BBVS - Blockchain Based Voting System

Assistant Professor Dr. Viji Rajendran V
Akshit Jasrotia
Ghulam Murtaza
Rohit Sharma

Department of Computer Science and Engineering (APJ.AKTU.), Palakkad, Kerala
NSS College of Engineering, Palakkad, Kerala

Abstract:- Any democracy must have an open voting process that satisfies the needs of the populace to give the appropriate individual the power. Additionally, the traditional voting systems currently in use have significant flaws and lack security and transparency. It has long been difficult to create a safe electronic voting system that provides the transparency and flexibility provided by electronic systems, while maintaining the fairness and privacy of present voting schemes. In this project, we assess a blockchain-based implementation of distributed electronic voting systems. It addresses some of the well-known blockchain frameworks with the aim of building a blockchain-based electronic voting system and presents a novel electronic voting system based on blockchain that tackles some of the shortcomings in existing systems. In particular, we evaluate the potential of distributed ledger technologies through the description of a case study; namely, the process of an election, and the implementation of a blockchain-based application, which improves the security and decreases the cost of hosting a nationwide election.

***Keywords**:- Blockchain, Ethereum, Voting System.*

I. INTRODUCTION

Democracy is the concept of allowing people to choose their leaders through the process of voting. It is crucial for the electoral system to be democratic, independent, and unbiased. This means that the voting process should be transparent, secure, and inclusive, allowing individuals to express their opinions freely. However, many individuals around the world lack trust in the election system. Conventional voting methods are often subject to control and interference by intermediaries. Issues such as booth capture, dummy voting, lack of proper monitoring, long queues at polling booths, fraudulent voting, pre-vote casting, redundant votes, inadequate law enforcement and audits, political instability, lack of awareness, and distant polling booth locations contribute to this lack of faith. Additionally, elderly individuals face significant challenges that result in a lower turnout of votes from this demographic.

The Electronic Voting Machine (EVM) has been proposed as an alternative to address the issues associated with the traditional voting system. However, even though EVMs were introduced to overcome certain problems, they still have their own set of security concerns and face challenges in gaining universal approval. One major issue with EVMs is their vulnerability to malware injection, which can manipulate the device and interfere with the server.

Another form of voting is Digital voting, which utilizes automated tools for casting ballots. There are two types of digital voting: e-voting, where voters use a voting machine, and i-voting, where they use an internet browser. Digital voting systems offer advantages such as flexibility, confidentiality, security, and convenience, as they enable voters to cast their ballots from anywhere in the world without being limited by geographical constraints. Several countries have already implemented digital voting methods. Estonia, for instance, was the first country to establish a national Internet voting system, allowing citizens to vote remotely through the internet from anywhere globally. Subsequently, Switzerland and Norway adopted electronic voting for regional and local elections, respectively.

Digital Voting, despite its advantages, also has certain drawbacks. One of the main criticisms of electronic voting systems in Estonia and Norway is the lack of transparency in significant portions of the code. The Estonian I-Voting system has limitations on ballot format due to concerns about confidentiality. Additionally, the centralization of power in the system makes it susceptible to Distributed Denial of Service (DDoS) attacks, which could render electoral elections unavailable to voters. Concerns about fairness and confidentiality of the voting process may also arise among voters. Police and security services have access to network traffic and processing capabilities, which raises the possibility of examining polling data for potential alterations. Despite efforts to enhance security, system attacks remain a possibility in previous schemes. Therefore, it is necessary to implement improved security measures or processes to ensure the reliability of voting and prevent the aforementioned issues.

Blockchain technology offers a reliable solution to address the aforementioned problems. With the emergence of blockchain, the concept of decentralization has gained recognition. Blockchain operates as a decentralized network, where node members exchange data while maintaining identical data replication. It provides features such as dissemination, privacy, and data accuracy. Leveraging blockchain technology, it becomes possible to establish a secure and dependable electronic voting system. This technology offers the potential to overcome the challenges associated with traditional digital voting systems.

