



Voting Application Using SHA-256 Algorithm In Blockchain

PARMESHWAR HALE
CS,DPCOE(SPPU)
PUNE,INDIA

YOGESH MANDLIK
CS,DPCOE(SPPU)
PUNE,INDIA

HARSHAL DHAPATE
CS,DPCOE(SPPU)
PUNE,INDIA

MANGESH OHOL
CS,DPCOE(SPPU)
PUNE,INDIA

PROF. SUPRIYA RAJSHEKHAR
AGRE
CS,DPCOE(SPPU)
PUNE,INDIA

Abstract— This project proposes the design and implementation of a blockchain-based voting application. The proposed system utilizes the Java programming language and the SHA-256 hashing algorithm to ensure secure data storage. The voting process is conducted using Java servlet pages, and the system utilizes proof of work for consensus. Security and privacy analysis, as well as performance evaluation, are conducted to ensure the efficiency and reliability of the system.

Keywords—*sha-256;proof-of-work; java; blockchain; etc.*

Introduction —Voting is an integral part of democracy and an essential aspect of any election process. With the advancement in technology, the traditional method of voting has become outdated and vulnerable to various threats such as tampering and hacking. The use of blockchain technology has emerged as a potential solution to address these issues by providing a secure, transparent, and tamper-proof platform for conducting voting. This project aims to develop a voting application using blockchain technology. The purpose of this project is to design a voting application using blockchain technology. The use of blockchain technology in voting systems provides an immutable and transparent ledger of votes that can be audited and verified by anyone. The proposed system will be implemented using the Java programming language and will utilize the SHA-256 hashing algorithm for secure data storage.

The use of blockchain technology in voting systems has been a topic of interest in recent years. Several studies have been conducted on the potential benefits of utilizing blockchain for voting. One study found that blockchain technology can enhance the security and transparency of voting systems while also providing a verifiable and tamper-proof ledger of votes. Another study explored the use of blockchain in electronic voting systems, highlighting its potential to reduce the risk of electoral fraud and improve voter confidence in the electoral process. Blockchain technology has gained immense

popularity in recent years due to its potential to provide a secure and transparent platform for various applications. Several researchers have proposed blockchain-based voting systems that aim to address the challenges of traditional voting methods. The existing literature suggests that blockchain-based voting systems can provide a secure and transparent platform for conducting elections.

The implementation and related performance measurements are given in the paper along with the challenges presented by the block chain platform to develop a complex application like e-voting. The paper highlights some shortcomings and presents two potential paths forward to improve the underlying platform (block chain technology) to support e-voting and other similar applications. Block chain technology has a lot of promise; system in its current state it might not reach its full potential. There needs to be concerted effort in the core block chain technology research to improve its features and support for complex applications that can execute within the blockchain network efficiently and effectively.

Literature survey— System presented in the Issues and Effectiveness of Blockchain Technology on Digital Voting that block chain is a technology that enables moving digital coins or assets from one individual to other individual. Blockchain concept can be understand with the concept of linked list in Data Structure, because its next key address is stored in previous key and they are linked with each other [1]. System presented in the Electronic voting machine based on Blockchain technology and Aadhar verification that A nation with less voting percentage will struggle to develop as choosing a right leader for the nation is very essential. Our proposed system designed to provide a secure data and a trustworthy election amongst the people of the democracy. Since aadhar card is the most needed for a person identity hence deploying an election process using

it is highly recommendable. Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it [2]. An E-Voting Protocol with Decentralization and Voter Privacy that a potential solution to the lack of interest in voting amongst the young tech savvy population. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on block chain technology. This paper explores the potential of the block chain technology and its usefulness in the e-voting scheme. an e-voting scheme, which is then implemented [3]. System present the Design of Distributed Voting Systems. Electronic voting systems attempt to be as easy to use and secure as ideal traditional elections and attempt to eliminate the human errors described [4].

