International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET22948

A Novel Vote Counting System Based on Secure Blockchain

Mansi Bajpai*[1], Atebar Haider[2], Dr. Alok Mishra[3], Dr. Yusuf Perwej[4], Dr. Neeta Rastogi[4]

[1*]Scholar B. Tech Final Year, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, Uttar Pradesh, India

[2]Assistant Professor, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, Uttar Pradesh, India

[3]Director, Ambalika Institute of Management and Technology, Lucknow, Uttar Pradesh, India

[4]Professor, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, Uttar Pradesh, India

Article Info
Volume 9, Issue 4
Page Number : 69-79

Publication Issue :
July-August-2022

Article History
Accepted : 01 July 2022
Published: 10 July 2022

ABSTRACT

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 methods. Voting, especially during elections, is a technique where participants do not trust one another since the system might be attacked not just by an outsider but also by participants themselves (voters and organizers). The traditional methods of voting systems find it challenging to maintain the characteristics of an ideal voting system since there is a chance of tampering with results and disturbing the process itself. As a result, the effectiveness of the voting system is increased by translating the characteristics of an ideal voting system into digital space. It greatly lowers the expense of the elections and the work of the inspectors. In this essay, we'll use the open-source Blockchain technology to suggest a new electronic voting system's architecture. New chances to create new kinds of digital services are being provided by Blockchain. Numerous elements of our life have been altered by Blockchain technology, including the ability to save digital transactions via the Internet, confirm their legitimacy, license them, and provide the greatest level of security and encryption. This system offers a distributed architecture for storing the data, which distributes the data among many servers. In addition to maintaining voter identity outside of the vote count, this technology makes the voting process transparent.

Keywords: Voting System, Blockchain, Trust, E-Voting, Security, e-government.

I. INTRODUCTION

People have the most freedom to make decisions and choose an effective leader in a democracy. Election results serve as the last say on that choice [1]. Voting for the candidates that have chosen to participate in the election is how it is done. According to the words of Abraham Lincoln, "of the people, by the people, for

the people," the candidate with the most votes will win the election and become the new leader. Voting, especially during elections, is a technique where participants do not trust one another since the system might be attacked not just by an outsider but also by participants themselves (voters and organizers). Because of the potential for tampering with results and disturbing the voting process, traditional voting methods [2] struggle to maintain the qualities of a perfect voting system. As a result, the effectiveness of the voting system is increased by translating the characteristics of an ideal voting system into digital space. It greatly lowers the expense of the elections and the work of the inspectors. The method of voting has been a subject that is constantly changing in this environment [3]. The main force behind this progress is the goal to make the system visible, verifiable, and secure. Given its importance, ongoing attempts have been undertaken to increase the voting system's overall effectiveness and robustness.

One of the cutting-edge technologies, Blockchain has solid cryptographic underpinnings that enable apps to take advantage of these capabilities to produce robust security solutions. In this application, block chain technology aids in preserving the security against cyber-attacks. Information security issues can be solved with the use of encryption methods [4]. Voting, and especially election-related voting, is a process where players lack faith in one another since both the system and its users (voters and organisers) are capable of attacking it [5]. We will try to showcase certain Blockchain-enabled electronic voting methodologies in this article, together with their findings and recommendations.

There are several nations that are attempting to implement electronic voting, but the issues of validity and proof among other things need to be given extremely careful thought by governments, technologists, and ultimately the general public. This research proposed a system built on an adaptive block chain that could identify the problems that arise during voting, would aid in choosing an appropriate hashing algorithm, is beneficial even in choosing modifications to the Blockchain [6], and would aid in safeguarding the content of block data. The Internet of Things (IoT), cryptocurrency, service supply chains, and other businesses all employ Blockchain technology. Blockchain contributes to enhancing the security of the ledger's transactions by preventing data from being altered, falsified, or corrupted by chain members. Transparency, fraud protection, and decentralisation are among other benefits of Blockchain technology [9].

II. RELATED WORK

This highlights and examines a number of papers relating to Blockchain-based electronic voting systems that have the potential to address the issues with security and privacy in electronic voting systems. David Shaum invented the first electronic voting system in the early 1980s. Voting was done using public key cryptography, which also protected voter anonymity. The Blind Signature Theorem was applied to ensure that there were no connections between voters and ballots [10]. Blockchain technology may be used to address the issues with digital voting, claims the research paper "Digital Voting with the use of Blockchain Technology" by Andrew Barnes, Christopher Brake, and Thomas Perry [11]. It provides a basic explanation of Blockchain technology, the distinction between e-voting and i-voting, and how a Blockchain network functions. The servers are set up and votes are transferred via DVDs in the existing voting method. In the study, a Blockchain-based solution is suggested for this problem. Both offline and online registration options are available for the user. According to Nir Kshetri [12], each voter is regarded as a wallet, and there can only be one transaction at a time between Wallets. Because the candidates are viewed as the wallet's recipient. Actually, the vote is the exchange of money between all of the candidates' or recipients' wallets. The technology utilised in this study is blockchain-enabled electronic voting, which

makes use of an encrypted key and user IDs that cannot be changed.

