, covers real-world uses and the evidence we have, and points out areas where this project wants to improve things. Early systems for voting from a distance focused on making sure votes stay private, the count is correct, and people can check everything. They used techniques like mix-nets, homomorphic tallying, and end-to-end (E2E) verification (like Benaloh challenges or methods that stop voters from proving they voted in a certain way). While systems like Helios showed that you can check results openly in low-stakes situations, they had problems with preventing voters from being forced to vote a certain way, handling issues if a device is hacked, and being easy enough to use in big, real elections. Traditional systems that relied on a central server also had risks, like a single point where something could go wrong, and required people to trust a small group of administrators.

Electronic voting systems have developed over many years, providing benefits like efficiency, transparency, and possible improvements compared to traditional paper ballots. Studies in this area focus on key requirements such as ensuring the system is secure, keeping votes private, confirming voters are eligible, making sure results are correct, allowing voters to check their votes, and preventing others from influencing their choices. Other important factors include the ability to review the system and its ability to handle large numbers of voters. Techniques like cryptographic methods such as mixnets, homomorphic encryption, group or ring signatures, and zero-knowledge proofs are essential in meeting these needs. Blockchain technology also offers greater transparency and unchangeable records, but it comes with its own challenges when it comes to putting it into practice.

The last group of e-voting systems we look at are all the ones that use blockchain technology. Blockchains became really popular in the 2010s because of their role in cryptocurrencies. They might help create e-voting systems that are easy to check and keep secure. As of June 2023, e-voting systems that use blockchain have been tested in Japan, Russia, and Switzerland for non-binding or local elections. Before we talk about the research we've reviewed, let's quickly go over the main features of blockchains. Bistarelli and others created a fully decentralized e-voting system using the Bitcoin blockchain. The platform checks users' identities using an Anonymous Kerberos protocol or blind signatures. Votes are recorded on the blockchain either as regular Bitcoins or as digital asset coins. In the first case, the vote token is the smallest amount you can send in Bitcoin plus a fee. The Digital Asset Protocol lets you create special coins that can clearly identify voting tokens. This system meets most of the requirements for e-voting but doesn't support receipt freeness, which means it's not fully resistant to coercion.

In Shahzad and Crowcroft's work, they introduced block creation and sealing as ways to make e-voting on blockchains more secure. Block creation is different from normal blockchain tech because the block is made before the election and is linked to a random number's hash. Also, there's no consensus process like proof of work, since the blockchain is controlled by the election authority. Block sealing improves the safety of each block after the election, especially to make sure the data stays unchanged. Even though this approach covers many important e-voting features, it doesn't talk about resisting coercion. Another large-scale e-voting

system is built as a smart contract on Ethereum, proposed by Wang et al. This system uses one-time ring signatures that can't be linked, offering anonymity. It also uses ElGamal encryption and a delegated proof of stake method to make the system run faster. Using elected delegates makes the process quick and good for big elections. This system has most of the needed e-voting features but doesn't protect against coercion. Votereum is another e-voting system that works as a smart contract on Ethereum.

Lastly, Chafiq and their team suggested a blockchain-based system to make elections in Morocco more transparent and trustworthy. This system was built to work both in-person and from a distance. It uses a multi-layer structure built on the Solana blockchain, which was picked because it has fast processing times, handles a lot of transactions quickly, and has a reasonable cost for each transaction. The first layer is called the Distributed Permission Ledger Technology, which checks and confirms each transaction. The second layer, based on Solana, keeps a permanent record of all transactions. An auditor can ask the blockchain to check the logs, which then sends back the verified results, making the election process open and accountable. The authors said that although their system reduces costs and speeds things up compared to traditional electronic voting, it might still have weaknesses and needs ongoing updates and care for the blockchain network. Other research: We now include some studies we think are important to mention, even though they don't fit into the earlier categories. First, Khan and their team made a version of the Prêt à voter system using a private blockchain (specifically, Multichain) and verified users through fingerprint scans. Also, Hardwick and their group created a fully decentralized system using blockchain, allowing every voter to collect, check, and add their votes to the blockchain. This system also lets people vote again or cast invalid votes, but it still needs a central authority to confirm that voters are eligible.

