SEVA - Secure and Efficient Voting Application

[1]Adarsha Sagar H V, [2]Isha Varma, [3]Achintya A A, [4]Adith Kadam, [5]Anika Prem

[1]Assistant Professor,[2]Student,[3]Student, [4]Student, [5]Student
[1]department of Computer Science and Engineering,
[1]RV Institute of Technology and Management, Bangalore, India

Abstract - Voting refers to the act of formally expressing one's choice or opinion in a decision-making process. It is commonly associated with the election of representatives, the enactment of laws, or other significant determinations. In recent times, there has been a shift from traditional paper-based voting systems to electronic voting systems. Electronic voting systems offer many advantages over traditional paper-based systems, including reduced voting time, increased accuracy, and the ability to count votes quickly and easily.

However, there are concerns regarding the security and authenticity of electronic voting systems, particularly in centralized systems where there is the potential for manipulation and fraud.

This paper introduces a voting mechanism based on Ethereum Blockchain with the aim of overcoming the challenges faced by contemporary voting systems and ensuring the electoral process remains fair and secure. The use of blockchain technology has been proposed as a solution to enhance the integrity of electronic voting systems. Blockchain-based voting systems are decentralized, transparent, and secure, ensuring that the voting process is free from manipulation and fraud.

Index Terms – Blockchain, E-Voting, Decentralized, Cryptography, Secure

I. INTRODUCTION

Voting is the manifestation of citizens' commitment to the country and the government's devotion to the citizens. Voting is considered a fundamental component of democratic societies; it is an act which enables the people of the state to express their political, socio-economic, legal, and religious opinions plainly and freely. The paper-based voting system is high-priced, prolonged, and labor-intensive, thus, prompting the exploration of electronic voting as an alternative. Various cryptographic procedures have been implemented in an attempt to introduce transparency and trust in electronic voting systems. The present-day electronic election method is vulnerable to numerous obstacles including election tampering, decreased voting accuracy, and disenfranchisement.

Blockchain is a rapidly developing technology that has already established itself as a reliable means of transferring data and facilitating transactions without the need for intermediaries. It is one of the most sought-after building blocks for applications that aid finance, healthcare, education, and other related domains. Essentially, a blockchain is a decentralized and distributed digital record collection which facilitates secure and transparent storage or transfer of data. In the last several years, the term "blockchain" has been synonymous with a secure online example of technology.[1] Electronic voting (e-voting) is one of the emerging applications of blockchain whereby researchers aim to leverage benefits such as integrity, anonymity and non-repudiation which are critical for a voting application.[2]

Connected to a centralized database, the contemporary voting machine can be tampered with by a person who has physical access to it. It may cause single point of failure in the whole network of the voting system; on the other hand, an immutable blockchain would not be affected by an individual saboteur in the network. In a blockchain, the data is being stored in a decentralized manner, which is constantly verified if the records are accurate. Therefore, in case of a malicious attack on a node, only that node would be affected and peer to peer network still provide all services.[3] Most voting procedures are now centralized, licensed by the critical authority, controlled, measured, and monitored in an electronic voting system, which is a problem for a transparent voting process in and of itself.[4] Blockchain will allow all to cast their votes on smartphone or from the computer with the apps, rather than having a queue at polling stations. Implementing blockchain will not require a government to change their existing system rather their existing platform can be re-modelled.[5] In theory, blockchain-based voting systems have a number of advantages over conventional ones such as decentralization, transparency, and immutability.[6]

This paper encourages the implementation of a more smart, secure, transparent, simple and swift method for vote casting. The approach describes the use of Ethereum Blockchain to decentralize the process and Keccak cryptographic algorithm to encrypt the information regarding the voters and votes. SEVA (Secure and Efficient Voting Application) will, thus, entirely transform the practice of voting for the government and the citizens.

II. EXISTING SYSTEM

K. Keerthi et al.[1] put forth a block chain-based electronic voting system to allay concerns about the security and dependability of large-scale e-voting systems. The goal of the paper is to identify conditions that can result in a successful attack by looking into the potential for transaction malleability attacks within a block chain-based application (e-voting). The proposed system implements the AES algorithm. This algorithm converts the given plain text into a cipher text by using methods such as byte substitution, shifting rows, mixing columns, and adding round keys.

Chang-Hyun Roh and Im-Yeong Lee[7] have proposed an electronic voting system that uses blockchain technology to ensure reliability and data integrity, as well as secret voting. The paper highlights the importance of addressing concerns regarding the security and reliability of e-voting systems, especially when implemented on a large scale. The proposed system utilizes a method involving two factor authentication. Each user is provided with a pin before and after casting the vote which provides a sense of increased security to the entire system.