According to T. G. Rossler [13], using remote internet voting will improve voter convenience, boost voter trust, and boost voter turnout. The study found that electronic voting is the best advancement since it not only offers more voter convenience but also maintains security. In this method [14] developed by Sagarshah et al. & Kashif et al., block chain-based voting assures block chain implementation utilising distributed ledger technology, enabling the peer-to-peer network to detect the questionable nodes. A decentralised node for electronic or online voting is provided by Blockchain technology. Due to the benefits of end-to-end verification, distributed ledger technologies like Blockchain have recently been employed to create electronic voting systems [15]. Crowcroft [16] suggests practical hashing strategies to assure data safety, such as block construction and sealing. Blockchain algorithm with consensus-based technique is employed. The benefits include their own architecture and a superior hashing technique. In their proposal for e-voting, N. Aditya Sundar, M. V. Kishore, and Ch. Suresh [17] suggest employing RSA for voter registration and MD5 for voting. MD5, however, is less effective than SHA-256. As a result, we suggest using the SHA-256 technique to encrypt the votes in this project. A member of the SHA-1 family is SHA-256 [18]. For the numerous requirements for an e-voting system, Kang at. el. suggests a solution utilising a Blockchain [19]. Because the voter's voting result is not stored in the Blockchain during the implementation of this electronic voting system, the actual voter cannot verify that his or her vote was properly reflected in the results. Instead, an encrypted voting result is sent to the calculator by using a uniform password. A brand-new technology dubbed the Blockchain-based electronic voting system has been introduced by Cosmas at. el. [20]. To present the new system, they offer a method that combines Blockchain technology with double envelope encryption. The three parts of the developed system are the voter's side, the electoral commissions, and the BC network. A unique key is generated by Ha at. el. based on voter biometric authentication and utilised for signatures. The encryption key is probably revealed if the voter's biometric data is made public [21]. Transactions are sent to each candidate's address using a different address during the voting process.

Zhang [22] suggests a local voting system based on the blockchain to aid in decision-making for the networks of its peers. It safeguards privacy and makes cheating detection and repair possible. Blockchain algorithm with distributed consensus is the approach employed. Elections may be utilised as a Blockchain component of Smart Contracts, Peer to Peer networks, Consensus, and Two Phase Validation, which is a benefit (decryption pvt key, smart contract verification). A Blockchain as a Service is presented by Fririk at. el. [23] to construct a new e-voting system. Smart contracts are used in the proposed service to provide complete authenticity for both the voters and the election itself. In order to prevent compelled voting and increase security, the authors have also built up the BC utilising Go-Ethereum permissioned Proof-of-Authority (POA) as a private network. Estonia was the first nation to allow voters to cast ballots using just an electronic national identity card and the Internet. The voting ID card was created with an integrated circuit, a Java chip platform, and a 2048 bit PIN for security [24].

III. BLOCKCHAIN

A Blockchain is similar to a data structure that stores and distributes all of the transactions that have been carried out since its inception. It functions primarily as a distributed decentralised database that keeps an exhaustive list of continuously accumulating and expanding data records protected against illegal manipulation, tampering, and alteration. A peer-to-peer payment system that enables monetary transactions across the Internet without depending on trust or the requirement of a financial institution was initially proposed by Satoshi Nakamoto (a pseudonym)

[25]. A system with a high byzantine failure tolerance, such as Blockchain, is safe by nature [27]. In order to develop a money that could be transferred via the Internet and rely only on cryptography to safeguard the transactions, Bitcoin is regarded as the first implementation of the Blockchain idea. Blocks of transactions are organised into a data structure called a Blockchain. Each block in the chain is connected to the one before it. The foundation of the stack is the initial block in the chain. A Blockchain is a stack of newly produced blocks that are added one on top of the other [28]. A hash that is written on the header identifies each block in the stack. The Secure Hash Algorithm (SHA-256) is used to provide a fixed-size, 256-bit hash that is essentially distinctive. The National Security Agency (NSA) created the widely used algorithm in 2001 and utilised it as the protocol to protect all federal communications [29]. Any amount of plaintext may be entered into the SHA-256 algorithm, and it will encrypt it to a 256-bit binary value. The SHA-256 function is a one-way operation that always yields a 256-bit binary result. The fundamental reasoning behind SHA-256 encryption is depicted in figure 1.