Blockchain-based e-voting aims to use the built-in features of blockchains like being unchangeable, relying on many computers to agree on what's true, and being open to everyone checking. Different designs have been proposed, including fully open blockchains (like Ethereum), private ledgers (like Hyperledger Fabric or Tendermint), and mixed models (like sidechains or rollups). The idea is to have logs that show changes clearly, counts that can be checked again, and audits that everyone can see without having to trust one authority. However, studies show that blockchains don't just automatically fix all security issues. Instead, they change where the risks are, introducing new challenges in smart contracts, the part of the network where transactions wait, the network itself, how keys are managed, and how the system is updated or controlled.

III. RESEARCH GAP:-

Even though there's a lot of interest in using blockchain for electronic voting, there are still big problems with security and practicality that aren't being solved.
Most of the work focuses on the security of the blockchain itself, like making sure data can't be changed and keeping agreement among users, but they don't look deeply at other areas where attacks could happen. These areas include the devices people use to vote, the apps they run, how they prove their identity, the network connections they use, and how they keep their keys safe. There's no clear, tested model that covers all the steps in the voting process like signing up, casting a vote, counting votes, reviewing results, and handling disputes especially when things like remote voting, low-powered devices, and attackers who can control the system are involved.

Many voting systems that protect privacy focus on keeping votes secret or stopping people from being forced to vote a certain way, but they don't do both at the same time.
And they usually don't measure how much information leaks out through things like timing, network patterns, or blockchain data. Testing and checking for security flaws is also limited. A lot of proposals don't have ways to test how they handle attacks in real situations, and they don't give clear guarantees about how secure they are when things go wrong, like when the network is split, when bad actors can

manipulate transactions, or when people pretend to be others or control validators in a private system. User experience and human factors like losing keys, falling for scams, or accidentally casting wrong votes aren't studied enough.

Also, risks related to managing the system—like changing rules, updating keys, or making emergency fixes—aren't looked at closely either. Plus, not many studies compare how safe and fast a system is while still allowing people to check everything from start to finish, being able to handle future computer threats, and following laws that protect voters' privacy and allow for audits and recounts. This lack of research shows the need for a complete list of possible threats, realistic ways to test for them, and guides for building voting systems that are secure, easy to use, and keep privacy while using blockchain.
Even though there have been many new ideas and improvements, making secure and reliable electronic voting systems that work well for big elections is still not fully solved.

The studies show there are several big problems that keep happening:

Scalability and Performance:
Blockchain and smart contract methods face serious challenges when trying to handle large elections. These systems are too slow because they use slow ways to agree on data, take too long to process votes, and can't handle a lot of votes quickly or affordably.

Coercion Resistance and Privacy:
Most blockchain-based voting systems do not stop people from forcing others to vote a certain way or from proving they voted.
Since blockchains are public, they can be used to cheat by buying votes or pressuring people, making voters unsafe in tricky situations.

Device and Infrastructure Security:
Strong e-voting needs secure devices and networks for voters.
But there are often problems in the devices people use, their internet connections, and the systems supporting them. These issues make remote voting less trustworthy.

Transparency vs. Confidentiality:
It’s hard to have both open checks (so everyone can see the system works) and secret votes. No fully digital system has fully solved how to balance these two things.

Quantum Resistance:
The security tools used in e-voting, like digital signatures, might not work well if quantum computers become powerful. There's not much research on making voting systems safe against these future threats.

Usability and Accessibility:
Making e-voting easy and accessible for everyone especially people with disabilities and those in remote places—has not been done in a way that works for all.

Empirical Validation:
Most new systems are only tested in small groups or in theory.
There's not enough real-world testing in different political, social, and technical settings.

