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/IJSRSET52310218

Blockchain Based Electronic Voting System

N Jeenath Laila, Sathya M
Department of CSE, GCE Tirunelveli, TamilNadu India

ARTICLEINFO

Article History:

Accepted: 01 June 2023
Published: 06 June 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
361-371

ABSTRACT

In today's digital environment, the voting system has moved from paper based to a digital system. A digital e-voting system has many properties such as transparency, decentralization, irreversibility, and non-repudiation. The growth in the digital e-voting system raises many security and transparency issues. In this paper, we used the blockchain technology in the digital electronic voting system to solve the security issues and fulfill the system requirements. It offers new opportunities to deploy a secure e-voting system in any organization or country. The solution is far better as compared to other solutions because it is a decentralized system, containing the results in the form of bit-coins, having different locations. We will also analyze the security of our proposed voting system, which shows our protocol is more secure as compared to other solutions. The paper proposes a novel electronic voting system based on block chain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain based e-voting system. In particular, we evaluate the potential of distributed ledger technologies through the description of a case study namely, the process of an election, and the implementation of a blockchain based application, which improves the security and decreases the cost of hosting a nation wide election.

Keywords: EVoting, Blockchain, Digital vote

I. INTRODUCTION

Recent days, the paper based voting system has moved to a digital system. Voters can cast their vote from a remote location with the help of some smart devices like smart-phones, tablets etc. to find out the best suitable candidate in an organization, country, or university. The movement from paper based voting systems to electronic systems brings new enhancements such as real time counting, instant result, environment friendly, transparent, anonymity, less error and decentralization. With the development in the digital voting system, there are a number of security issues, flaws, and attacks coming. In any electronic voting system the authentication, anonymity, accuracy, consistency, and verifiability are

the basic system requirements.Blockchain stores transactions in a block, the block eventually becomes completed as more transactions are carried out. Once complete it is then added in a linear, chronological order to the blockchain

The initial block in a blockchain is known as the 'Genesis block' or 'Block 0'. The genesis block is usually hardcoded into the software; it is special in that it doesn't contain a reference to a previous block ('Genesis Block'). Once the genesis block has been initialised 'Block 1' is created and when complete is attached to the genesis block. Each block has a transaction data part, copies of each transaction are hashed, and then the hashes are paired and hashed again, this continues until a single hash remains; also known as a merkle root.Blockchain is a distributed, immutable, incontrovertible, public ledger. This new technology has three main features:

Immutability: Any proposed "new block" to the ledger must reference the previous version of the ledger. This creates an immutable chain, which is where the blockchain gets its name from, and prevents tampering with the integrity of the previous entries.

Verifiability: The ledger is decentralized, replicated and distributed over multiple locations. This ensures high availability (by eliminating a single point of failure) and provides third-party verifiability as all nodes maintain the consensus version of the ledger.

Distributed Consensus: A distributed consensus protocol to determine who can append the next new transaction to the ledger. A majority of the network nodes must reach a consensus before any new proposed block of entries becomes a permanent part of the ledger.

Some of the characteristics are :

Transparency: Any Election has to be transparent at every step. Everything should be available for scrutiny to all its stakeholders.

The integrity of Ballot: The votes cast in a ballot should be secure and immutable. There has to be a mechanism to check the integrity of the ballot.

Privacy of Voter: Votes cast by voters should be kept private to them and there should be no way that votes to voter match could be found.

Accessible to every voter: An election must be organized so that it should be accessible to every eligible voter.

Equal Treatment to all Contestants: Every contestant should be treated equally and there should be no unfair procedural advantage to any of the contestants.

Ensuring Eligibility of all Stakeholders: It should be made sure that there are necessary checks for verifying the eligibility of all voters and contestants.

One Voter One Vote: Every voter should have only one vote.

These features are in part achieved through advanced cryptography, providing a security level greater than any previously known record-keeping system. Blockchain technology is therefore considered by many, including us, to have a substantial potential as a tool for implementing a new modern voting process.

II. LITERATURE REVIEW

Ronald Cramer at al proposed a multi-authority secret-ballot election scheme that would guarantee robustness, universal verifiable, and privacy. where voters will participate using a computer, and the main consideration is the voter's efforts.In this system voters cast their ballot on a bulletin board. The bulletin board works with extended memory such that any part can access its content but won't be able to modify the data. The ballot does not contain any information about the vote itself but it does have an acknowledgment that it is a valid vote. The final tally is done when the deadline is over can be verified by any individual against the product of all submitted votes. This ensures verifiable due to the encryption method used.