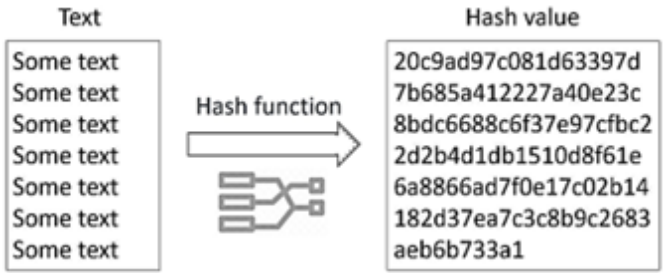

Figure 1. The Function of the SHA-256 Hash

Each header provides data that connects a block to its preceding block in the chain, forming a chain that is connected to the foundation, the very first block ever generated. Each block's encrypted hash found in its header serves as its principal identification. A digital fingerprint that was formed by merging two different types of data, first the data about the newly created block and then the second preceding block in the chain. A block is submitted to the Blockchain as soon as it is created. When new blocks are received, the system will monitor them and update the chain accordingly. So, because to its solid cryptographic underpinnings [30], Blockchain has been utilised more and more to prevent fraudulent transactions across [31] many domains. The numerous issues that were raised in these early attempts at online voting may all be resolved by Blockchain. The security of an Internet connection is unimportant to a Blockchain-based voting application since any hacker who gains access to the terminal will be unable to influence other nodes. Voters can cast their ballots successfully without disclosing their identities or political affiliations to the general public. Because each ID can be linked to one vote, no fakes can be made, and tampering is impossible, officials may tally ballots with complete confidence.

IV. CURRENT ISSUE

Voting, especially during elections, is a technique where participants do not trust one another since the system might be attacked not just by an outsider but also by participants themselves (voters and organizers). Voter and election data are extremely important for [32] a democratic country. Secure digital identity management is one of the most pressing technological issues now facing e-voting systems, but it is not the only one. Before the elections, every prospective citizen should register with the voting process. Their information must be in a format that can be processed digitally. In addition, any information that involves them should keep their identification information private.

V. PURPOSE

Our purpose is to use Blockchain technology to address the problems associated with electronic voting. E-voting with Blockchain support might enhance voter access and decrease voter fraud [33]. The voting process need to be impenetrable. No group with a desire for power should be allowed to influence and rig

elections. When the most crucial conditions are met using a Blockchain, [4] only registered voters will be permitted to cast ballots. The mechanism forbids any communication between the voters' identities and the votes they cast. Once cast, votes are irrevocably recorded and cannot, under any scenario, be altered or edited. Voting procedures should be transparent. The auditor should be able to see the voting process in the event that there is an audit of the election. Voters shouldn't attempt to rig the system by casting multiple ballots or by changing their votes.

VI. NECESSITY

In this part, we give a concise explanation of the need and how the suggested system satisfies it. To protect a voter's privacy, the system makes use of Blockchain cryptographic features. More specifically, as soon as a voter registers with the system, Blockchain generates a voter hash, which serves as the voter's unique identification inside the Blockchain [34] and is safeguarded against misuse thanks to the collision resistance quality of the cryptographic hash. Because of this, a vote's traceability is likewise non-trivial, safeguarding the voter from coercion. All eligible users must register using distinctive identifiers, such as official papers, to demonstrate their status.

Additionally, our system uses finger printing technology to provide a robust authentication mechanism that guarantees that only approved voters [35] may access the system. Additionally, the system can prevent multiple voting thanks to the usage of biometrics. The suggested method allows voters to cast their ballots in the manner they like and generates a cryptographic hash for each such occurrence (transaction). This is necessary to establish verifiability, or to determine whether a particular vote was counted. Nevertheless, having this hash does not allow for the extraction of voting-related data. The system's voting procedure requires little user input because to the system's user-friendly web-based interface. For example, fingerprinting is used as an authentication method to eliminate the need to memorise usernames and passwords. Additionally, the workflow as a whole is integrated, allowing for smooth user interaction. A user is given their specific transaction ID in the form of a cryptographic hash after properly casting their vote. This transaction ID can be used by a user to determine whether their vote was counted. However, this procedure, which was established to lessen threats while acting under pressure, does not allow a user to observe how they voted. As a result, we think the research provided here significantly adds to what is already known about using Blockchain technology to create a safe digital voting system.

VII. PREREQUISITE

A voting application has been supported by the system in the real-world setting while taking into consideration certain needs like privacy, eligibility, convenience, receipt-freeness, and verifiability. With the suggested approach, safe digital voting is achieved without sacrificing usability.