This is needed to make sure systems are safe and accepted when used widely. Fixing these issues is important for future work. Researchers should focus on better systems that can handle lots of votes, better privacy tools, secure hardware, quantum-safe methods, and thorough testing before big elections use them.

- **What is missing in previous work:**

• A complete threat model that covers attacks on the blockchain, outside the blockchain, the network, and human behavior, based on realistic assumptions about voters and devices.

• Resistance to coercion and the ability to keep secrets, along with measurable risks from side-channel leaks like timing, metadata, and graph analysis on the blockchain.

• A testing environment for attackers and clear security measures, including how often attacks succeed, how quickly they are detected, and how strong the evidence is.

• Risks in the consensus layer, such as MEV/front-running, network reorganization delays, validator collusion in private networks, and how these affect secrecy and fairness in voting.

• Managing encryption keys and linking identities securely, including defenses against phishing, recovery without relying on trusted third parties, and handling device theft or compromise.

• Issues caused by user mistakes, like incorrect or duplicate votes, and ways to detect them while still keeping voters safe from coercion.

• Risks from changes in governance and system upgrades, including protocol changes, smart contract upgrade tools, emergency access keys, and how they can be misused.

• Handling large-scale voting while keeping everything checkable, including the trade-offs between speed and full verification, and new risks from layer two solutions and rollups.

• Preparing for a future with quantum computers, using secure signatures and commitments that don't slow things down or make voting harder for users.

• Making sure cryptographic evidence meets legal and audit standards, so it can be used in official reviews, recounts, and disputes.

- **Our study will cover the following points:**

- We will create a complete and detailed list of all possible attacks on blockchain-based electronic voting, including those that happen on the blockchain itself, outside of it, across the network, through social engineering or user experience flaws, and related to governance**.**
- We will build a simulation and testing framework to check how real-world voting systems perform under different attack situations like Sybil attacks, Eclipse attacks, MEV (miner extractable value) and front-running, device takeovers, and coercion.
- We will suggest and test security methods that protect privacy and make it harder to coerce voters, such as zero-knowledge proofs that hide links between users and their votes and don't require receipts. We will also measure how much information about users can be leaked.
- We will examine the key steps in managing user identities, like signing up, recovering lost access, and revoking access, making sure these processes are resistant to phishing attempts.

- We will create performance and security standards for scaling the system, along with design advice that fits with the need for transparency and legal compliance.
- This electronic voting system uses blockchain and advanced security techniques to ensure that voting is secure and can resist attacks. Here's how these systems work, along with a detailed look at the technology used.

IV. PROPOSED METHOD FOR E-VOTING SYSTEMS:-

Creating a safe and dependable electronic voting system is difficult, which has led to many ideas and solutions developed by both researchers and companies. voting systems used in real elections, like scanners, DREs, and remote voting tools, have often been shown to have weaknesses when checked by security experts. we look at attacks on e-voting systems, including those used in real elections. This section also covers studies about electronic voting systems. We pay special attention to research that focuses on systems where voters can check their votes and uses blockchain technology.

In particular, we organize this section in the following way: first, we talk about end-to-end on-site voter-verifiable systems. Then, we look at studies that try to build dependable remote voter-verifiable systems.