Patrick McCorry et al had proposed the internet voting protocol with decentralized features and maximum voter privacy using Open Vote Network (OVN). The OVN is a smart contract for the Ethereum Blockchain. After implementing this system the creators concluded

that it costs 0.73$ per voter on this system. They had an upper limit for the number of voters to 50 to reduce the gas usage. However, the researchers soon found out that OVN is susceptible to DOS attacks. It could also suffer through traffic jams during the transaction which could delay the voting process for a longer time. Hence this implementation is successful for boardroom meetings with a major drawback that each individual who wishes to vote needs to download the entire copy of the network.

Mrunal Pathak et al proposed a system for the Indian Election System based on the Hyperledger Network. The booth agents at different polling booths act as different nodes. These agents are selected by the Election Commission of India. For each phase, the consent of 5 nodes is to be considered. Membership Service Provider is also present on polling booths which helps to authenticate the voters and generate public and private keys. Here they have suggested having three phases. During the preparation phase, a voter has to go to the nearest authorized voting center and register with his credentials so that his name is included in the Hyperledger network. During the Voting Phase, the MSP issues the public and private keys to the voter. Once the voter casts a vote for a candidate it is counted as a transaction. The process of the Hyperledger network begins here. Each transaction is endorsed by at least 5 nodes. These transactions are sent to the ordering services and later to the main chain. The Post Voting phase includes steps such as recording votes in the main chain after validation, locking the authority of the voter for the time frame, counting of votes and so on. The validation is done by 5 different nodes to avoid any manipulation which is still computationally impossible.

Suporn Pongnumkul et al compared the two most popular Blockchain technology platforms viz Ethereum and Hyperledger. They developed an application that can transfer money from account A to account B. On comparing execution time, they found that as the no of transactions increases, the execution time increases. However, Hyperledger's execution time is always less than that of Ethereum.On comparing latency it was found that on less no of a transaction, Ethereum's latency is 2x times that of Hyperledger. Also on varying no of transactions the change of average throughput of Hyperledger is relatively larger than sthat of Ethereum.

Denis Kirillov et al proposed a system that can integrate traditional paper voting with blockchain technology which increases the trust among the participants. Due to rapid development of ledger based technology and their potential to solve existing problems a modified version of the earlier developed protocol is being cited in this paper.

M. Pawlak et al proposed that the voting process relies on citizen's email addresses that can be hacked or manipulated easily. To be obvious, there will always be some people who register to the system using someone else's mail address and vote on behalf of them. For example, a grandson may open an email address for his grandparents from different devices, and cast their votes. This method guarantees none of the required qualifications such as security, data integrity or privacy that an e-voting system has. For such a system, stealing votes or changing votes are totally.

P. Tarasov et al proposed a peer-to-peer blockchain based voting system. Main focus of this research is to protect the anonymity of the ballots and commitment of the votes to the blockchain. For this purpose, they propose a unique vote commitment format. Their solution has a solid base for such a vote commitment format but we propose a different system that leans on another system that is maintained by the government. In this purpose we preferred to use a structure for chains that consists of different key-value pairs representing the vote itself.

R. Hanifatunnis et al designed a system that creates blocks following collection of ballots from voters to keep them in a database until the end of election process [1]. In this paper, authors tried to eliminate the need for a database. Blockchain is being used for various areas such as IoT. Since there are so many

different devices and each of them are processing different data, new approaches emerged from this area. S. Bartolucci et al discussed the blockchain IoT interactions in the paper and one of the models that have been discussed is hybrid model that uses different chains in different layers and levels which inspired us in our blockchain based e-voting system.

A. Reyna proposed a one-time ring signature in order to ensure the anonymity of the voting citizen. However, each candidate in the election needs a public key pair in this architecture and adding a new candidate increases the complexity of the signing process and at every node demanded CPU power increases. One time ring signature architecture does not depend on any trusting center but in our special case we give the authority of selecting a candidate to the government which is the trusting center for the election.

III. EXISTING SYSTEM

In order to make the voting process more effective the institutions like 'Election Commission' came into existence in different parliamentary democracies. The institutions, along with setting up the process and legislation for conducting the elections, formed the voting districts, electoral process, and the balloting systems to help in conduct of transparent, free, and fair elections. The concept of secret voting was introduced since the beginning of the voting system.