In order to forecast future developments, Kumar D Dwijesh et al.[8] examine the current state of blockchain-based voting research and online voting systems. The authors claim that the chain of blocks is built and maintained by a peer-to-peer network, and that each block in the chain is kept intact by sophisticated cryptography algorithms. The paper proposes a novel approach that combines two different blockchains in order to achieve privacy and anonymity.

Md. Razu Ahmed et al.[9] have designed a system which implements the longest chain rule as a solution to multiple users casting their vote which might end up linking to only one hash code. A major limitation of this system is that the voter cannot withdraw his/her vote once casted. However, the paper focuses on how block chain technology has the potential to change elections and ensure the validity of the voting process.

III. PROPOSED SYSTEM

Blockchain is a decentralized digital ledger in a P2P network, where a copy of the append-only ledger of digitally signed and encrypted transactions is maintained by each participant.[6] It creates a data 'block' for every transaction or piece of information that is provided to the system. Each block is then added to the existing chain of blocks, thereby creating a record of the data. Every block is uniquely identified using a digital signature called a hash, which is generated using different security or digital authorization algorithms. A hash is responsible for a block's security and ensuring that it is not tampered with. Adding new blocks to a chain is done by a network of computers (called nodes) which verify and validate each new piece of information they get. Each block consists of a cryptographic hash value of the previous block, a timestamp and transaction data. For using distributed ledger, blockchain manages peer-to-peer network which helps in inter-node communication and validating new blocks.[5] The structure of blockchain is shown in Figure 1.

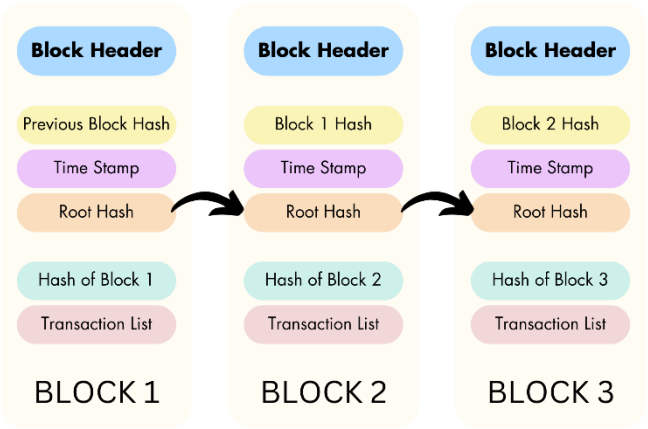

Figure 1. Structure of Blockchain

The most important feature of blockchain technology is that all participants have the same data in the form of the distributed databases. Periodically generated blocks are connected in order of block thus, if the data is falsified or modulated, the attacker cannot easily modulate the data because the subsequent blocks must be changed from the previous block.[7] Blockchain has various classifications and characteristics, as indicated in Table 1 below.

Table 1. Taxonomy of Blockchain

	Public	Private	Consortium
Participants	Anyone	Individuals/Companies	Consortium Members
Network	P2P Network	Fast Network	Fast Network
Bookkeeper	Anyone	Custom	Consortium Negotiation
Incentive Mechanism	Need	No need	Optional
Decentralization	Decentralized	Centralized	Polycentric
Validation Speed	Slow	Fast	Medium
Transaction Data	Public	Semi-Public	Private

Smart contract is an automatic program contract, which is triggered automatically once the pre-set conditions are satisfied. Blockchain makes smart contract possible through a reliable code execution environment. The smart contract is written into blockchain in a digital form, and the features of blockchain technology ensure that the whole process of storage, reading, and execution is transparent, traceable, and not tampered with.[6] Smart contracts allow trusted transactions to be made without third parties. Due to its consistency and widespread use along with the provision of smart contracts, Ethereum and its network is one of the most suitable platforms for e-voting via blockchain. The research methodology for SEVA has been described in Figure 2.

