

Reliable Electronic Voting using Blockchain Technology



Sophia.B, Aishwarya.S, Hariprasath.B.R, Diwakar.S.S

Abstract: Voting is the principal incident in any democratic country. Generally voting is done using ballots system, but this technique is ancient and can be easily sabotaged. There is a necessity to bring in new technologies to ensure effective implementation of digital voting systems. The security of digital voting is a significant aspect for implementation and must meet the requirements to be appropriate for trust worthiness. Block chain technology provides reliable electronic voting system that can be secured by adding more decision so that the possible attacks can be avoided. Block chain technology based on crypto currency implements diffused database architecture with transaction records secured by transactions.

Keywords: Reliable voting, Block chain for voting, Digital voting, Secure Hashing.

I. INTRODUCTION

Block chain technology is prominently being used in scenarios that require flexible and trustworthy options. Voting by digital means require security and that can be ensured by using the hashing techniques relevant to block chain. The aim is to use a hashing algorithm that is implemented namely MD5, which is one of the secure hashing algorithms. There are many more cryptographic algorithms that can be chosen from however MD5 is the suitable for the implementation of such solution. Block chain is a digital technology primarily used for crypto currency system - a digital system exclusively dealt in commerce and industries. Crypto currency is paperless and maintained online to enable purchase or sell or both any asset and transact any business deal. Digital signature of the dealing business man is the authority to safeguard the transactions executed and shared. The database in block chain is connected with the nodes of all transactions.

Block chain does not have any centralized separate server for

the storage of data but has the facility for validation and verification of the data.

The Block chain technology is attributed with some distinctive features that makes it a promising technique to ensure trusted and distributed solution for implementing digital voting systems. These features enable us to use block chain as a suitable and secured system for reliable digital voting.

- **Decentralized and Consensus-based:** Block chain is connected with nodes that will receive every transaction and the distribution register of the block chain is updating and sharing each transaction. Every transaction is valid and it is done using consensus algorithms and the related network participants will know that well.

- **Secured:** As the data in block chain is shared among all the participants the system cannot be misused or abused and there is no concern for cyber issues. Block chain, through its cryptographic technology and permission methodology provide secured access to authorized participants only.

- **Reduced Time and Cost:** As the data collected in block chain is transparent there is no need for third party verification and time is saved in processing. : Block chain technology is not only latest but also cost effective as it stores data with reliability and there is no need for data verification by third parties.

- **Transparent and Flexible:** Every node in block chain has a copy of the Block chain data and so they have access to all transaction data.. Block chain provides platform for model contracts signed on certain special conditions.

II. LITERATURE SURVEY

The system of blockchain is indeed a blessing for balloting and the perfect electoral system as it provides the data as it is and ensures credibility and durability. Previous systems of digital vote casting is indeed a burden in the long run as the database is to be saved in servers which becomes very difficult to maintain.[3].

At present, more experimentation is done in many countries with digital vote casting despite having a lot of practical difficulties. Hence, Blockchain technology will become inevitable in future as it is built with the design of storing the election data directly, of better transparency and of simplified electoral process. The technical feature such as cryptographic hash in the blockchain architecture ensures the layout of block chain to prevent tampering of votes and assuring immutability of data [6].

Blockchain technology was originally followed in the sphere of cryptocurrencies for transactional purposes. On seeing the advantage of this technology steps are now being

Revised Manuscript Received on April 25, 2020.

* Correspondence Author

Mrs.Sophia.B*, M.E., Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology Coimbatore, India. Email: sophiab@skcet.ac.in

Ms.Aishwarya.S, B.E., Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology Coimbatore, India. Email: 16eucs009@skcet.ac.in

Mr.Hariprasath.B. R.B.E., Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology Coimbatore, India. Email: 16eucs05@skcet.ac.in

Mr.Diwakar.SS, B.E., Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology Coimbatore, India. Email: 16eucs046@skcet.ac.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](http://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

Reliable Electronic Voting using Blockchain Technology

taken in the election system for greater transparency and reliability.[8]Blockchain technology will be a solution for a tamperproof balloting and more reliable outcomes.

The voters' trust on franchising is increased and enhances the comfortability of casting votes through online from his/her place. The blockchain technology thus will bring Free and fair election which will be a good sign of healthy democracy. It is hoped that it may take a few years to experiment this system in the Indian context.[10]

Blockchain will be serving as an effective digital tool to store data and to carry out any transaction. Used in the crypto currency / bitcoin in the beginning, this blockchain technology was experimented with public elections as a proven device to rely with in the future through its well designed and developed software [11]. Blockchain aims at avoiding proxy votes, safeguarding accuracy in polling, disseminating the message of safety and security in polling and storing the cast votes and paving the way for comfortability in exercising the votes online.