Since the trust on democratic systems is increasing it is important to uphold that the trust on voting should not decrease. In the recent past there have been several examples where it was noted that the voting process was not completely hygienic and faced several issues including transparency and fairness, and the will of people was not observed to be effectively quantified and translated in terms of formation of the governments.Since all these countries are among the emerging democracies, it is pretty likely that in next decades they will emerge as full democracies and the vote and the voting process willearn more respect and trust over time.

IV. METHODS AND MATERIAL

The proposed system enables the voter to vote from their remote location. Initially, the voter has to register into the voting system with fingerprint registration. After the successful registration, each voter will receive a unique identity number. On the polling day, the voter has to enter his/her unique id to login into the voting system to cast their vote. Before casting the vote, the voter has to be authenticated by the biometric system. The record of the voter is checked with the help of a local database.Once the voter has passed the authentications check, he is brought to the voting screen to vote. From the voting machine the names and respective party symbols of each candidate are displayed and the voter can vote according to his will. The confirmation screen seeks the confirmation of the voter and records the vote casted by the voter.The voter can vote only once, and once the vote is casted is voting record is marked as "voted", which restricts the voters from voting again. The name of the voter can be blocked or eliminated from the list of eligible voters list for the current elections, once he has casted the vote.The polling process continues until the voting time ends or all the voters in the voting list have casted their votes. Finally, the election commission will declare the results of the election.

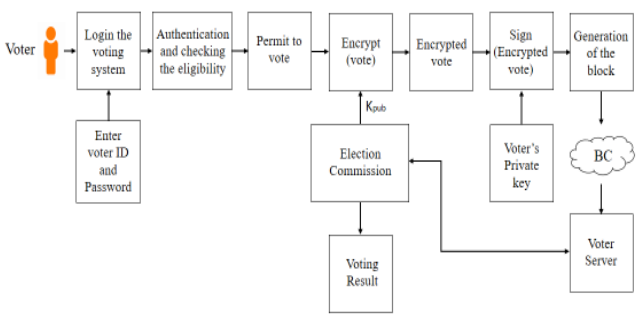

Figure 1: A Block diagram

The proposed electronic voting system is made based on the two concepts: hashing and encryption. The system contains the following components: participants = {Voters}, organizers = {Election coordinators}, inspectors = {Election commission}, encryption algorithm = {AES}, Hash algorithm = {SHA-256}, voting server.

- HASHING : Hashing is the process of changing the arbitrary and variable size input to a fixed size output [3]. There are different functions that perform hashing of different level.
- SHA (Secure Hashing Algorithm) is another cryptographic hash function that yields a 160 bit hash value consisting of 40 hexadecimal characters. The algorithm could not resist the collusion attacks against it and its usage has declined after 2005. In this time several new algorithms have also been proposed, including SHA 3, and SHA 256. The SHA 2 set of algorithms is designed by the US's Nation Security Agency. SHA 256 and SHA 512 are new hash functions that do not have collision problems and are deemed secure.
- Proof of work : The concept of the proof of work deals with the mining / creation of the blocks in such a way that it can be proved that a significant effort has been made for the resolution of the mathematical problem introduced for the creation of a block in the blockchain. The mathematical complexity is increased on the creation of every new block so make the creation of the block complex and a rewarding scenario. The increasing complexity is introduced with the help of the hash functions, merkle trees, and the nonce value.

A. Election Creation

Election administrators create election ballots [1].The election administrators create the election, register voters, decide the lifetime of the election.Election administrator defines a list of candidates for each voting. The registration of voters phase is conducted by the election administrators.When an election is created the election administrators must define a deterministic list of eligible voters.The admin will authenticate the user's identity proof and register the voters with their fingerprint authentication.

B. User Authentication

To authenticate a person a valid UID number is required.This record is extracted from the local database and sent to authenticating servers.For verification the person's fingerprint will be scanned at the client-side and matched one-to-one at the servers with the data extracted from the local database.

Figure 2 Fingerprint Device

The device shown in figure 2 will be used for fingerprint authentication. This device will scan the fingerprint of the user during the registration process. On polling day, again the voter is verified by this device by matching the fingerprint stored on the local database. Thus the user will be authenticated.