A distributed web application that operates on the Ethereum blockchain is known as a dApp. These dApps utilize features such as Smart Contracts and can be developed and executed without the need for third-party manipulation, forgery, or interference. Smart contracts enable dApps to interact with the blockchain, and they are executed on the Ethereum Virtual Machine (EVM), which is a specialized platform for running these contracts. Once a smart contract is deployed on the EVM, it becomes immutable, meaning its code cannot be modified or tampered with.

Ethereum's EVM and its dedicated programming language have contributed to the significant growth of decentralized and distributed applications. These features have fostered a vibrant development community, continuous advancements, and the introduction of new technical possibilities.

When it comes to a voting system, it must fulfill several security properties such as authentication, transparency, anonymity, integrity, security, privacy, mobility, fairness, and verifiability to ensure a fair and transparent outcome. However, implementing an Ethereum-based application can be costly. Therefore, it is essential to consider the security properties that the proposed system satisfies while minimizing computational and storage costs. The implementation can be done using Ganache, a local blockchain platform integrated into Truffle, and the costs associated with general elections can be analyzed. Furthermore, a comparison can be made between the performance of the current proposal and previous approaches.

II. PROBLEM DEFINATION

Democratic countries worldwide face numerous challenges that hinder their growth due to illegal activities like corruption and human rights violations. One of the main issues lies in the voting system, which often prevents citizens from actively participating in elections. This lack of accessibility and transparency in the voting process leads to confusion and insecurity among the general population. In countries like Bangladesh, traditional voting systems involve lengthy processes, repetitive tasks, and various obstacles, including the capture of polling stations, tampering with ballots, separating poll agents from competitors, and intimidating voters to discourage their participation. Senior citizens, who make up 5.2% of the population in Bangladesh, particularly struggle to cast their votes, thereby compromising the true essence of democracy.

Furthermore, instances of unregistered voters participating in elections or dishonest clerks and officers manipulating results after voting further undermine the integrity of the electoral system. Authorities sometimes enforce strict measures such as ordering non-residents to leave the area, shutting down mobile networks, and implementing transportation bans to ensure fairness in voting, causing inconvenience and distress to the public. These restrictions also affect individuals who have urgent matters such as catching a flight or seeking emergency medical care. Additionally, citizens who are on holiday, business trips, or residing abroad for other reasons, including members of associations, are often unable to participate in the electoral process, resulting in decreased overall engagement and limiting their right to vote.

The concerns raised by citizens encompass issues related to protection, secrecy, accessibility, and anonymity in the voting process. Such circumstances breed a lack of trust in the democratic process and the administration, which ultimately undermines the society's belief in exercising their right to choose their leaders. These challenges pose significant obstacles to the true functioning of democracy and hinder the country's progress.

III. RELATED WORKS

In 2019, Pavel Tarasov and Hitesh Tewari [1] identifies a gap in the domain that can be filled with a protocol using a different technology. Blockchain technology offers an inherently secure platform, and the recent development of anonymous transaction schemes such as Zcash make it possible to tackle the anonymity issues of blockchain transactions, which could open up a possibility for blockchain voting. Although Ethereum has offered smart contract functionality since its inception, the much-needed anonymity factor has not been present in the protocol until now. The rapid growth of the Ethereum protocol and its integration with Zcash is likely to produce a protocol suitable for a widespread and inexpensive voting system.

The proposed protocol's applications are not limited to government elections but can be stretched to opinion polls or corporate elections, providing a unified platform for voting regardless of cost or circumstance. The goal of the proposed protocol is to create a cheaper and unified electronic voting system that can overcome the current limitations of electronic voting systems. The protocol has the potential to grow into a widespread implementation that deals with the assumptions and concerns that limit the current system.

In 2019, Xingyue Fan, Ting Wu, Qiuhua Zheng, Yuanfang Chen, Muhammad Alam, Xiaodong Xiao [2], proposed a new electronic voting scheme called HSE-voting to reduce the computational workload of the ballot tallying process. This scheme uses homomorphic signcryption, which allows for the encryption and signature of the ballot to be completed in one step and reduces the number of signature verifications needed during tallying. The scheme also provides privacy for voters and ensures the security and verifiability of the voting process. Citizens can view information on the B Board, voters can check their ballots, and anyone can verify the eligibility of the ballots.