Conventional elections have a lot of issues to face in its conduction. Proxy polling, Identity of voters, law and order maintenance, time killing counting system and safe storing of machines for long period are some of the problems the existing election system is facing. Block chain technology is proving an efficient antidote to the existing weak system. Foolproof data security, voters' comfort ability in casting votes, no necessity of creating force and other logistics for law and order in elections, voters privacy, quick results delivery are some of the advantages of the block chain platform[9].

III. PROBLEM DEFINITION

3.1 EXISTING SYSTEM

• Plenty of electronic and non electronic voting methods are currently adopted in various countries of the world. There are more challenges and difficulties these systems face to follow and conduct elections to get the desired results and implement in a practical scale.

• Online election system was first conducted in Estonia during elections 2005 and 2007 through online voting. ID cards were provided to the citizens to identify the voters and all other details were recorded in these cards including government database records, banking details and other digital documents.

3.2 DISADVANTAGES OF EXISTING SYSTEM

- Security of these systems can be compromised and the hackers can hack the servers through malware
- There are possibilities of Election tampering
- Diminished efficiency and accuracy
- Centralized control by a single organization

IV. DESIGN OF PROPOSED SYSTEM

4.1 PROPOSED SYSTEM

- Reliable Voting through Blockchain Technology.
- A Blockchain provides a decentralized method to keep track of creation and changes in the documents in the form of blockchain. The votes can be recorded as transactions and a blockchain can be created and effectively implemented with blocks and can be kept track by major groups involved and

any change or modification can be easily found by the hash values.

- A transparent and consensus –based method can be used to count the votes and the system ensures no illegitimate votes can be added votes cannot be changed or removed. All nodes will have a copy of the block chain and ensures traceability.

4.2 ADVANTAGES OF PROPOSED SYSTEM

- The proposed system ensures trustworthiness and augmented security using transactions.
- Refined traceability
- The cost and time savings results in increased efficiency and speed

4.3 MODULE DESCRIPTION

4.3.1 CREATE ELECTION SYSTEM

- The System consists of Candidate registration, Admin Login which will be handled by Election Commission and a candidate login which will be handled by Candidate.
- Admin create an election and mention the candidates also admin verify User id.

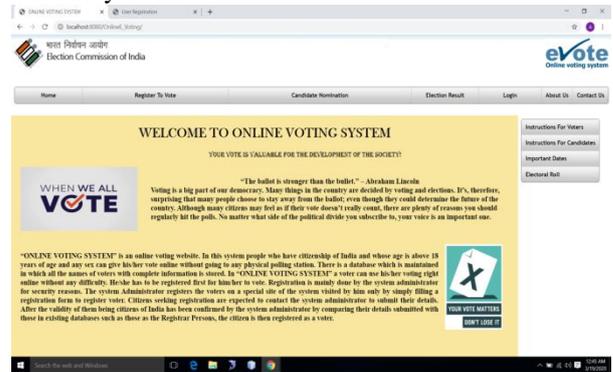


Fig 4.3.1.1

4.3.2 USER LOGIN AND GIVE VOTE

- Voters login with correct username and password
- Voter choose candidate in the election system

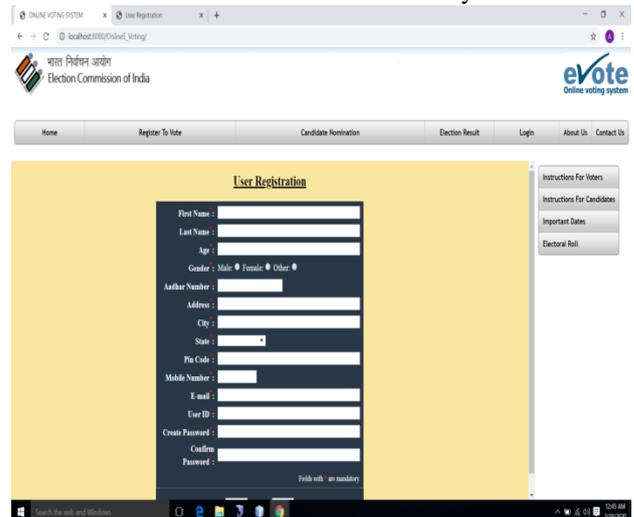


Fig 4.3.2.1

4.3.3 CREATE A BLOCK CHAIN

Design the Blocks for the Block chain. Basically, a block contains the following information :

- Timestamp is used to store the time records in the block
- Hash of the previous Block
- Vote stored in the Block.
- Hash of the present block is ensured for the integrity of its content.