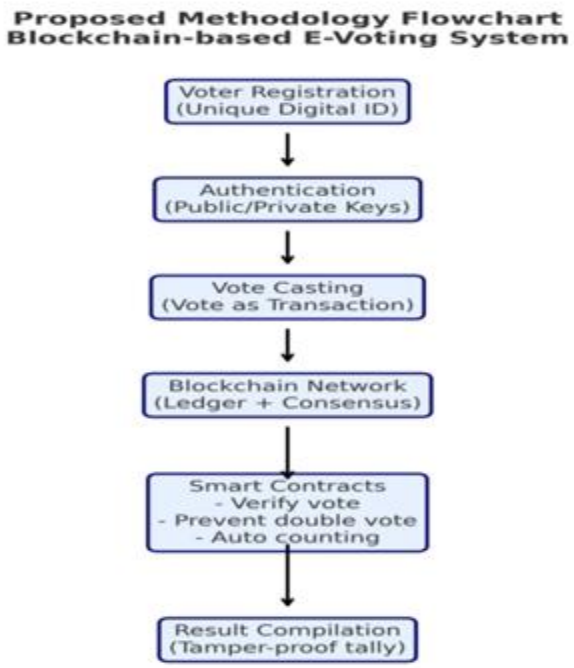

Figure 1: The Flowchart E-Voting System

Finally, we cover works that use blockchain technology for e-voting. At the end of each subsection, we visually summarize all the works we looked at, listing the most important features along with the strengths and weaknesses of each e-voting system in that category. To wrap up, we have a section where we compare the different methods discussed in the literature review based on the key properties they offer.

V. DATA COLLECTION:-

Because this is a system security project, the data we need will come from simulation-based datasets and performance logs, not from regular surveys.
The system we are building will create and gather its own data as we develop and test it.
The types of data we will collect include:

1. **Number of Voters –** We will use simulated voter identities, created with cryptographic keys, to test how the system performs under different levels of voting activity.
2. **Number of Votes Cast –** Each vote will be recorded as a blockchain transaction to check how efficiently the system works.
3. **System Response to Attacks –** We will collect logs whenever we simulate attacks, such as double voting, DoS attacks, 51% attacks, and eclipse attacks, to see how well the system can handle them.
4. **Blockchain Transaction Logs –** We will track when transactions happen, how quickly they are confirmed, and how block validation works, to evaluate both the performance and security of the system.

VI. Blockchain Technoloy:-

In essence, blockchain technology is a public ledger of events or transactions that are documented and kept in blocks that are related both temporally and linearly. The hash of earlier blocks is then preserved by later blocks. Blockchain is a distributed digital ledger technology that eliminates the need for middlemen by enabling network users to securely and transparently communicate and validate transactions. Because of the technology's decentralized architecture, data is kept on a network of computers rather than in a single database. This preserves the system's integrity and security by making it more difficult to hack or alter the data. With the rise of Bitcoin, the first decentralized cryptocurrency, blockchain technology became more well-known. Since then, though, the technology has been used in a number of sectors, including voting, healthcare, supply chain management, and finance. As the name suggests, blockchain operates by generating data blocks that are connected in a chain. Every block has a hash, which is a unique code created from the block's contents. A chain of blocks is created by connecting the block to the one before it using this hash. A block cannot be removed or changed once it has been put to the blockchain without the agreement of all network users. This renders the system unchangeable, guaranteeing the transparency and tamper-proofness of the data recorded on the blockchain. All things considered, blockchain technology has the power to completely transform how we exchange and keep data, making it safer, more transparent, and easier to access. A key element of many cryptocurrency systems, including the one that first introduced it, Bitcoin, is blockchain technology. It basically comprises of a peer-to-peer network with a decentralized digital ledger. Each network participant (node) maintains a copy of the append-only ledger.

Figure 2: The Blockchain Structure

The primary general characteristics of a blockchain are as follows.

- **Decentralization:** Since there is no central authority in the network, every node has the same rights and responsibilities.
- **Immutability:** A block of transactions cannot be altered or removed once it has been added to the chain with the consent of the majority of nodes.
- **Non-repudiation:** The sender of a transaction cannot revoke it once they have signed it using their private key.
- **Transparency:** All transactions on a public blockchain are available to the general public.
- **Pseudonymity:** Every transaction's identifier is generated in a pseudo-random manner. Nevertheless, after examining several transactions, some information regarding the true identities can still be deduced.

Because of these characteristics, blockchains can be used for a number of purposes outside of cryptocurrency, including online electronic voting.
In the context of electronic voting, smart contracts—that is, program contracts that run automatically if a predefined set of circumstances is met—are especially pertinent. Blockchain-based smart contracts eliminate the need for relying on third parties and enable the execution of trusted, unchangeable transactions. There are instances of smart contract applications in both public and private blockchains. Since there is no central authority on a public blockchain, any entity can create and validate transactions and take part in the consensus process.