C. Creation Of Blocks

Unlike the bitcon's blockchain, where a significant proof of work is required, it is not the case for the voting system. [3] It is vital that the nodes / block are created before the transaction can take place in the respective blocks. The creation of the blocks on the blockchain is a sensitive matter and requires sufficient security before a block can be created. The creation of the block takes place when following have been met.The presiding officer (PO)verifies his unique identity number and his biometric authentication.The biometric are verified and the permission is granted.The system shall generate a random number by using the SHA-256 hashing algorithm, system will

generate a hash and send the result to the presiding officer to generate a block. Along with the other information of the block the hash value is also saved in the block header which is visible to others as well.

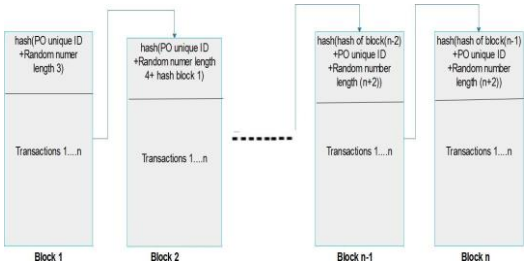

Figure 3 Block creation

The next block to be generated will be requested by the next presiding officer. Based on the hash value of the first block, the presiding officer will submit his unique identity for the creation of the next block. The next block is generated by generating a new random number, associating that with the hash of the previous block and applying the SHA-256 algorithm., i.e (RN describe random number).

- *Block 1 = hash(UID + RN (length = 3))*
- *Block 2 … n = hash(UID + Block (n-1)+ RN (length = n+2)) (2)*

D. Sealing Of The Blocks

The polling process shall continue until either the polling time finishes or the number of registered voters has completed. Once the polling is complete, the next step is to seal the blocks to ensure that the block come even more secure and adding security is included. [3] In order to seal a block following items are considered.It is to be ensured that either the polling time has elapsed or all the registered voters have casted their votes.The completion of the polling process is to be confirmed by the PO of that polling station.

The data of the block (i.e. the entire result) will be hashed using the SHA-256 algorithm. This is done by concatenating the results inside the block and hashing them in pairs; the block is hashed based on the hashed contents of the block. Another system generated random number can be added in the hashing to make it more secure.

Every proceeding block that confirms the completion of the transactions will have used the hash of the previous block, a new random number, and hash of the block to generate the hash value that will be used by the proceeding blocks.

The sealing of the block means that the block has now been sealed with a hash function and the contents of the block can't be changed by ensuring the application of the mathematical puzzles that are NP hard to solve. The sealing process uses the hashing algorithm called SHA-256 and following equations introduce the mathematical complexity.

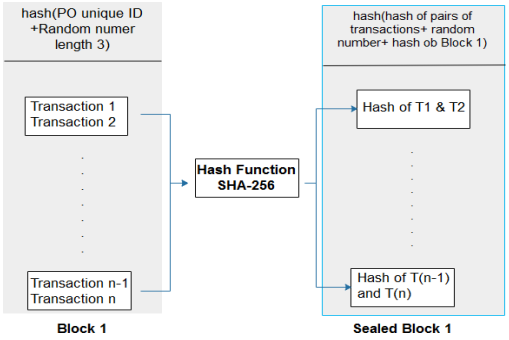

Figure 4 Sealing of the blocks

The sealing process of the blocks is demonstrated in Fig 4. After the block has been sealed, the sealed block represents the actual block.

The representation of the sealed blocks is such that the blocks are integrated among themselves by using the chained hash key and the key of one block is used by its proceeding block to generate the next hash and this chain continues unless the blocks finish.

During the process of applying the hash function on the transactions a pair of transactions (sequential) are selected and the hash is applied on them. This sequential hashing process runs on all pairs of transactions and a hash is gen- erated based on all the hashed data by applying the SHA-256 algorithm. Once the hash of a block has been generated it is integrated

with the hash of the previous block and a new random number and the outcome is hashed again to ensure that the hash outcome function is not solvable without the capability of the solving NP hard problems. The purpose of the blockchain based electronic voting is to introduce secure voting process that can gain trust of the stakeholders, including, voters, political parties, and state institutions. The security of the casted vote is ensure by the block creation, block sealing, and content hashing. While the created block is secured by the (1) and (2) and uses the SHA-256 algorithm which is known to be sufficiently secure to secure the e-voting process, the blocks is sealed with the unique hashes produced by the SHA-256 algorithm based on the unique input values, mentioned in (1), (2), (3), and (4).

The Merkle trees are formed as each block is associated with the next and previous block (except the first and the last block) in terms of accepting and providing the hash value that is used for stitching the block with the chain.