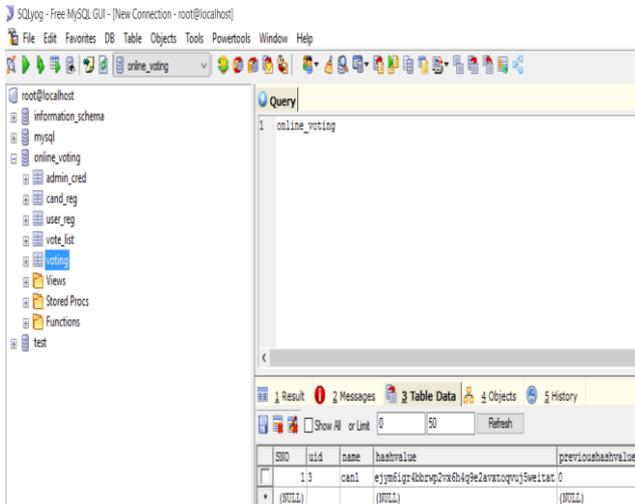


Fig 4.3.3.1

4.3.4 CHECKING THE RESULTS

Since, all the data will be converted into hash values, the results can be viewed only by the admin, to avoid tampering and casting of fake votes.

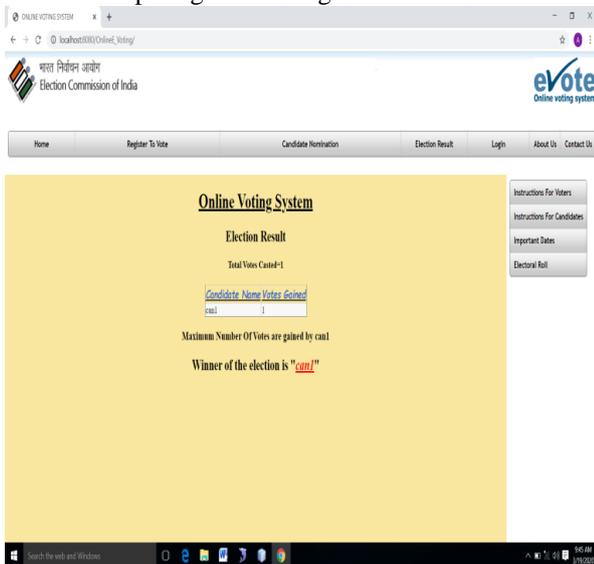


Fig 4.3.4.1

V. METHODOLOGY

5.1 HASH FUNCTION IMPLEMENTATION

Hashing technique follows the sequence of steps to be implemented. First it gets an input string of any length. The output of a hashing algorithm is of fixed length. The hash value is unique and the block chain dealing in bitcoin or crypto requires this algorithm based hash. A hash function encrypts the input to a hash value of a fixed length output.

INPUT	HASH
Hi	639EFCDo8ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCA43326B8
Welcome	33A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Fig 5.1.1

5.2 CRYPTOGRAPHIC HASH FUNCTIONS

Cryptographic hash functions helps to create secure hash values with any form of mathematical computation which must ensure to satisfy that has a variety of properties for cryptography. These properties are incorporated in the hash values and provide the security needed for blockchain based voting systems.

- Deterministic Hash values
- Different inputs have different hash values
- Small change in input reflects largely in the hash value
- Fast and Easy Computation
- Computationally infeasible to extract the input data from the output

Using Cryptographic hash will always produce same result for a particular input and will not change. This property provides the uniqueness of the hash values for a particular input. To implement hashing for efficient practical use the hash function should return the hash of an input quickly. It is certainly very hard to determine the original input from its hash value. The original input can be found through its process on entry of inputs, hashing and comparing the output till finding a match only by brute force method.

5.3 TIMESTAMP

Timestamps show that the blocks are connected in a collective order. The initial block in blockchain is called as genesis block. It marks the period of each transaction on the block chain. It ensures the method of keeping track of the transactions that specifies the time of creating and modifying a document. Time stamp provides the exact details of any document with date and time to all parties involved without any doubt or concern.

5.4 NONCE

A number that is used only once is called nonce. A nonce is added to a hashed block to verify the difficulty levels which can be seen by rehashing the respective block. Transactions are entered in a way in which the order in which they obtained. The hash value of the current record will not only depend on the input but also on the hash value of previous transaction. A small change in the input will be largely reflected in the hash value so any change can be traced in the transactions.. A Block chain is distributed over group of computers called nodes are connected and has a copy of the blockchain. These nodes keep track of the changes made and if a new transaction is made and approved by major groups then it is updated with a block. This block must refer to the preceding block and a chain is formed and th blockchain is updated

5.5 MD5

MD5 algorithm is used for generating this hash value. The MD5 algorithm will always produce an output of 128-bits length only for any input. If the input data is in large number the output will be only limited. So in the block chain provision has been given to remember the hash will be only limited. So in the block chain provision has been given to remember the hash and kept track. The hashing functions help to track the output in full length. This algorithm is used to analyse integrity of any data input and ensures it is unique for the particular data. The MD5 algorithm developed by Ronald L. Rivest produces a technique that ensures, it is "computationally infeasible" that any two informations that have been input to the MD5 algorithm could have as the output of the similar message sends, or that a false message could be created through apprehension of the message sent. MD5 extends more security and faster compared to its predecessors like MD2 and MD4. MD5 is an extended version of MD4 but more secure and swift.