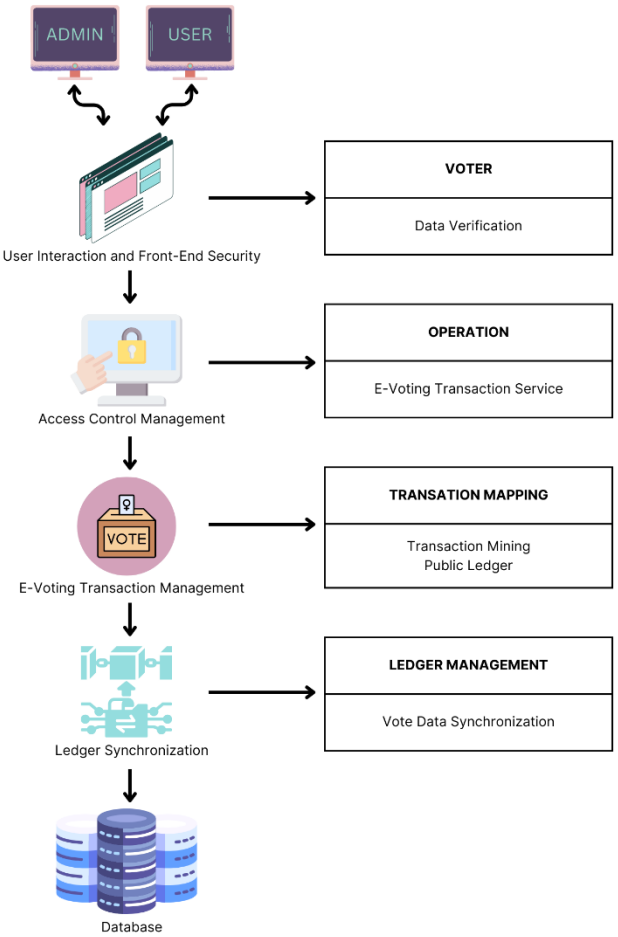

Figure 2. Research Methodology

This blockchain voting system uses Keccak-256, a cryptographic function, which is a part of Solidity (SHA-3 Family). The function computes the hash of an input to a fixed-length output. This cryptographic hash function can only be used in one direction and cannot be reversed. Ethereum uses Keccak-256 in a consensus engine called Ethash. Its structure, shown in Figure 3 is the extremely simple sponge construction and internally it uses the innovative Keccak-f cryptographic permutation. After its selection as the winner of the SHA-3 competition, Keccak has been standardized in 3GPP TS 35.231 for mobile telephony, and in NIST standards FIPS 202 and SP 800-185.

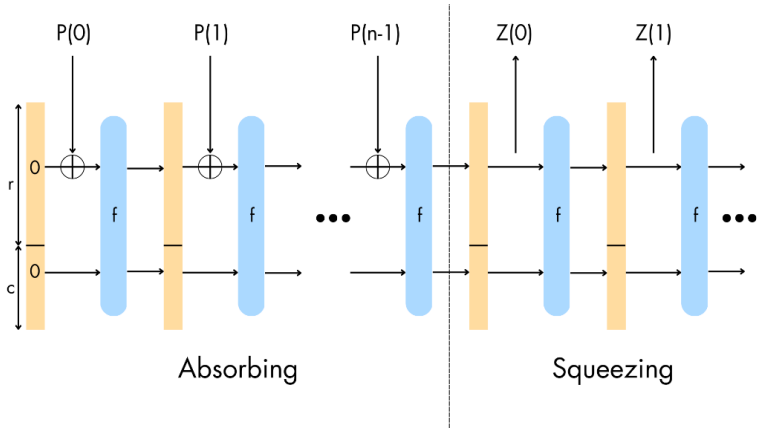

Figure 3. Sponge Construction of Keccak Algorithm

The proposed system implements the Keccak (SHA3-512) cryptographic algorithm to enable secured transactions. Unlike the SHA-256 algorithm applied in various similar applications, Keccak offers higher security against collision attacks. Software implementation of Keccak have reported 41 cpb on IA-32+MMX - Intel Pentium 3, 20 cpb on IA-32+SSE - Intel Core 2 Duo or AMD Athlon 64 and 12.6 cpb on a typical x86-64-based machine.[11] Keccak works faster on systems which have functions to specifically compute SHA3. In hardware implementations, SHA3 is remarkably faster than SHA2 and SHA1.[12] Table 2 demonstrates the features of Keccak which make it a safer and more effective algorithm to use for the blockchain voting system.

Table 2. Comparing Keccak with SHA-256

Algorithm	Rounds	Output Size (bits)	Internal State Size (bits)	Block Size (words)	Operations	Security Against (bits)		Performance on Skylake (median cycles/byte)	
						Collision Attacks (bits)	Length extension Attacks (bits)	Long Messages	8 Bytes
SHA-256	64	256	256	32-bit	AND, XOR, OR, SHR, ADD (mod 2^{32})	128	0	7.63	85.25
Keccak (SHA3-512)	24	512	1600	64-bit	AND, XOR, ROT, NOT	256	1024	15.88	164

In the proposed system, citizens must register themselves as voters through the portal. Their identity is verified and cross-checked with Aadhar details using their Unique Aadhar Number. Only the administrator can add information of the candidates appearing for the election. The administrator must confirm the authenticity of the registered information and verify the registrants. Once a citizen has been authorized as a valid voter by the administrator, he/she may proceed to the voting area. The voting area is only accessible after all candidates have been registered and election is declared open. A voter can vote for once for only one candidate (following the rules of the election). When the voting period is over, the administrator announces the end of the polling process. The votes are calculated automatically and the result is displayed in the result section of the portal by the administrator. The entire process is completely transparent and anyone can verify the legitimacy of the election. The below Figure 4 represents the basic model of the SEVA architecture.