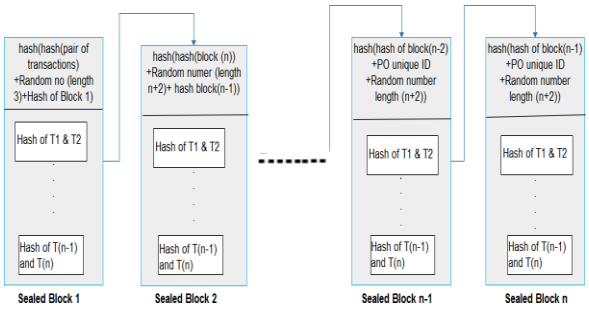

Figure 5 Sealed block

The representation of the sealed blocks is demonstrated in Fig 5. that shows the connection of the block after they are sealed.

E. Block Mining

Miners create new blocks on the chain through a process called mining. In blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains.

The encrypted data needs decryption to prove validity. Decrypting the data encoded in blocks is not an easy task and demands computational hardware and software alongside human efforts. [2] One single code decryption will take an enormous amount of time and energy both for the computer and the human.A combination of the computational speed and human intelligence will result in the decrypted data, which, when linked with the adjacent blocks, verifies the transaction.The miners need to solve the complex problem to find the perfect hash that matches and fits. The solution to the hidden code encryption is known as the 'Proof-of-work.' As the name suggests, it is a proof of the abundance of resources, time, and energy that is spent by the miner. This proof-of-work is challenging to produce and may sometimes prove to be of lower profitability.When a transaction takes place, a mathematical problem is given to all the single users in the blockchain network to solve.Once the solution is found, all the other miners in the blockchain network will validate the decrypted value and then add it to the blockchain. Thus, verifying the transaction.

F. Collection Of Voting Results

The collection of the results is done from the stored data on the blocks through the significant organization of the nodes in the blockchain[1]. The chain of blocks works at the lower end and works to accumulate the data in the containers (block) that are chained together through an algorithm serially. However, a Merkle tree is maintained that records the distribution of the block and the degree of their decomposition.

It can be observed that the record of each transaction taking place is stored at the top level, i.e. level 0. At level 1, the layer describes the national seats while at level 2, the layer demonstrates the polling stations in any constituency. Thus, any transaction, in any block, can directly be located and recorded by keeping them distributed and open for transactions.

V. RESULTS AND DISCUSSION

Figure 6 Homepage

Fig 6 is the actual home page for the electronic voting system. This page allows the voter to poll from their remote location with the help of smart devices.

Figure 7 Election enroll

To create a new election, the admin can enroll by specifying election name,constituency,election date and result date depicted in Fig 7

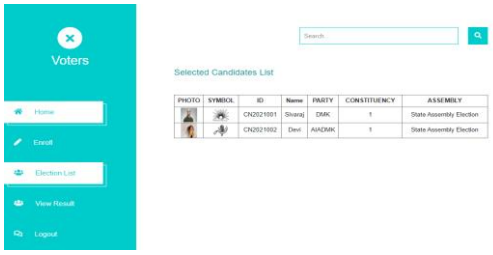

Figure 8 Election List

Fig8 shows the list of candidates participating for a particular election can be viewed in the election list.

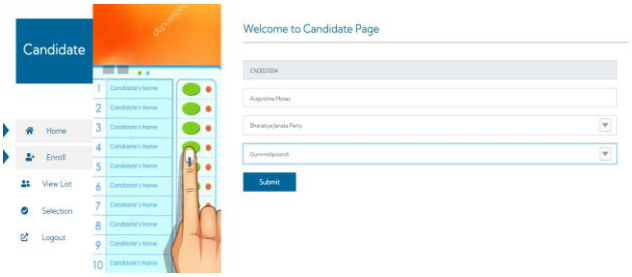

Figure 9 Candidates enroll

In Fig 9 depicts how to enroll a new candidate, admin has to specify the candidate name, party and constituency from the list of constituencies.

Figure 10 Candidates view list

Each candidate photo and symbol can be uploaded for respective candidates.