VI. CONCLUSION

The voting process is leveraged by block chain through its secure trustworthy flexible functionality. It delivers a viable digital platform for future free and fair democratic elections and certainly provides its optimum benefit in the process of voting. The failures such as false voting, time consuming process, and expensive system in the existing voting process can be set right by the block chain and it will ensure an advanced system of technology meant for an advanced community in learning, knowledge and in practice.

VII. FUTURE WORK

Uniqueness and innovations that are beneficial to any existing systems should always be adopted and utilized; Block chain is a modern advanced technology that provides much space for efficient, fair, cost effective and digital voting democratic elections. Though block chain is in its early stage of adoption and experimented in very few countries only, its speed in delivering of results, secured storage of election database, reliability, privacy and comfortability for voters may attract the world countries to adopt the block chain in their elections in future. This digital voting system will provide the best solution to the existing procedural failures in elections in the years to come

REFERENCES

1. M. Volkamer, O. Spycher, and E. Dubuis, "Measures to establish trust in internet voting" in Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance, 2011, pp.1-10.
2. É. Bélanger and R. Nadeau, "Political trust and the vote in multiparty elections: The Canadian case," European Journal of Political Research, vol.44, no. 1, 2005, pp. 121-146.
3. T. Kunioka and G. M. Woller, "In (a) democracy we trust: social and economic determinants of support for democratic procedures in Central and eastern Europe," in The Journal of Socio-Economics, vol. 28, no.5, 1999, pp. 577-596.
4. D. Basin, H. Gersbach, A. Mamageishvili, L. Schmid, and O. Tejada, "Election Security and Economics: It's all about Eve," in Proceedings of International Joint Conference on Electronic Voting, 2017, pp. 1-20.
5. S. Wolchok et al., "Security analysis of India's electronic voting machines," in Proceedings of the 17th ACM Conference on Computer and Communications Security, 2010, pp. 1-14.

6. M. Pilkington, "Block chain technology: Principles and applications", in Research Handbook on Digital Transformations. 2016, pp. 225-253.
7. G. Gabison, "Policy Considerations for the Blockchain Technology Public and Private Applications" in SMU Science and Technology Law Review, vol.19, no.3, 2016, p.327.
8. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm" in Lecture Notes in Computer Science 3156, 2004, pp. 357-370.
9. Samuel Agbesi, "Electronic voting recording system based on blockchain technology" in International Journal of Electronic Governance, CMI Aalborg University, Department of Electronic Systems, Copenhagen, Denmark, 2019, p. 1-8.
10. Watt, B, "Implementing Electronic Voting," A report addressing the legal issues by the implementation of electronic voting, University of Essex, 2002.
11. Mitrou, L., Gritzalis, D., Katsikas, S., Quirchmayr, "Electronic Voting: Constitutional and Legal Requirements, and their Technical Implications" in Secure Electronic Voting. Advances in Information Security, vol 7. 2003, pp. 43-60.
12. Xenakis, A., and Macintosh, A., "Procedural security in electronic voting" Proceedings of the 37th Hawaii International Conference on System Sciences, vol. no 5, 2004, pp1-8.
13. Kohno, T., Stubblefield, A., Rubin, A., and Wallach, D "Analysis of an Electronic Voting System" Proceedings of in IEEE Symposium on Security and Privacy, 2004, pp.1-23

AUTHORS PROFILE



Mrs. Sophia B., M.E., is currently working as Assistant Professor in the Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore. She has completed her B. Tech in Information Technology, M.E in Computer Science and Engineering. Her area of research includes Artificial Intelligence, Data Analytics, Machine Learning and Deep Learning techniques. She has authored several National and International research publications.



Ms. Aishwarya S., B.E., is currently a final year student who belongs to Department of Computer Science and Engineering in Sri Krishna College of Engineering and Technology. She has presented a paper in IEEE conference and Organised many events on idea presentation. She has also got certification on Business Cambridge English – Preliminary and Enhancing softskills.



Mr. Hariprasath B.R., B.E., is currently a final year student who belongs to Department of Computer Science and Engineering in Sri Krishna College of Engineering and Technology. He has presented a paper in IEEE conference and Organised many cultural events in the campus. He has also done certification on 'Joy of computing using python'.



Mr. Diwakar S.S., B.E., is currently a final year student who belongs to Department of Computer Science and Engineering in Sri Krishna College of Engineering and Technology. He has presented a paper in IEEE conference and attended many workshops.