7.1. Hashing

The usage of hash functions ensures the security of the Blockchain. With the use of hashing, one may apply a hash function to the data that computes a comparatively unique result for data of practically any size. As long as the data hasn't changed, hashing can enable users to independently receive input data, hash it, and generate the same outputs. Cryptographic hash functions come in a variety of forms, including SHA-0, SHA-1, SHA-2, SHA-3, BLAKE-2, etc. According to a research, SHA-1 is the quickest, taking 708.3 ms for short sequences and 909.3 ms for lengthy sequences, outpacing MD-5, SHA-256, and SHA-512 [36]. Since the SHA-1 lightweight hash function is vulnerable to attacks, SHA-256 can take its place in the information exchange process. Because of SHA-256's strong anti-collision properties, voting systems are immutable and less vulnerable to assaults. The National Security Agency developed SHA-2 (Secure Hash Algorithm 2)

in 2001 as a replacement for SHA-1. The SHA-256 algorithm is one variant of SHA-2. A 256-bit value is produced using the patented cryptographic hash algorithm SHA-256. Data is changed into a safe format during encryption so that it cannot be read unless the receiver possesses a key. The data may be as big as you like when it's encrypted, and it's frequently the same size as unencrypted data. In contrast, data of any size may be translated to data of a certain size via hashing [38]. For instance, SHA-256 hashing would reduce a 512-bit string of data to a 256-bit string. One of the most secure hashing algorithms available is SHA-256. The US government mandates that its agencies use SHA-256 to secure specific sensitive data. Even though the precise mechanics of SHA-256 remain classified, we do know that it is constructed using a Merkle-Damgard structure that was itself generated using the Davies-Meyer structure from a specialised block cypher.

7.2. Eclipse

Java is used to develop the Eclipse IDE. It primarily comprises of a base "Workspace" and a plug-in system so that we may expand the capability of the IDE by adding new features to it through plugins. Eclipse is compatible with all of the main operating systems, including Windows, Mac OS, Linux, etc. It offers strong capabilities that may be utilised to create whole projects. Almost all of Eclipse's features are plugins. By adding plugins to the IDE, we may increase the capabilities of Eclipse and use it for new programming languages, version control systems, or UML. supports a variety of source knowledge features, including code editing with syntax highlighting, grading, a macro definition browser, and folding and hyperlink navigation. good visual code debugging tools are available. Eclipse features a fantastic user interface with drag-and-drop UI design capabilities. supports source navigation, the traditional make framework, and the administration of many tool chains for project development.

7.3. MYSQL

It's important to comprehend the database before you can understand MySQL. Software that stores an organized collection of records is known as a database. The user will have no trouble using it or managing it. Because data is arranged into tables, rows, columns, and indexes, we can quickly retrieve crucial information [39]. MySQL has a strong data security layer that shields private information from outsiders. Additionally, MySQL encrypts passwords. Because MySQL enables multi-threading, scaling is simple. It can manage practically any volume of data, up to 50 million rows or more. A 4 GB maximum file size is the standard. The maximum amount of data we could theoretically store would be 8 TB. According to several benchmark tests, MySQL is one of the most fast database languages.

7.4. Apache Tomcat

Tomcat's full name is "Apache Tomcat." It was created in a collaborative, open environment and made its debut in 1998. The Java Servlet API and the first Java-Server Pages used it as their reference implementation at first. Even though it is no longer the recommended implementation for either of these technologies, people still see it as their top option. Sun Microsystems developed Tomcat before giving the code base to the Apache Software Foundation. Nowadays, a lot of businesses utilise Apache Tomcat since it implements a lot of the Java EE specs. It may be downloaded, installed, and used without charge by anybody, anywhere, making it the top option among new users and developers. Due to its wide customization possibilities, lightweight design, and great flexibility, a user may operate it in any way they like and it will function flawlessly.