Proof of Stake (PoS) and Proof of Work (PoW) : are the two most popular consensus techniques. Only approved nodes are permitted to join in a private (also known as permissioned) blockchain, which has a centralized control authority. It is typically used for tracking purposes by businesses or by banks that issue their own private currencies.

Proof of Work vs. Proof of Stake: In a PoW consensus process, nodes compete to solve a challenging mathematical problem in order to commit the ledger first. These systems typically have scalability issues due to their high resource consumption and inability to ensure a high throughput. The selection of validators in a PoS consensus method is contingent upon the stake, or total quantity of cryptocurrency possessed. Since the consensus is based on the stake and, thus, on the quantity of transactions conducted by each member, anonymity is weakened even though high throughput and minimal resource usage are made possible. Ethereum blockchains recently switched to PoS, whereas Bitcoin is still based on PoW.

VII. Blockchain Attacks:-

Blockchain Attacks: These are attempts to either target the mining process or the Blockchain's network. Indeed, there have been cases when hackers have targeted blockchain-based electronic voting systems. For instance, a node attack occurred on Russia's blockchain-based electronic voting system in 2020. illustrates the various risks associated with blockchain technology, such as DDoS, phishing, selfish mining, eclipse, and (51%).

Figure 3:- The Common Attacks

Sybil Attacks:-

- Multiple fake voter identities are created and used to cast fraudulent votes.
- Impact: Inflated vote counts, compromised authenticity of voters.

51% Attack:-

- In a blockchain network, consensus is maintained by the majority of nodes (miners or validators).
- If an attacker (or group) controls more than 50% of the network‘s computational power (in Proof-of-Work) or stake (in Proof-of-Stake), they can dominate the consensus process.
- Impact on E-Voting: The attacker can rewrite or reverse voting transactions. They may prevent new votes from being confirmed, creating election delays. Votes can be altered or removed, leading to election fraud.

Eclipse Attack:

- In an eclipse attack, a malicious entity isolates a target node (e.g., a voter‘s device or a validator) by surrounding it with fake/malicious peers.
- The victim node only communicates with the attacker-controlled peers, cutting it off from the real network.
- Impact on E-Voting: Voters may see false results or altered transactions. Attackers can delay or filter votes from reaching the blockchain. Nodes (like election authorities) can be fed manipulated information, impacting the final tally.

Double Spending Attack:

- In blockchain, once a transaction (like a vote) is recorded, it should be irreversible.
- In a double spending attack, an attacker tries to spend (or use) the same digital asset more than once.
- Applied to E-Voting, this means a voter could attempt to cast multiple votes using the same identity or token.

- Impact on E-Voting: Fraudulent multiple votes from a single voter. Loss of fairness and trust in the system.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks:

- Attackers flood the voting server with excessive requests, making it unavailable to legitimate voters.
- Impact: Election process disruption, voter disenfranchisement, and lack of availability.

VIII. Ethereum:-

To develop a decentralized application, use the Ethereum blockchain. Often referred to as "the world computer," Ethereum was discovered in 2013 by Vitalik Buterin. The program known as "Smart Contract" is implemented by Ethereum, an open-source, worldwide decentralized infrastructure (Lavayssière 2018). Ether is the coin that powers the Ethereum blockchain. to PoS.