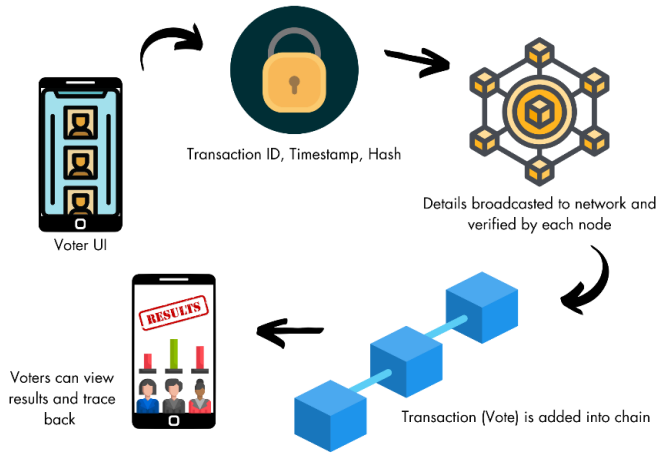

Figure 4. Blockchain Voting Architecture

IV. Conclusion

It is evident through various researches and comparisons that the current electronic election procedure is on the decline. A voting system based on blockchain will undoubtedly be secure against cyberattacks and traditional vulnerabilities. With blockchain voting, issues regarding voter confidence, transparency and accessibility can be easily solved in future elections. It presents other advantages such as low-cost set-up, rapid and accurate results, and fraud prevention. A system like SEVA can be implemented achieve an end-to-end verifiable e-voting scheme and revolutionize elections in the country.

V. References

[1] K. Keerthi, N. Venkatesh, G. Dhana Lakshmi, N. Sai Chand, D. Haritha, "E-Voting System Using Blockchain Technology," *Journal of Critical Reviews*, vol. 9, no. 4, pp. 243–254, 2022, doi: 10.31838/jcr.09.04.31.

[2] Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan, "Investigating performance constraints for blockchain based secure e-voting system", *Future Generation Computer Systems*, vol. 105, pp. 13-26, 2020, doi: 10.1016/j.future.2019.11.005.

[3] M. S. Farooq, U. Iftikhar, and A. Khelifi, "A framework to make voting system transparent using blockchain technology," *IEEE Access*, vol. 10, pp. 59959–59969, Jun. 2022, doi: 10.1109/ACCESS.2022.3180168.

[4] Jafar, U.; Aziz, M.J.A.; Shukur, Z. "Blockchain for Electronic Voting System—Review and Open Research Challenges", *Sensors*, vol. 21, pp. 5874, 2021, doi: 10.3390/s21175874.

[5] A. Indapwar, M. Chandak, and A. Jain, “E-voting system using blockchain technology,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 2775–2779, 2020, doi: 10.30534/ijatcse/2020/45932020.

[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,” *ACM Computing Surveys*, vol. 54, no. 3, pp. 1–28, Apr. 2021, doi: 10.1145/3439725.

[7] C.-H. Roh and I.-Y. Lee, “A Study on Electronic Voting System Using Private Blockchain ,” *Journal of Information Processing Systems*, vol. 16, no. 2, pp. 421–434, Apr. 2020, doi: 10.3745/JIPS.03.0135.

[8] Kumar D Dwijesh, Chandini D.V., Reddy Dinesh, "Secure Electronic Voting System using Blockchain Technology", *International Journal of Smart Home*, vol. 14, pp. 31-38, 2020, doi: 10.21742/IJSH.2020.14.2.04.

[9] Md. Razu Ahmed, F M Shamrat, Md. Asraf Ali, Md Rajib Mia, Mst. Arifa. Khatun, "The Future of Electronic Voting System Using Blockchain", *International Journal of Scientific & Technology Research*, vol. 09, pp. 4131-4134, 2020.

[10] M Kamil, A Bist, U Rahardja, N Santoso, Mohd. Iqbal, "Covid-19: Implementation e-voting Blockchain Concept", *International Journal of Artificial Intelligence Research*, vol. 5, no. 1, pp. 25-34, Dec, 2020, doi: 10.29099/ijair.v5i1.173.

[11] Longa, P., Wang, W., Szefer, J. (2021), "The Cost to Break SIKE: A Comparative Hardware-Based Analysis with AES and SHA-3", *In: Malkin, T., Peikert, C. (eds) Advances in Cryptology – CRYPTO 2021, Lecture Notes in Computer Science()*, vol 12827, Springer, doi: 10.1007/978-3-030-84252-9_14.

[12] Thibaut Vandervelden, Ruben De Smet, Kris Steenhaut, An Braeken, "SHA3 and Keccak variants computation speeds on constrained devices", *Future Generation Computer Systems*, vol. 128, pp. 28-35, 2022, doi: 10.1016/j.future.2021.09.042.