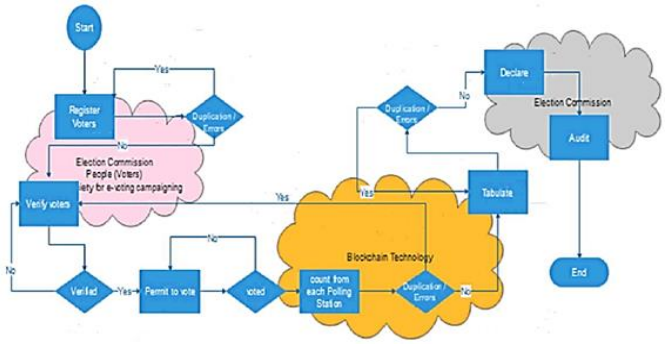

Figure 2 The Student Data Flow Diagram

VIII. PROPOSED SYSTEM

Three parts make up the project: users, the electoral commission, and Blockchain technology. Members of the election commission will register candidates for office, users or voters, and monitor the outcome. Voters would be permitted to change their password and log in to cast their votes once they had been confirmed by EC members. The voter can view the candidates in his or her state and district before casting a ballot. The Blockchain [40] seen in figure 2 will encrypt and store these votes. SHA-256 is the algorithm used to encrypt the votes. Voters cannot amend their vote or log out after casting their ballot. The flow of all transactions is logged in the database, so if any network user tries to tamper with it, it would be quite obvious. Any modifications to earlier transactions result in a new hash code, which alerts the auditor to any attempts to tamper with the database [41].

For access to the application depicted in figure 3, this module must first verify voters and Election Commission members [42]. The Election Commission members can use this module to register candidates and voters and view the results displayed in Figure 4.

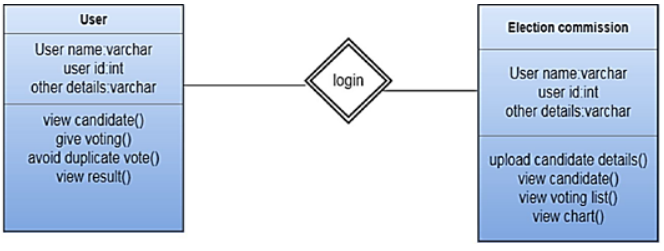

Figure 3 The Network module

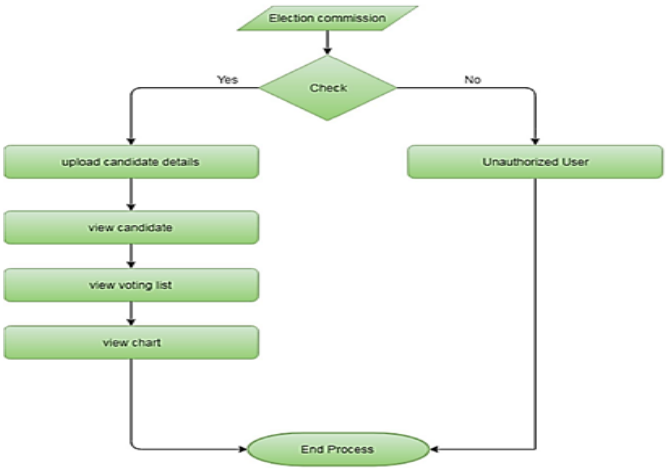

Figure 4 The Flow Diagram for Election Commission Member

An authenticated voter may login, view the candidates for whom he may cast a ballot, and do so just once. This module assists in tallying the votes cast for a candidate and displays them as the different graphs in figure 5.

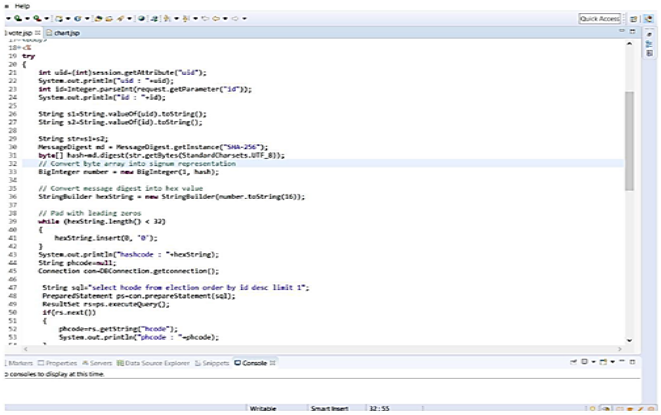

Figure 5 The SHA-256 Code

IX. FINDINGS AND EVALUATION

Members of the election commission can register the candidates running in the election depicted in figure 6 after logging in. The electoral commission members have the ability to verify and register voters. It is possible to obtain a list of every candidate running for office. After the vote is cast, the election commission can use a variety of graphs to view the results and declare a winner. If the voter tries to vote again or changes his vote, he will not be allowed to logon again. In the scenario depicted in figure 7, a pop-up would appear.

