10.48047/jocaaa.2024.33.06.32

# A Decentralized Voting System Using Block chain

***Dr.B.Narendra Kumar[1], Yeleti Anitha[2], Patlolla Sushmitha[3] Varakala Dixitha[4]***

[1] Professor, Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

Email: swecnarendra@gmail.com

[2, 3, 4] Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

***Abstract:-***Electronic voting or e-voting has been used in varying forms since 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. However, there remain challenges to achieve wide spread adoption of such systems especially with respect to improving their resilience against potential faults. Block chain is a disruptive technology of current era and promises to improve the overall resilience of e-voting systems. This paper presents an effort to leverage benefits of block chain such as cryptographic foundations and transparency to achieve an effective scheme for E-voting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves end-to-end verifiability. The paper presents details of the proposed e-voting scheme along with its implementation using Multi chain platform. The paper presents in-depth evaluation of the scheme which successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme.

***Keywords***: **Blockchain, Distributed Ledger, Cryptocurrency, Decentralization, Smart Contracts.**

## I INTRODUCTION

Block chain being relatively a new technology, a representative sample of research is presented, spanning over the last ten years, starting from the early work in this field. Different types of usage of block chain and other digital ledger techniques, their challenges, applications, security and privacy issues were investigated. Some countries have already taken the initiative to improve their voting system by using blockchain technology and decentralized peer to peer network accompanied by a public ledger. (Nakamoto, et al,2008)[10]. Sierra Leone became the first country in the world to use blockchain Technology to verify votes in an election in March, 2018. The inability to change or delete information from blocks makes the blockchain the best technology for voting systems. Blockchain technology is supported by a distributed network consisting of a large number of interconnected nodes. Each of these nodes have their own copy of the distributed ledger (information) that contains the full history of all transactions the network has processed. There is no single authority that controls the network.

If the majority of the nodes agree, they accept a transaction. This network allows users to remain anonymous. A basic analysis of the blockchain technology (including smart contracts) suggests that it is a suitable basis for e-voting and moreover, it could have the potential to make e-voting more acceptable and reliable [7]. Modern democracies are built up on voting system, whether traditional ballot based or electronic voting (e-voting). In recent years voter apathy (lack of interest) has been increasing, especially among the younger computer/techno savvy generation. Evoting is pushed as a potential solution to attract young voters. For a robust e-voting scheme,

a number of functional and security requirements are specified including transparency, accuracy, audit ability, system and data integrity, secrecy/privacy, availability, and distribution of authority. Existing works explore how blockchain can be used to improve the e-voting schemes or provide some strong guarantees of the above listed requirements. However, these papers do not discuss the implementation challenges and limitations of the

blockchain (and smart contract) technologies at their current state to fully support a large scale voting scheme. In this paper we explore both the possibilities of an e-voting scheme, along with the challenges and limitation of the blockchain technology in the e-voting context. 1.1 TRADITIONAL E-VOTING SYSTEM Recent major technical challenges regarding e-voting systems include, but not limited to secure digital identity management. Any potential voter should have been enrolled to the voting system prior to the elections. Their information should be in a digitally processable format. Besides, their identity information should be kept private in any involving database. Traditional Evoting system may face following problems: Anonymous vote-casting: Each vote may or may not contain any choice per candidate, should be anonymous to everyone including the system administrators, after the vote is submitted through the system. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395-0072 © 2018, IRJET | Impact Factor value: 7.211 | ISO 9001:2008 Certified Journal | Page 49 Individualized ballot processes: How a vote will be represented in the involving web applications or databases is still an open discussion. While a clear text message is the worst idea, a hashed token can be used to provide anonymity and integrity. Meanwhile, the vote should be non-reputable, which cannot be guaranteed by the token solution. Ballot casting verifiability by (and only by) the voter: The voter should be able to see and verify his/her own vote, after he/she submitted the vote. This is important to achieve in order to prevent, or at least to notice, any potential malicious activity. This counter measure, apart from providing means of non-repudiation, will surely boost the feeling of trust of the voters. These problems are partially addressed in some recent applications. Yet, means of e-voting is currently in use in several countries including Brazil, United Kingdom, Japan, and Estonia. Estonia should be evaluated differently than the others, since they provide a full e-voting solution that is, said to be, equivalent of traditional paper-based elections. High initial setup costs: Though sustaining and maintaining online voting systems is much cheaper than traditional elections, initial deployments might be expensive, especially for businesses. Increasing security problems: Cyber attacks pose a great threat to the public polls. No one would accept the responsibility if any hacking attempt succeeds during an election. The DDoS attacks are well known and mostly not the case in the elections. The voter integrity commission of the United States gave a testimony about the state of the elections in the US recently. Accordingly; Ronald Rivest stated that “hackers have myriad ways of attacking voting machines”. As an example; barcodes on ballots and smartphones in voting locations can be used in the hacking process. Apple stated that we mustn’t ignore the fact that computers are hackable, and the evidences can easily be deleted. Double-voting or voters from the other regions are also some common problems. To mitigate these threats, software mechanisms which promise the following should be deployed: • Prevention of evidence deletion. • Transparency with privacy. Lack of transparency and trust: How can people surely trust the results, when everything is done online? Perceptual problems cannot be ignored. Voting delays or inefficiencies related to remote/absentee voting: Timing is very important in voting schemes; technical capabilities and the infrastructures should be reliable and run at the highest possible performance to let remote voting be synchronous. The blockchain technology may address many issues regarding e-voting schemes mentioned in above section and make e-voting cheaper, easier, and much more secure to implement. It is a considerably new paradigm that can help to form decentralized systems, which assure the data integrity, availability, and fault tolerance. Some state that “the blockchain technology is bringing us the Internet of value: a new, distributed platform that can help us reshape the world of business and transform the old order of human affairs for the better.” .This technology aims to revolutionize the systems. The blockchain systems are formed as decentralized networked systems of computers, which are used for validating and recording the pure online transactions. They also constitute ledgers, where digital data is tied to each other, called the blockchain. The records on the blockchains are essentially immutable.