Proposed system—

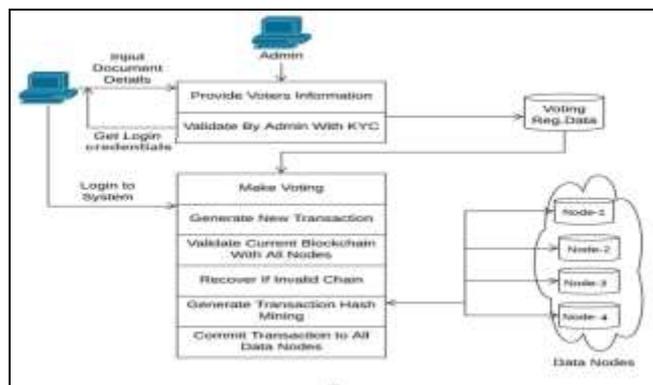


Fig.1 System Architecture

The proposed scheme utilizes blockchain technology to maintain a tamper-proof record of all votes. The system uses smart contracts to automate the voting process, ensuring that all votes are counted correctly. The system also utilizes digital signatures and encryption techniques to ensure the security and privacy of voter information. The proposed system utilizes several algorithms and formulae to ensure the security and privacy of voter information. These include the SHA-256 hash function [10]. The proposed system is designed to operate on a distributed network of nodes that are responsible for storing and validating transactions. The system utilizes the SHA-256 hashing algorithm to secure the data stored on the blockchain. The voting process is conducted using Java servlet pages, which are dynamically generated web pages that can interact with the backend database. The proposed voting application will utilize a blockchain-based architecture to store and validate votes. The system will employ proof of work as a consensus mechanism to ensure that all transactions are valid and consistent across the network. The voting process will be conducted using Java servlet pages, which will communicate with the backend blockchain database.

User can vote online by using this system. User first need to register his/her information. After register he/she need to login into the system. If the user is valid then he/she can vote. Else they cannot. This system is manage by the Admin. Admin can validate all attributes . Admin upload information in database . The the information is valid profile will be upload successfully . After that it will update to all nodes.

Methodologies—

The proposed system will utilize the following methodologies:

- I. Blockchain technology for secure data storage and validation.
- II. Proof of work as a consensus mechanism for validating transactions.
- III. Java servlet pages for conducting the voting process.
- IV. SHA-256 hashing algorithm for securing the data stored on the blockchain.

Blockchain, the digital ledger technology that can securely maintain continuously growing lists of data records and transactions, has the power to potentially transform health care, according to industry experts. By simplifying and expediting the way the voting industry processes data in such areas as revenue cycle management, health data interoperability and supply chain validation, blockchain has the power to dramatically reduce back-office data input and maintenance costs and improve data accuracy and security.

- I. *Product Perspective:* This product is independent and self-contained. It is not a part of any larger software and can be used as a standalone product.
- II. *Product Feature:* The major functionalities that the software shall provide are: -Enabling users to vote online. Admin can manage the system effectively.

- III. *User Classes and Characteristics:* The average user of this product is assumed to be familiar with online programming contests and their functioning. The voter is also expected to know standard terminology like ‘vote’, ‘submissions’ etc. We have optimized our interface to suit the needs of such users.
- IV. *Operating Environment:* The result is a very comprehensive catalog of organizational and technical requirements for the operational environment of electronic elections. Examples are technical prerequisites like secure hardware, secure communication channels, secured rooms for server computers, and emergency precautions as well as organizational matters like secure registration of voters, monitoring of the voting system, and trustworthy personnel.
- V. *Design and Implementation Constraints:* client-side web interface should be (Google Chrome) browser dependent Since many processes are simultaneously working so the browser must support and enable JavaScript. Also, the server must ensure the safety and security of data and authentications of user logins and passwords.

The following assumptions are made about the hardware and software on the underlying running the software. The supported operating systems for this product are Windows and Linux. We also assume that the users have the Google Chrome browser installed. Server Machine needs to have the following software installed:

- I. Windows
- II. JDK
- III. MySQL DB Server
- IV. Apache Web Server

System Features: The following describes the functional requirements from the client's perspective and needs:

- I. **Database:** The Personal details of the user and candidate are stored in a database.
- II. **User:** The user does the registration on the system for voting, also user has personal details of their own login accounts. user can vote candidate and then the system keeps the details of the voter and candidate.