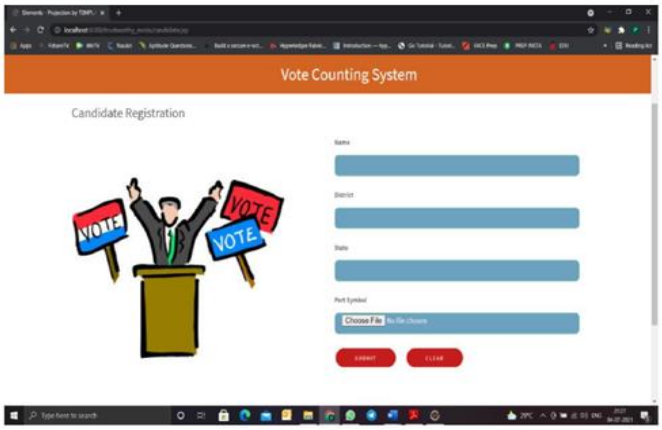

Figure 6 The Candidate Registration

Figure 7 The Voter Cannot Login Again

Once the elections are over, that is, when all of the voters have cast their ballots as illustrated in figure 8, the encrypted votes saved in the Blockchain network will be utilised to reveal the results. Various graphs would be used to present the results. With the use of these graphs in figure 9, the election commission members may announce the results.

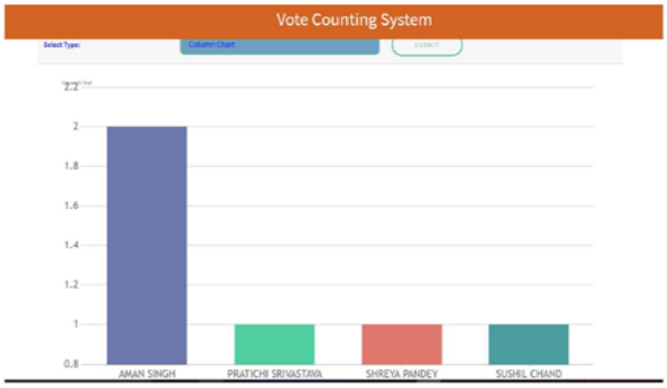

Figure 8 The Graphs for Results

X. CHALLENGES

Blockchain technology can be used to address several concerns with electronic voting, making it more convenient and cost-effective. The electronic voting systems based on Blockchain face major technological difficulties. Blockchain functions well for a limited set of users. However, as the network is used for widespread elections, the user base grows, increasing the cost and time required to process the transaction. Pseudonyms are used by Blockchain as usernames. This tactic does not guarantee total secrecy and privacy. The user's identity may be ascertained by looking through and analysing the transactions because they are open to the public [43]. While accuracy and security are two areas where Blockchain shines, people's confidence and trust are crucial for effective Blockchain electronic voting. The complexity of Blockchain may make it challenging for people to embrace Blockchain-based electronic voting, and it may eventually prove to be a substantial barrier to adoption for the general populace.

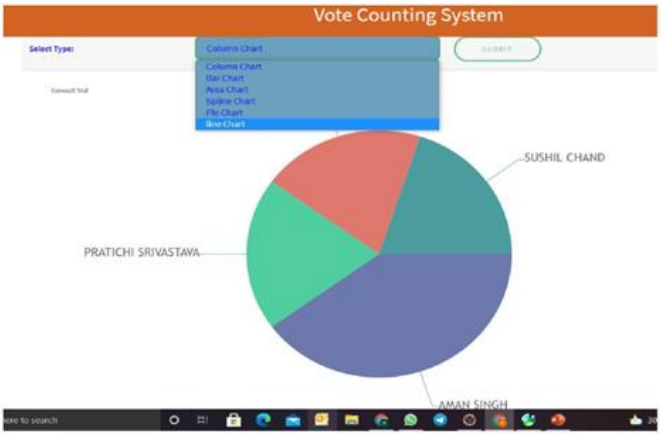

Figure 9 The Different kinds of graphs available

XI. CONCLUSION

Any democracy must have an open voting process that satisfies the demands of the populace in order to give the appropriate individual the authority. Additionally, there are several problems with the current traditional voting systems, including a lack of security and transparency. A Blockchain-based electronic voting

system that we have created involves the encryption and verification of vote results. The Blockchain links each vote cryptographically, block by block. The suggested approach is effective in ensuring security for the votes that have the power to alter a person's whole life. The suggested approach protects the voter's anonymity by using block chains and hashing techniques. The foundation of Blockchain technology is comprised of hashing algorithms since hash functions are essential to its security and dependability. If the input data hasn't changed, hashing can enable users to independently receive input data, hash it, and generate the same outputs. The output size, file size, execution time, and algorithmic speed may all be used to study hashing algorithms. With the aid of the analysis, one may choose the kind of hashing method to use. Vote counting is completed significantly faster and with far more security than with traditional technologies. The suggested solution would make the voting process visible, verifiable, untraceable, unusable, and impossible to interfere with. E-voting would encourage more people to participate in elections throughout the world. The system would become trustworthy and fraud-resistant through the usage of Blockchain and hashing technology.