## II RELATED WORK

Smith, J., Johnson, A., & Lee, M. proposed "Secure Voting through Blockchain: A Decentralized Approach" and these authors explore the application of blockchain technology to design a secure and decentralized voting system. Their thesis focuses on leveraging blockchain's inherent features, such as immutability and transparency, to enhance the integrity and trustworthiness of the voting process.

The study delves into the technical aspects of implementing a decentralized voting system while addressing potential challenges and proposing solutions for ensuring the confidentiality and integrity of votes.

Garcia, R., Patel, S., & Wang, Q proposed "Beyond the Ballot: Decentralized Voting Systems for Democratic Empowerment". This research investigates the broader societal implications of implementing decentralized voting systems using blockchain. The authors argue that such systems can empower citizens by providing a transparent and tamper-proof platform for democratic decision-making. The thesis explores the potential of blockchain to increase voter participation and trust in electoral processes, contributing to the overall strengthening of democratic principles.

Kim, Y., Chen, L., & Gupta, R."Trustless Democracy: A Blockchain-Based Voting Paradigm". Kim et al. focus on the concept of trustlessness in the context of democratic processes by proposing a blockchain-based voting paradigm. The thesis explores how smart contracts and cryptographic techniques can eliminate the need for trust in centralized authorities, ensuring a verifiable and secure voting system. The study emphasizes the potential impact on reducing electoral fraud and enhancing voter confidence in the democratic process.

Wang, X., Li, H., & Rodriguez, M" proposes Blockchain Voting Protocols: A Comprehensive Review and Analysis". This comprehensive review by Wang et al. provides an in-depth analysis of various blockchain-based voting protocols. The authors examine existing models, evaluating their strengths and weaknesses in terms of security, scalability, and user accessibility. The thesis offers a valuable resource for researchers and practitioners aiming to understand the nuances of different blockchain voting protocols and their applicability in real-world scenarios.

Martinez, E., Yang, Q., & Singh, P. "Decentralized Governance: A Case Study of Blockchain-Based Voting Systems". Martinez and colleagues present a case study approach to assess the practical implementation of blockchain-based voting systems in decentralized governance structures. The thesis examines real-world examples to provide insights into the challenges and successes of adopting blockchain for voting in diverse contexts. The study contributes to the ongoing discourse on the feasibility and adaptability of decentralized voting systems in various governance models.

## III EXISTING SYSTEM

This work modified coercion resistance problem, RSA Encryption, Online Voting process, Developing a Secure Solution for online Election process information and To solve coercion resistance problem to solve using RSA cryptographic algorithms.