They discusses the challenges in electronic voting schemes where the verification process in ballot tallying increases with the number of voters and candidates due to the requirement for digital signature verification. To address this issue, the authors propose a new electronic voting scheme called HSE-voting, which uses homomorphic signcryption to reduce the computational cost of verifying voter signatures. The signature homomorphism feature enables the number of signature verifications to depend on the number of candidates only, while the encryption homomorphism feature ensures that ballots are not decrypted during the tallying process.

In 2020, Micha Pawlaka, Aneta Poniszewska-Marandaa, Natalia Kryvinskab [3] proposed the ABVS e-voting system which proposes a solution for increasing the security of voting by using agents as intermediaries between voters and the system. These agents would be distributed by nodes, making it difficult to modify them outside of the nodes and enabling easy detection of any attempts to break into the system and manipulate the data.

Furthermore, this approach allows for the use of computing resources located in polling stations to process votes, which reduces the load on nodes. This solution has research potential, but it can be improved by incorporating smart contracts - digital agreements, scripts, and applications originating in the Ethereum network. Smart contracts enable automatic execution of contract terms without third-party involvement. Thus, they can be used to send intelligent agents in the form of transactions between the voting applications and trusted nodes, enhancing the efficiency and security of the e-voting system.

In 2020, Antonio M. Larriba, Jose M. Sempere, Damian Lopez [4],proposes a two-authorities voting system that provides the necessary security properties for a secure voting protocol. The proposed approach is correct and efficient and is based on simple RSA primitives, making it scalable and suitable for real-world scenarios. Unlike other systems, it does not rely on time-demanding interactive proofs or complex architectures. The vote encoding is flexible and minimal, allowing multiple types of elections with no overhead. The elector can check the traffic of messages to ensure the integrity of the system, and public bulletins can be audited by a third party.

The authors suggest that future research could investigate the possibility of implementing the identification of electors using an independent, public, and scrutinizable data structure, which would reduce the weight of the assumption of two unrelated entities. They also suggest adding mechanisms to allow the elector to certify more than one ballot as a way to bypass coercers. Empirical testing with real data would be essential to grant a solid infrastructure, which unfortunately is currently out of reach for the group.

In 2021, S K Geetha [5] introduced the first electronic voting system that used the Blind Signature Theorem as its foundation. The goal of the work was to protect the privacy of voters by using public key cryptography. Since then, extensive research has been conducted on electronic voting. Utilizing SHA1/SHA2, electronic scrambled marks are made conceivable by the ID card. Additionally, the Estonian ID card can be utilized as proof of identity when traveling within the EU and to access other electronic services offered by Estonia, such as health insurance and bank accounts. Even though the citizen is only known by a public location in the Blockchain organization, the panel that gave the option to participate knows the comparing address to each elector, so the citizen isn't completely unknown. This is the primary issue with these proposed Blockchain-based frameworks. Subsequently, the original technique makes decisions more open at the finish of the review. The public is guaranteed access to the decentralized system, which stores data, for checking and acquiring purposes by the system.

However, there is no assurance that the data will be error-free provided by the system. The accuracy of the data it receives must be guaranteed by a blockchain-based voting system.