XII. THE FUTURE OF WORK

The traceability component may be taken out of this application to make it better. The project's performance and efficiency can be improved by transferring it to hyper ledger fabric. The project can be executed on a big scale, such as the national voting system. Blockchain defences against quantum computer assaults are thus a potential field of study in the future.

XIII. REFERENCES

[1]. Patrick McCorry, Siamak F. Shahandashti and Feng Hao, A Smart Contract for Boardroom Voting with Maximum Voter Privacy, 2017

[2]. Wolchok et al., "Security Analysis of India's Electronic Voting Machines", Proceedings of the 17th ACM Conference on Computer and Communications Security CCS 2010, October 4-8, 2010

[3]. Spyros Ikonomopoulos, Costas Lambrinoudakis, Dimitris Gritzalis, Spyros Kokolakis and Kostas Vassiliou, "Functional Requirements for a Secure Electronic Voting System", IFIP Advances in Information and Communication Technology, pp. 507-520, 2002

[4]. Yusuf Perwej, "A Pervasive Review of Blockchain Technology and Its Potential Applications", Open Science Journal of Electrical and Electronic Engineering (OSJEEE), New York, USA, Volume 5, No. 4, Pages 30 - 43, 2018

[5]. Tadayoshi Kohno, Adam Stubblefield, Aviel D Rubin and Dan S Wallach, "Analysis of an electronic voting system", Security and Privacy 2004. Proceedings. 2004 IEEE Symposium on, pp. 27-40, 2004

[6]. S. A. Adeshina and A. Ojo, "Maintaining Voting Integrity using Blockchain", 2019 15th International Conference on Electronics, pp. 1-5, 2019

[7]. Yusuf Perwej, Firoj Parwej, M. Mi. Mohamed Hassan, Nikhat Akhtar, "The Internet-of-Things (IoT) Security: A Technological Perspective and Review" , International Journal of Scientific Research in Computer Science Engineering and Information Technology, Volume 5, Issue 1, Pages 462-482, 2019, DOI: 10.32628/CSEIT195193

[8]. Prof. Kameswara Rao Poranki, Yusuf Perwej, Nikhat Akhtar, "Integration of SCM and ERP for Competitive Advantage", TIJ's Research Journal of Science & IT Management – RJSITM, International Journal's-Research Journal of Science & IT Management of Singapore, Volume 04, Number 05, Pages 17-24, 2015

[9]. F. Casino, T. K. Dasaklis and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status classification and open issues", Telematics and Informatics, vol. 36, pp. 55-81, Mar. 2019

[10]. D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communication of the ACM. Vol. 24(2). pp. 84-90, 1981

[11]. Barnes Andrew, Christopher Brake and Thomas Perry, "Digital Voting with the use of Blockchain Technology", Team Plymouth Pioneers Plymouth University.

[12]. Blockchain-Enabled E-Voting Nir Kshetri and Jeffrey Voas https://ieeexplore.ieee.org/document/8405627

[13]. Rossler T.G, "E-voting: A survey and Introduction", Available at http://wiki.agoraciudadana.org/images/5/56/Anoduction%2Bto%2BElectronic%2BVoting%2BSchemes.pdf, Retrieved on 15th June 2022.

[14]. Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan, "Secure Digital Voting System based on Blockchain Technology"

[15]. Ometov, A.; Bardinova, Y.; Afanasyeva, A.; Masek, P.; Zhidanov, K.; Vanurin, S.; Sayfullin, M.; Shubina, V.; Komarov, M.; Bezzateev, S. An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends. IEEE Access, 8, 2020

[16]. Trustworthy Electronic Voting Using Adjusted Blockchain Technology, BASIT SHAHZAD AND JON CROWCROFT https://ieeexplore.ieee.org/document/8651451

[17]. N. Aditya Sundar, M.V. Kishore, Ch. Suresh, "A Secure E-Voting System Using RSA and Md5 Algorithms Using Random Number Generators", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 11, pp 9468-9473, 2018

[18]. Yusuf Perwej, Kashiful Haq, Uruj Jaleel, Firoj Perwej, "Block Ciphering in KSA, A Major Breakthrough in Cryptography Analysis in Wireless Networks", International Transactions in Mathematical Sciences and Computer, India, ISSN-0974-5068, Volume 2, No. 2, Pages 369-385, 2009

[19]. Kang Hee-jung. Designing and Implementing a Reliable Blockchain Based E-voting System, Sunghin Women's University Graduate School, Diploma (Master), Sungshin Women's Uni. Graduate School: Computer Science, 2019

[20]. Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato." A Proposal of Blockchain-based Electronic Voting System". Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2018