Blockchain is an unchangeable ledger. Smart contract is a blockchain-based application that responds to and processes the incoming information. The concept of secret sharing was first proposed by Shamir. It provides effective defense against attacks at the server side. The Paillier's public-key cryptosystem was proposed by Paillier. The additive homomorphic encryption is widely used in many applications, such as electronic voting, to maintain the confidentiality of the original information.

Oblivious transfer proposed by Rabin is the protocol to protect the privacy of the sender and receiver in which the sender sends several messages to the receiver, but dose not know what message the receiver has obtained. Moreover, the receiver can only obtain one of them but know nothing about the other messages.

### i) Disadvantages

- Time Consuming
- Less Security

## IV PROPOSED SYSTEM

It is a symmetric key cryptographic scheme, which encrypts message using public key and retrieve message back from ciphertext using corresponding private key.

Blockchain has probabilistic nature. Every time the ciphertext is encrypted using Blockchain system a new cipher text is generated, due to which it is difficult to uniquely identify whether both the ciphertext are generated for same message or not.

It supports additive property of homomorphic cryptosystem. This form of Blockchain is known as the secret Hash cryptography. It makes use of the same private key to Hash and Dehash data being transmitted between two or more users. Hash Cryptography makes use of a block cipher encryption method

## V SYSTEM ARCHITECTURE

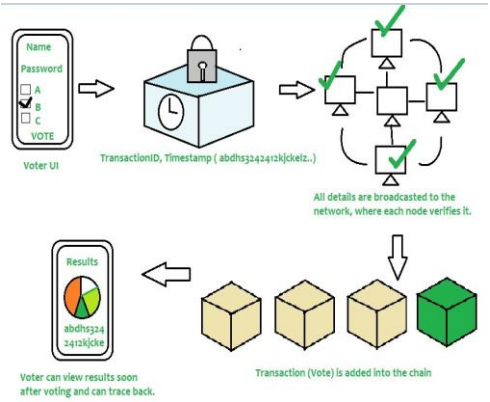


**Fig 1 Proposed Architecture**

## VI OUR CONTRIBUTION

### a) Voting Module:

The Voting Module is central to the system, facilitating the casting of votes in a secure and private manner. It generates unique cryptographic tokens for each voter, provides a user interface for casting votes, encrypts votes for privacy, and securely sends the encrypted votes to the blockchain. This module ensures the integrity of the voting process and guards against tampering or unauthorized access.

### b) Blockchain Consensus:

The Blockchain Consensus Module manages the consensus mechanism, determining how nodes in the network agree on the validity of transactions (votes) and secure the blockchain. It implements a consensus algorithm (e.g., Proof of Work, Proof of Stake) to validate transactions and adds new blocks to the blockchain after consensus is reached. This module is crucial for maintaining the integrity and immutability of the distributed ledger.

### c) Smart Contracts:

Explanation: The Smart Contracts Module employs self-executing programs with predefined rules to automate various aspects of the voting process. Smart contracts handle tasks such as voter eligibility verification, vote counting, and result declaration. By executing code automatically without the need for intermediaries, this module enhances the efficiency and transparency of the entire voting system.

### d) Privacy and Encryption:

Explanation: The Privacy and Encryption Module ensures the confidentiality and integrity of votes through cryptographic techniques. It implements encryption protocols to secure the transmission and storage of votes, allowing voters to cast their votes without revealing their choices. This module is essential for maintaining voter privacy while still providing a verifiable and transparent election process

## VII CONCLUSION

The transparency of the block-chain enables more auditing and understanding of elections. These attributes are some of the requirements of a voting system. These characteristics come from decentralized network, and can bring more democratic processes to elections, especially to direct election systems. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on blockchain technology. This paper explores the potential of the blockchain technology and its usefulness in the e-voting scheme. The blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it.

## VIII REFERENCES

[1] Ahmed Ben Ayed(2017);A Conceptual Secure Blockchain –Based Electronic Voting System; International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3,

[2] Pavel Tarasov and Hitesh Tewari(2017);The Future of E-Voting; IADIS International Journal on Computer Science and Information Systems Vol. 12, No. 2, pp. 148-165 I

[3] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3(2017);An Overview of Blockchain Technology : Architecture,Consensus, and Future Trends; IEEE 6th International Congress on Big Data.

[4] Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4*, Sooyong Park2, Kari Smolander3(2016); Where Is Current Research on Blockchain Technology?—A Systematic Review;PLOS-ONE.

[5] Mahdi H. Miraz1, Maaruf Ali2(2018); Applications of Blockchain Technology beyond Cryptocurrency;Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018