IX. Smart Contract:-

A smart contract is a program that the Ethereum Virtual Machine executes inside the Ethereum Blockchain. Since the code of a smart contract is immutable, it cannot be changed or rewritten after it has been created and added to a blockchain. This idea is best expressed by Vitalik as "code is law." A Solidity language is utilized in Ethereum Smart Contracts. When the code is finished and prepared for deployment, developers might choose to move it to Mainnet, the actual network that uses real ether.
Ropsten, Kovan, Rinkeby, and Goerli are the four Ethereum Testnets where developers can deploy their smart contract to test it. No actual ether is used on these testnets. Instead, one of these Testnets' faucets can be used to request Ether by the developers. Functions, events, modifiers, and state variables make up a smart contract. A specific amount of "gas" will be used for each transaction, which is each function call that modifies the state variables inside the Smart Contract. Gas consumption will be determined by the function's memory and complexity. As long as they are not called from another mutative function and the return function does not change the values of the state variables, other functions like the return function or pure function do not use 14 gas.
Since millions of users maintain the blockchain, the fundamental benefit of using Smart Contracts is that there is essentially never any downtime. The Smart Contract will remain in effect as long as the Ethereum blockchain network is operational.

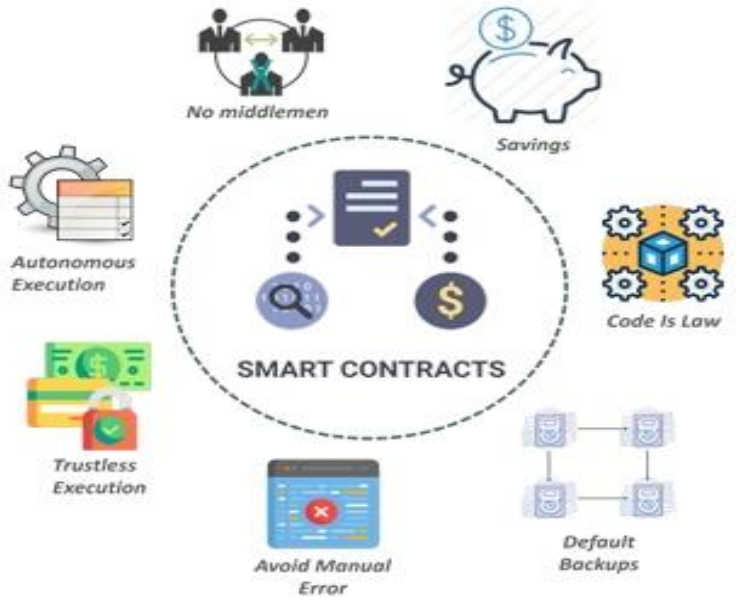

Figure 4:- Smart Contracts

X. SHA-256:-

SHA-256 is a cryptographic hash function that is one of the most popular and safest algorithms in the digital world. It can transform any length of input into a fixed 256-bit (32-byte) text. Digital signatures are cryptographic techniques that use asymmetric key pairs to confirm the integrity and validity of data. They make sure that documents, transactions, or messages are signed by a legitimate party and haven't been altered. A member of the SHA-2 family, SHA-256 was created by the NSA and released in 2001. It is essential for integrity checking, digital signing, and blockchain security.

In order to produce a distinct, irreversible hash, the method processes data in blocks, going through padding, initialization, complex bitwise operations, and rounds of compression functions. It exhibits important characteristics like avalanche effect, impact resistance, and preimage resistance: It is extremely difficult for attackers to create matching hashes for bad data since even little changes in input result in wildly disparate results. Blockchain architecture is supported by SHA-256, which secures transaction data and connects blocks with hashes.