[21]. Ha Hyun-soo, Lee Seo-joon, Jung Gu-ik, Shin Yong-gu, Kim Myung-ho, Kim Young-jong. Anonymous E-voting Blockchain Platform Model Based on Public Blockchain, Korea Information Science Association, A collection of papers published by the Korea Information Science Association, 12(2): 1176-1178, 2017

[22]. A Blockchain-Based Network Security Mechanism for Voting Systems Hsin-Te Wu Department of Computer Science and Information Engineering, National Penghu University of Science and Technology

[23]. Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson,"Blockchain-Based E-Voting System", In the 11th International Conference on Cloud Computing IEEE, 2018

[24]. Trueb Baltic, "Estonian Electronic ID – Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application." http://www.id.ee/public/TBSPEC-EstEID-Chip-App-v3_5-20140327.pdf

[25]. National Institute of Standards and Technology, "Federal Information Processing Standards Publication", 2012

[26]. S. Nakamoto, "A Peer-to-Peer Electronic Cash System", 2008

[27]. F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System", Security and Privacy in Social Networks. pp. 1-27, 2013

[28]. Yusuf Perwej, Nikhat Akhtar, Firoj Parwej, "A Technological Perspective of Blockchain Security", International Journal of Recent Scientific Research (IJRSR), Volume 9, Issue 11, (A), Pages 29472 – 29493, 2018. DOI: 10.24327/ijrsr.2018.0911.2869

[29]. S. Raval, "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology." O'Reilly Media, Inc. Sebastopol, California, 2016

[30]. Yusuf Perwej, Prof. (Dr.) Syed Qamar Abbas, Jai Pratap Dixit, Dr. Nikhat Akhtar, Anurag Kumar Jaiswal, "A Systematic Literature Review on the Cyber Security", International Journal of Scientific Research and Management (IJSRM), Volume 9, Issue 12, Pages 669 - 710, 2021, DOI: 10.18535/ijsrm/v9i12.ec04

[31]. Asif Perwej, Dr. Kashiful Haq, Yusuf Perwej, "Blockchain and its Influence on Market", International Journal of Computer Science Trends and Technology (IJCST),ISSN 2347 – 8578, Volume 7, Issue 5, Pages 82- 91, 2019, DOI: 10.33144/23478578/IJCST-V7I5P10

[32]. L. C. Schaupp and L. Carter, "E-voting: from apathy to adoption", Journal of Enterprise Information Management, vol. 18, no. 5, pp. 586-601, 2005

[33]. T. P. Abayomi-Zannu, I. A. Odun-Ayo and T. F. Barka, "A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication", IEEE International Conference on Engineering for Sustainable World, 2019

[34]. A. Judmayer, N. Stifter, K. Krombholz and E. Weippl, "Blocks and Chains: Introduction to Bitcoin", Cryptocurrencies and Their Consensus Mechanisms, pp. 1-123, 2017

[35]. R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design", 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1-6, 2017

[36]. Fu Jinhua, et al, A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA, Wiley, p. 1., 2020

[37]. H. Mestiri, F. Kahri, B. Bouallegue and M. Machhout, "Efficient FPGA Hardware Implementation of Secure Hash Function SHA-2", IJCNIS, vol. 7, no. 1, pp. 9-15, 2015

[38]. Yusuf Perwej, "The Ambient Scrutinize of Scheduling Algorithms in Big Data Territory", International Journal of Advanced Research (IJAR), ISSN 2320-5407, Volume 6, Issue 3, Pages 241-258, 2018, DOI: 10.21474/IJAR01/6672

[39]. H G Molina, J D Ullman and J. Widom, DATABASE SYSTEMS The Complete Book 2 nd Edition, Pearson Education Inc, 2009

[40]. A. Barnes, C. Brake and T. Perry, Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers - Plymouth University, 2016

[41]. M. R. Clarkson, S. Chong and A. C. Myers, "Civitas: Toward a secure voting system", 2008 IEEE Symposium on Security and Privacy (sp 2008), pp. 354-368, May 2008

[42]. David Evans and Nathanael Paul, "Election security: Perception and reality", IEEE Security & Privacy, vol. 2(1), pp. 24-31, Jan. 2004

[43]. Wang, Y.; Gou, G.; Liu, C.; Cui, M.; Li, Z.; Xiong, G. Survey of security supervision on Blockchain from the perspective of technology. J. Inf. Secur. Appl., 60, 102859, 2021

Cite this Article

Mansi Bajpai, Atebar Haider, Dr. Alok Mishra, Dr. Yusuf Perwej, Dr. Neeta Rastogi, "A Novel Vote Counting System Based on Secure Blockchain", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 4, pp. 69-79, July-August 2022. Available at doi : https://doi.org/10.32628/IJSRSET22948
Journal URL : https://ijsrset.com/IJSRSET22948