To Compute the hash value based on SHA-256 We compute the hash value based on SHA-256. By comparing the hash value to an expected hash value, the data's integrity can be determined. SHA-256 is frequently used in the e-voting scheme to compute the hash value, which is depicted in Fig. 2 and illustrated as follows:

- I. The message is denoted by m with binary expression.
- II. Pad m with 100...000 sequence and the length of m with 64-bit expression, i.e., $m = \text{pad}(m)$.
- III. m is broken into 512-bit chunks, i.e., $M(1), M(2), \dots, M(N)$.
- IV. 64 constants are used, which are denoted by W_0, W_1, \dots, W_{63} , respectively.
- V. Eight working variables labeled $A = 0x6A09E667, B = 0xBB67AE85, C = 0x3C6EF372, D = 0xA54FF53A, E = 0x510E527F, F = 0x9B05688C, G = 0x1F83D9AB$, and $H = 0x5BE0CD19$ are used as the initial hash value.
- VI. Compute the 64-cycle cryptographic iterative computation for the first chunk, i.e., $M(1)$. Repeat the iterative computation for the next chunk based on the result for the last chunk.
- VII. The result of the last iterative computation is the hash.

Mining and generation of voting blocks: All votes in the blockchain are cryptographically linked block by block. Many secure hash algorithms can be applied to solve the problem of condensing the message in the current block to produce a message digest, such as SHA-256 [10].

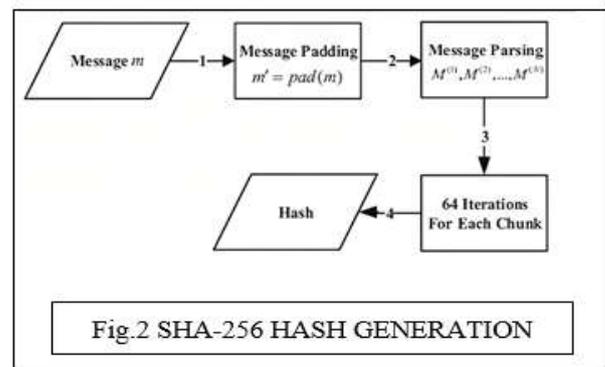


Fig.2 SHA-256 HASH GENERATION

A new block is generated by users from the P2P network. The new block generation is based on the PoW algorithm. When a new vote is submitted and verified, the miner generates a new block with the information of the vote and broadcasts the new blocks to the network. If new blocks have the same timestamp, the block with a higher value of signature is selected over others.

Security analysis—

A blockchain voting application can be analyzed from a security perspective in several ways. Firstly, the integrity of the blockchain must be ensured, meaning that the data stored in the blocks cannot be modified or deleted. This is achieved through cryptographic techniques such as hashing and digital signatures. Secondly, the consensus algorithm used to validate transactions must be secure and resistant to attacks, such as a 51% attack. Thirdly, the authentication and authorization of voters

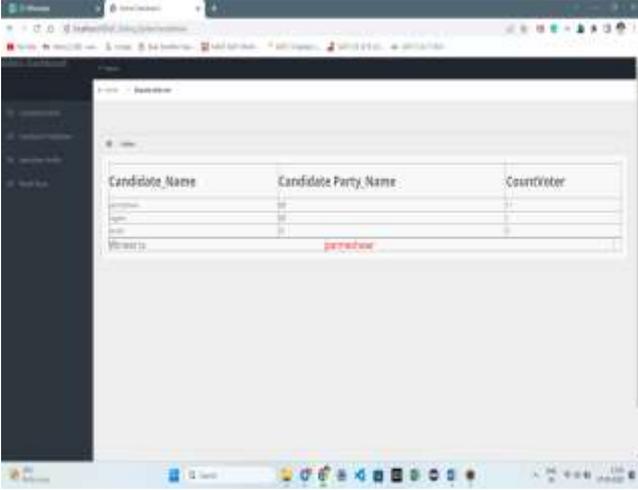
must be carefully implemented to prevent unauthorized access to the system. This can be achieved through various means such as biometric verification and digital identity verification. Additionally, the application must be protected against network attacks such as distributed denial-of-service (DDoS) attacks and man-in-the-middle attacks. Lastly, the privacy of the voters must be protected by ensuring that their identities and voting choices are kept anonymous and confidential. Overall, a thorough security analysis of a blockchain voting application is essential to ensure the reliability and credibility of the voting system.