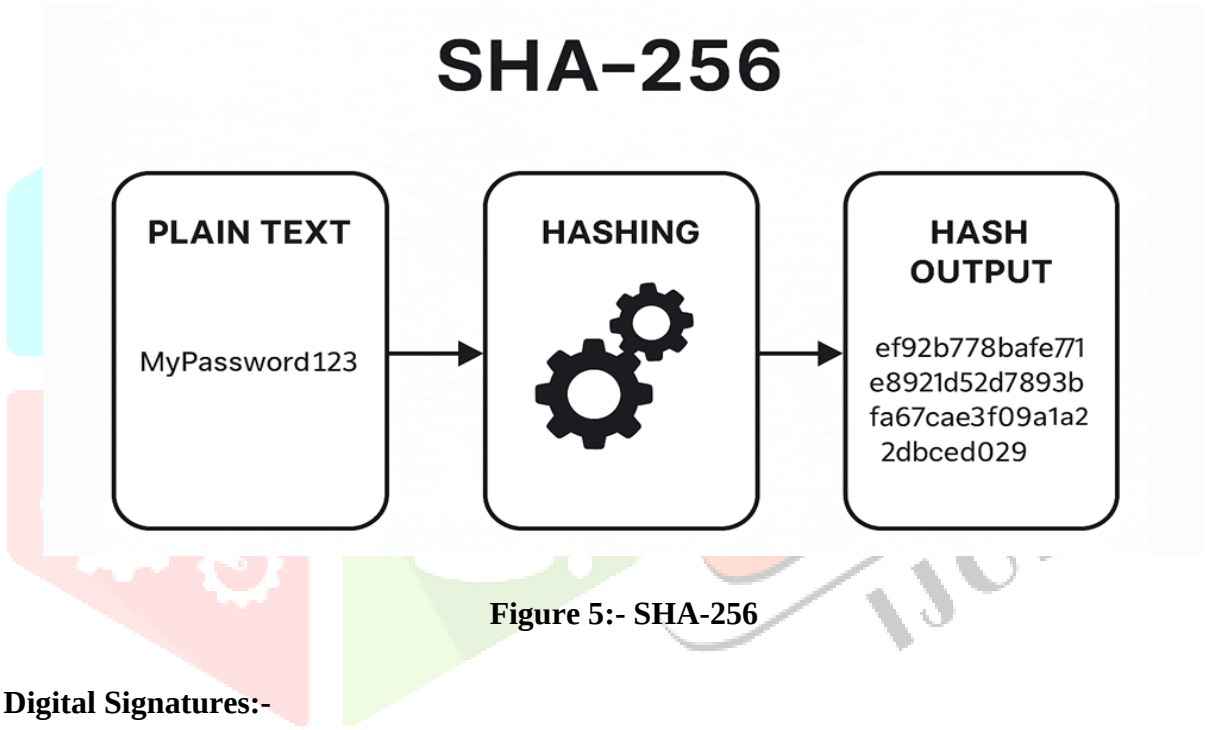

Figure 5:- SHA-256

XI. Digital Signatures:-

Asymmetric encryption, usually RSA or ECDSA, is the foundation of digital signatures. These methods use public-private key pairs for both signing and verification. When a communication is signed, the sender creates a signature over a hash of the message (often calculated using SHA-256) using their private key. The legitimacy of the data can be confirmed by the recipient or anybody who has the sender's public key; if the message or the signature were changed, verification would not be successful. To maintain trust and integrity across digital systems, digital signatures are used for safe transactions, software distribution, legal documents, and blockchain-based smart contracts.

In contemporary cryptography, SHA-256 and digital signatures together provide the technological foundation for safe communications and data integrity, particularly in blockchain systems where they guard against fraud, guarantee authenticity, and promote decentralized trust.

XII. Future Scope:-

To make blockchain-based e-voting more reliable, future work should focus on:
 Using AI and machine learning to detect and stop unusual voting behavior in real time.
 Using zero-knowledge proofs to protect voter privacy while keeping the process open and trustworthy.
 Looking into mixed consensus systems that work well in terms of speed, ability to handle many users, and protection from attacks like majority and eclipse attacks.
 Using cryptography that can resist attacks from future quantum computers to keep e-voting safe.
 Adding multi-factor authentication and biometric checks to make sure only real voters can cast their ballots.
By working on these areas, blockchain-based e-voting can become a strong, open, and widely accepted system for future elections.