In 2021, Saba Abdul-Baqi Salman, Sufyan Al-Janabi, Ali Makki Sagheer [6] discussed that earlier works that relied on the outline of bitcoin, such as O. Spycher et al. 2012), who has suggested a template for the authorities to use in determining whether a ballot was forged. By utilizing computerized cash's blockchain blueprint, counterfeit voting forms can be checked much more completely. This system does not use bitcoin or smart contracts and is entirely custom-programmed. As a result, the goal of this solution was to stop small chains from being attacked. Czepluch also discussed the uses of the blockchain in 2015, pointing to the possibility of using the blockchain for electronic voting systems. Czepluch utilized a brilliant agreement, which could make it slow and difficult to refresh the records. This paper discusses the application of Zcash, Bitcoin, Ethereum, and a cryptographic signature. First, the electronic voting system for the smart contract. This kind of implementation makes use of Ethereum wallets. This wallet can be used to identify the voter. Each voter's information is saved permanently by smart contact, but updating it is challenging and interacting with the voting system and scale takes time. Second, an electronic voting system based on Zcash. To hide bitcoin transactions, the cryptocurrency platform Zcash is used as a layer. To attack the zcash system, malicious software can be installed on the end-user device. Third, implementing electronic voting with a custom blockchain. These electronic voting systems work by building a blockchain without planning and without using a pre-built platform. This is a good option because the developer has control over the design, authentication, and security tools. Fourth, an electronic voting system that relies on a cryptographic signature. This kind of blockchain system makes use of bitcoin wallet addresses and ring signatures. This system hashes a key made from the voter's private key, candidate ID, and all voters' public keys. In any case, it is possible to use a signature in this type. As a result, e-voting can be implemented using a variety of blockchain paradigms that raise authentication and security concerns. Last but not least, this study recommends developing a brand-new platform to address the privacy and security concerns raised by the four most obvious platforms.

IV. PROPOSED METHODOLOGY

The proposed Digital Voting System allows voters to use smart devices to cast their votes, while those without smartphones can vote at designated voting stations. Both online and onsite voters follow the same voting process. The responsibility of initiating and concluding the election lies with the Admin, which interacts with smart contracts in the system. These smart contracts define the roles and actions involved in the election agreements, including various components and transactions. In the proposed blockchain-based digital voting, three smart contracts are utilized: the voter contract, candidate contract, and voting contract.

The voter contract handles the registration process, ensuring the security of voter information by storing the hash value of their data. This approach not only protects voter information but also maintains voter anonymity. The hash values are later used for voter authentication during the voting process. The candidate contract contains information about the candidates participating in the election.

Once the election begins, voters go through the authentication process, and they select a candidate from the list provided by the candidate contract. They then cast their vote using a vote coin, which represents their voting status. A vote coin with a balance of 1 indicates that the voter has not cast their vote, while a balance of 0 signifies that the voter has already voted. The casted vote is encrypted using a public key generated by the Admin's crypto server. The encrypted ballot is then sent to the voting contract and added as a block in the blockchain.

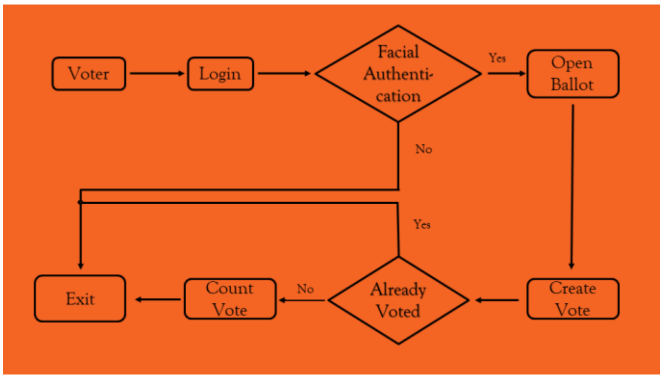

Fig 1: Proposed Architecture

V. IMPLEMENTATION

In order to create a decentralized application that can serve as a viable alternative to traditional voting systems, the development of a website is essential. This website will provide a secure and accessible voting environment for users. It will also cater to individuals who are unable to physically visit their designated polling locations, allowing them to conveniently vote through an intuitive online platform that displays their city's election ballot.

The initial step in implementing a blockchain-based voting system on the Ethereum network involves setting up the required infrastructure and environment. This entails creating the necessary technical framework and components to support the secure and transparent functioning of the voting system.

The overall system can be divided into two parts:

A. Server-Side
B. Client-Side

A. Server-Side

The server-side of the system consist of the following components.

- ➢ *Truffle*

As we mentioned that Truffle is a popular blockchain development framework that aims to make it easier for developers to build, test, and deploy decentralized applications (DApps) on the Ethereum network. It provides a suite of tools and features that allow developers to quickly develop and test smart contracts, deploy DApps to the blockchain, and interact with the Ethereum network.