- I. *DDoS*: To successfully DDoS a distributed system such as we have proposed, the attacker must DDoS every single boot node in the private network. The individual or institution would be immediately located if that would occur. Each node is implemented with a Byzantine fault tolerance algorithm, which helps to locate failed nodes in the system.
- II. *Authentication vulnerability*: Each individual is identified and authenticated by them without supervision, an individual could vote for multiple people, if the individual had knowledge of the PIN for each corresponding voting ID he has. To further address this vulnerability in the near future, a biometric scan could be introduced.
- III. *Sybil*: Sybil attack is known against centralized systems, where an individual creates a large number of

nodes in an attempt to disrupt network operation by hijacking or dropping messages. Since our proposal is running in a private network no individual has the access to create one. Even the consensus protocol that is used in our system is prone to Sybil attacks.

Results—

The use of blockchain technology in a voting application can bring several benefits, such as increased security, transparency, and integrity of the voting process. The results of a voting application using blockchain can be more trustworthy as the decentralized nature of the technology makes it difficult to manipulate or alter the recorded votes. Additionally, blockchain-based voting can increase participation and accessibility as it enables remote voting and eliminates the need for physical polling stations. However, there may be some challenges, such as ensuring that voters can cast their votes anonymously while maintaining the integrity of the system. In summary, the results of a voting application using blockchain technology can be more secure, transparent, and accessible, leading to increased trust and confidence in the electoral process.



Candidate Name	Candidate Party Name	Count/Voter
...
...
...
...
...

Fig.3 Announcement of the winner

PERFORMANCE EVALUATION—

Performance evaluation of a voting application using blockchain technology involves assessing the efficiency and reliability of the system during various stages of the voting process. Blockchain provides a secure and transparent platform for voting by creating a decentralized network that records every transaction in a distributed ledger. To evaluate the performance of such an application, factors such as transaction speed, scalability, security, and cost should be considered. Transaction speed is a critical factor as it determines the time it takes for the vote to be recorded in the ledger. Scalability is also important as the system should be able to handle a large number of transactions during peak voting periods. Security is a primary concern as the system must protect against hacking attempts and ensure the integrity of the voting process. Finally, cost is a critical factor as the system should be cost-effective while maintaining high levels of performance and security. Overall, performance evaluation of a voting application using blockchain technology should focus on providing a reliable and efficient platform for secure and transparent voting [8].