XIII. Conclusion:-

This work did a thorough review of e-voting systems.We started by listing the important features that a secure e-voting system must have, from the basic ones that are always needed to the extra ones. Then we looked at the e-voting solutions that have been discussed in the literature, and grouped them into three main types: on-site, remote, and blockchain-based. We gave a special section to blockchain-based systems because blockchain technology seems to fit well with the idea of verifiable electronic voting, even though there are challenges in keeping votes secret. While early blockchain-based solutions have shown promising results, there are still several problems that need to be solved, such as scalability and resistance to coercion. We also reviewed the known attacks on e-voting systems. Overall, e-voting systems have been found to be vulnerable to many threats, including de-anonymization, tampering with votes, influencing voters to choose the wrong candidates, and creating fake votes to manipulate elections. By looking at both the proposed methods and the attacks against them, we aimed to provide a complete picture of the current state of research on e-voting systems. From our analysis, it is clear that, although the field has made significant progress in recent years, there are still several issues that make e-voting solutions unsuitable for high-stakes situations. Additionally, future research should also explore the threats and opportunities that will come with the rise of quantum computers.

XIV. References:-

[1] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp, Security analysis of India‘s electronic voting machines,‘‘ in Proc. 17th ACM Conf. Comput. Commun. Secur., Chicago, IL, USA, Oct. 2010.

[2] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, __Analysis of an electronic voting system,‘‘ in Proc. IEEE Symp. Secur. Privacy, Berkeley, CA, USA, May 2004.

[3] A. Tidey. (Nov. 2020). Why Don‘t More Countries Follow Estonia and Hold Elections Online. [Online]. Available: https://www.euronews.com/myeurope/2020/11/02/why-don-t-more-nations-hold-elections-online-here-s-how estonia-has-been-a-lone-trailblaze.

[4] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, __Analysis of blockchain solutions for E-voting: A systematic liter ature review,‘‘ IEEEAccess,vol.10,pp.70746–70759,2022.

[5] R. Tas and Ö. Ö. Tanröver, __A systematic review of challenges and opportunities of blockchain for E-voting,‘‘ Symmetry, vol. 12, no. 8, p. 1328, Aug. 2020.

[6] J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, and K.-K.-R. Choo, __The application of the blockchain technology in voting systems: A review,‘‘ ACM Comput. Surv., vol. 54, no. 3, pp. 1–28, Apr. 2022.

[7] A. Al Sammak, A. A. El Rahman, T. El Shishtawy, and A. Elewa, __Challenges of electronic voting—A survey,‘‘ Adv. Comput. Science: Int. J., vol. 4, no. 5, pp. 1 11, 2015.

[8] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, __Attacking the Washington, D.C. internet voting system,‘‘ in Proc. 16th Int. Conf. Financial Cryptogr. Data Secur., vol. 7397, Jan. 2012.

[9] T. Haines, O. Pereira, and V. Teague, __Running the race: A Swiss voting story,‘‘ in Proc. 7th Int. Joint Conf. E-Vote-ID, Bregenz, Austria. Cham, Switzerland: Springer, Jan. 2022.

[10] Reuters. (2017). Venezuelan Election Turnout Figures Manipulated by One Million Votes: Election Company. Accessed: Dec. 15, 2024.

[11] Al Jazeera. (2017). Election Chief Says Hacking Attempt Did Not Succeed. Accessed: Dec. 15, 2024.

[12] F. Rabia, A. Sara, and T. Gadi, __A survey on e-voting based on blockchain,‘‘ in Proc. 4th Int. Conf. Netw., Inf. Syst. Secur., KENITRA, Morocco, Apr. 2021.

[13] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, __E-voting system based on blockchain technology: A survey,‘‘ in Proc. Int. Conf. Inf. Technol. (ICIT), Amman, Jordan, Jul. 2021.

[14] U. Jafar, M. J. A. Aziz, and Z. Shukur, __Blockchain for electronic voting system—Review andopenresearch challenges,‘‘ Sensors, vol. 21, no. 17, p. 5874, Aug. 2021.

[15] T. Geng, L. Njilla, and C.-T. Huang, __A survey of blockchain-based electronic voting mechanisms in sensor networks,‘‘ in Proc. 20th ACM Conf. Embedded Netw. Sensor Syst., Nov. 2022,