We used Truffle for the compilation, deployment and debugging process of the smart contracts that are written to store the candidate details, changing the various phases of election, vote counting and result publication.

- ➢ *Solidity*

We used Solidity to write the system's Smart contracts. Solidity is a high-level programming language designed for writing smart contracts. Smart contracts are applications that run on the Ethereum blockchain and are automatically executed when certain conditions are met. Solidity is a statically typed language, which means that the types of variables and expressions must be declared before they are used. This helps to prevent errors and makes the code more readable. Solidity is also an object-oriented language, which means that code can be organized into classes and objects. This makes the code more modular and reusable.

- ➢ *Ganache*

We used Ganache for managing and testing the system at the local machine. Ganache is a personal blockchain development environment that allows developers to create, test, and deploy smart contracts without the need for a live Ethereum network.

- ➢ *Node Server*

A Node server, also known as Node.js server, is a web server built using the Node.js runtime environment. Node.js is a popular server-side platform that allows developers to build scalable, high-performance web applications using JavaScript.

Node servers can be used to handle tasks such as serving web pages, managing databases, and handling API requests. We use Node server to connect the client-side with the database, to integrate the face detection API with the system and to integrate the web server with the blockchain network.

B. *Client-Side*

The system has a client-side user interface that enables users to vote using their Ethereum accounts from any device. The UI is designed using CSS, JS, and HTML, and communication between the client and server is handled by the web3.js library, which provides an API for interacting with blockchain networks.

Metamask is a browser plugin used to store and manage Ethereum wallets and keys for sending and receiving Ethers. It acts as a bridge between the browser and the blockchain network and ensures user account security. The system ensures privacy and authentication by storing voter information as a hash in the blockchain network. The public key represents the voter's identity, and the hash value represents the voter's data, ensuring anonymity. Encrypted votes are sent to the smart contract, which then sends the vote coin to the candidate without disclosing the voter's identity. The system ensures that anonymity is maintained for voters' protection and privacy.

VI. RESULT

The system is successfully implemented and following are the results of the implemented system.

- *Anonymity*

To protect voters' anonymity, it is crucial that a voter's identity cannot be associated with a vote they make. Blockchain technology provides anonymity by using public keys as a voter's identification in the network. However, maintaining anonymity in an account-model-based system can be challenging because every transaction updates the account balance of both the sender and the recipient. Moreover, legislation can pose a new obstacle to widespread acceptance of the system even if privacy is well-protected. To ensure anonymity, the proposed method allows voters to enter their information into the blockchain anonymously using a hash function. Each voter's information is stored as a hash to preserve privacy and authentication. The public key represents the voter's identity, while the hash value represents the voter's data in the blockchain network. The casted vote is encrypted to prevent linking the voter's votes together. The smart contract decrypts all votes and sends the vote coin to the candidate without disclosing the voter's identity, thus preserving anonymity.

- *Integrity*

Ensuring the integrity of the voting process is essential to uphold the democratic principle of fair and transparent elections. In order to maintain voter privacy and prevent tampering, voter's identity is represented by a public key, and their vote is stored as a hash value. The use of a hash function and encryption ensures that individual votes cannot be traced back to specific voters.

To ensure the integrity of the voting process, the Merkle tree is used. The Merkle tree is a data structure that records each transaction in a block. Transactions are first hashed and placed in the tree's lowest tier. These hashes are then paired and hashed together, creating a new set of hashes that are then paired and hashed again until a single hash value remains at the top of the tree, known as the Merkel root. This process creates an unbroken chain of hashes, making it extremely difficult to modify or delete transactions without detection.

The use of the Merkle tree in the blockchain technology of the proposed digital voting system ensures the integrity of the voting process. Each transaction is recorded and hashed in the tree, creating an unbroken chain of hashes that make it difficult to modify or delete transactions without detection. This makes the proposed digital voting system secure, transparent, and trustworthy.