I. Time for pc VS keysize:

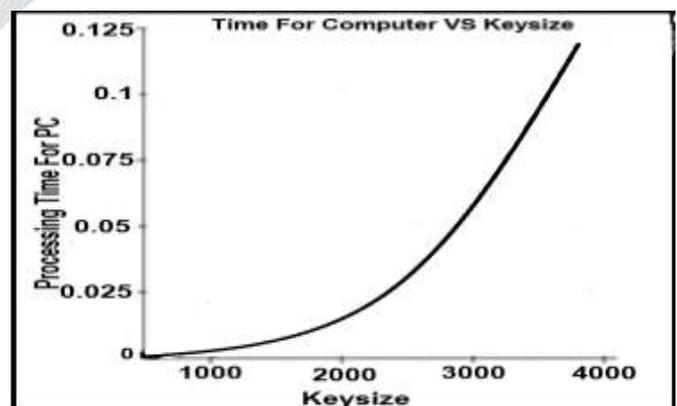


Fig.4 Time for computer VS Keysize

II. Time for smartphone VS keysize:

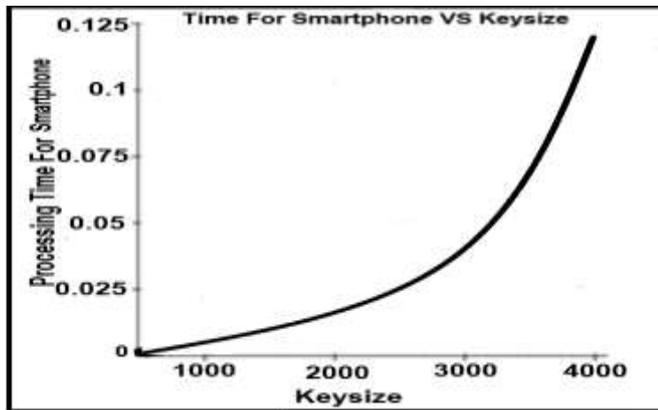


Fig.5 Time for Smartphone VS Keysize

From the above graph it is quite obvious that small key size helps the voting system to be faster and more efficient.

Conclusion—

An interoperable architecture would undoubtedly play a significant role throughout many voting use cases that face similar data sharing and communication challenges. From the more technical aspect, much research is needed to pinpoint the most practical design process in creating an interoperable ecosystem using the Blockchain technology while balancing critical security and confidentiality concerns in voting. Whether to create a decentralized application leveraging an existing Blockchain, additional research on secure and efficient software practice for applying the Blockchain technology in voting is also needed to educate software engineers and domain experts on the potential and also limitations of this new technology. Likewise, validation and testing approaches to gauge the efficacy of Blockchain-based voting architectures compared to existing systems are also important (e.g., via performance metrics related to time and cost of computations or assessment metrics related to its feasibility).

Future scope—

- I. Integration with existing voting systems: Blockchain-based voting applications can be integrated with existing voting systems to provide additional security and transparency. This integration can help increase voter confidence in the election process and provide more accurate results.

II. Adoption by governments and organizations:

Governments and organizations can adopt blockchain-based voting applications to conduct their elections, ensuring that the process is secure, transparent, and efficient. Implementation in developing countries: Blockchain-based voting applications can be implemented in developing countries where the traditional voting process is difficult to manage due to logistical challenges or political instability. This can help ensure that every citizen has access to fair and transparent elections.

References—

1. Gupta A, Patel J, Gupta M, Gupta H., (2017), *Issues and Effectiveness of Blockchain Technology on Digital Voting. International Journal of Engineering and Manufacturing Science, Vol. 7, No. 1*
2. Navya A., Roopini R., SaiNiranjan A. S. et. Al, *Electronic voting machine based on Blockchain technology and Aadhar verification, International Journal of Advance Research, Ideas and Innovations in Technology, (Volume 4, Issue 2)*
3. Hardwick, Freya Sheer, Raja Naeem Akram, and Konstantinos Markantonakis. "E-Voting with Blockchain: An E-Voting Protocol with
4. *Decentralisation and Voter Privacy.*" arXiv preprint arXiv:1805.10258 (2018).
5. Meter, Christian. "Design of Distributed Voting Systems." arXiv preprint arXiv:1702.02566 (2017)
5. Panja, Somnath, and Bimal Kumar Roy. "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain."
6. Martin A Makary and Michael Daniel. *Medical error-the third leading cause of death in the us. BMJ: British Medical Journal (Online), 353, 2016*
7. Paul Tak Shing Liu. *Medical record system using blockchain, big data and tokenization. In International Conference on Information and*

Communications Security, pages 254–261. Springer, 2016.

10. Securing e-voting based on blockchain in P2P networkHaiboYi <https://doi.org/10.1186/s13638-019-1473-6>

8. *d-Bame:Distributed Blockchain-Based Anonymous Mobile Electronic Voting Ehab Zaghloul, Tongtong Li, Senior Member, IEEE, and Jian Ren, Senior Member, IEEE*

1.

9. *Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth international*