- *Fairness*

In order to prevent any impact on the voting of remaining voters, it is important to not collect any early results. This ensures fairness in the voting process and prevents any manipulation of votes. The Fairness process uses a digital commitment method and separates the voting and counting stages to ensure that results are kept secret throughout the voting phase. All votes are encrypted from the moment they are cast until the end of the election, which prevents partial results from being obtained. After the election ends, all casted votes are decrypted for counting. The voting stage is kept separate from the counting stage.

- *Security*

The proposed digital voting system ensures the protection of votes by preventing unauthorized access and coercion. The unchanging nature of blockchain technology ensures that the recorded votes cannot be tampered with. Any attempt to modify a transaction requires re-mining all the data blocks from that block onwards, as the hash function and the hash function of the previous block are used in each subsequent block. This leads to a different hash value that conflicts with the next block's hash value, requiring it to be re-mined as well.

This process is required for every block in the chain, making it incredibly difficult to exploit a single block of data. The computational power required for this is immense and almost impossible in real life. Therefore, the blockchain technology makes the system secure and ensures that the votes recorded in the system cannot be manipulated in any way.

- *Privacy*

To ensure that an individual's voting method is kept private, non-electronic voting systems physically shield the voter from prying. Similarly, in electronic voting systems, anonymity is maintained by protecting the privacy of voter identities. In our proposed system, the identity of a voter is recorded as a hash, which is unique to that voter and cannot be traced back to their specific vote. Additionally, all casted votes remain encrypted until the end of the election, and only then are they decrypted for counting. This ensures that the privacy of the voters is maintained throughout the voting process.

- *Mobility*

Mobility in voting refers to the ability of a voter to cast their vote from any location, without any constraints or limitations. The voting system should be easily accessible to all voters at any time. The proposed voting method enables voters to participate in the voting process from anywhere, using only a device with an internet connection and a blockchain address. This eliminates the need for additional infrastructure or specialized voting equipment.

VII. CONCLUSION

Many countries face significant challenges in ensuring stability and credibility in their voting systems. To address these concerns and promote voter engagement and fairness, we have developed a blockchain-based digital voting system that utilizes smart contracts. With this system, three smart contracts perform various operations throughout the entire election process, reducing reliance on third-party intermediaries.

In our system, casted votes are encrypted and securely stored until the end of the election. This ensures the confidentiality of the vote and prevents anyone from linking a vote to a specific voter. Voter information is stored as a hash, further safeguarding anonymity and reducing costs associated with data storage. Additionally, after the election concludes, voters can verify their vote using a unique vote ID they receive during the voting process.

Our system enables voters to conveniently and securely cast their votes from anywhere in the world using smart devices. This accessibility aims to increase voter participation and contribute to democratic practices in all regions. In summary, our approach offers maximum security properties, including anonymity, integrity, security, privacy, fairness, verifiability, and mobility, making it a viable solution for the election process.

REFERENCES

[1]. Pavel Tarasov and Hitesh Tewari (2019), “The Future Of E-Voting”. International Journal on Computer Science and Information Systems ,Vol. 12, No. 2, pp. 148-165

[2]. Xingyue Fan, Ting Wu, Qiuhua Zheng, Yuanfang Chen, Muhammad Alam, Xiaodong Xiao (2019) “HSE-Voting: A secure high-efficiency electronic voting scheme based on homomorphic signcryption”. Future Generation Computer Systems Volume 111, Pages 754-762

[3]. Micha Pawlaka, Aneta Poniszewska-Marandaa, Natalia Kryvinskab (2020), “Towards the intelligent agents for blockchain e-voting system”. Procedia Computer Science, Vol 141,pg 239–246

[4]. Antonio M. Larriba, Jose M. Sempere, Damian Lopez (2020)“A two authorities electronic vote scheme”. Computers & Security,Volume 97, 101940

[5]. S K Geetha (2021) “A Secure Digital E-Voting Using Blockchain Technology”. Journal of Physics: Conference Series, Vol 1916, 012197

[6]. Saba Abdul-Baqi Salman, Sufyan Al-Janabi, Ali Makki Sagheer (2021) “A Review on E-Voting Based on Blockchain Models ”. Iraqi Journal of Science, 2022, Vol. 63, No. 3, pp: 1362-1375