Figure 11 Candidate Selection

From the list of candidates, the admin can select the number of candidates to be participated for a particular election was depicted in Fig 11

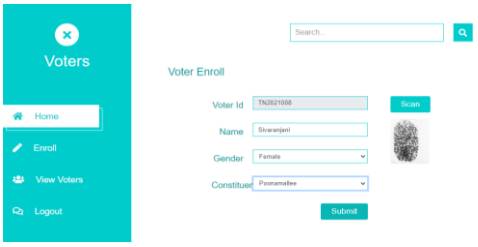

Figure 12 Voters Enroll

The admin can enroll each voter by entering the voter's name, Gender, Constituency and scanning fingerprint authentication was shown in Fig12

Figure 13 View voters

The list of voters enrolled for a particular election can be viewed in view voters option. Fig13 shows the view voter option

Figure 14 Polling

The voter can poll the vote by using the unique voter ID generated during voter's registration.

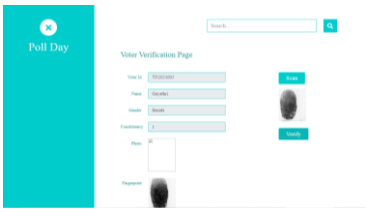

Figure 15 Verification of voters

On polling day, the voter is verified by one to one fingerprint matching and if it is matched only, the voter is permitted to vote.

Figure 16 Casting a vote

After fingerprint verification, the voter is allowed to cast a vote for a candidate. List of candidates and their respective symbols for each candidate are displayed. The voter can select a candidate only once and once the vote is casted, it is marked as voted which restricts the voter from voting again.

Figure 17 Data Encryption

After the voter is casted, the vote is encrypted by using SHA-256 algorithm and the block is verified by the miners and it is successfully added into the blockchain network.

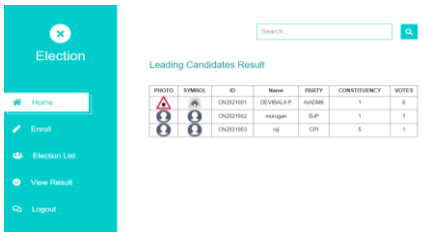

Figure 6.13 Instant Results

On the polling day, the admin is able to see the candidates' votes and the leading candidates' votes will be displayed at the top of the view results page.

VI. CONCLUSION

E-voting is still a controversial topic within both political and scientific circles. Despite the existence of a few very good examples, most of which are still in

use; many more attempts either failed to provide the security and privacy features of a traditional election or have serious usability and scalability issues. On the contrary, blockchain-based e-voting solutions, including the one we have implemented using the smart contracts and the Ethereum network, address (or may address with relevant modifications) almost all of the security concerns, like privacy of voters, integrity, verification and non-repudiation of votes, and transparency of counting. Yet, there are also some properties that cannot be addressed solely using the blockchain, for example authentication of voters (on the personal level, not on the account level) requires additional mechanisms to be integrated, such as use of biometric factors.

Blockchain technology has lot of promise, but in its current state its require lot more research and currently might not reach till its full potential. There needs a concerted effort in the core blockchain technology to improve its support for more complex applications.

VII. REFERENCES

[1]. Mohamed Ibrahim, Kajan Ravindran, Hyon Lee, Omair Farooqui " ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication" 2021 - IEEE 18th International Conference on Software Architecture Companion(ICSA-C).

[2]. Abhishek Kaudare, Milan Hazra, Anurag Shelar, Manoj Sabnis " Implementing Electronic Voting System With Blockchain Technology " 2020 International Conference for Emerging Technology (INCET) Belgaum, India. Jun 5-7, 2020.

[3]. Ashish Singh, Kakali Chatterjee " SecEVS : Secure Electronic Voting System Using Blockchain Technology " 2018 - International Conference on Computing, Power and Communication Technologies.

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

[5]. EIU Democracy Index 2017. Accessed: Aug. 3, 2018. [Online]. Available: https://infographics.economist.com/2018/DemocracyIndex/

[6]. ScienceDirect. Democracy Online: An Assessment of New Zealand Government Web Sites. Accessed: Aug. 1, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0740624X00000332

[7]. M. Volkamer, O. Spycher, and E. Dubuis, "Measures to establish trust in Internet voting," in Proc. 5th Int. Conf. Theory Pract. Electron. Gover- nance, 2011, pp. 1–6.

[8]. E. Bélanger and R. Nadeau, "Political trust and the vote in multiparty elections: The Canadian case," Eur. J. Political Res., vol. 44, no. 1, pp. 121–146, 2005.

[9]. 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," J. Socio-Econ., vol. 28, no. 5, pp. 577–596, 1999.

[10]. T. van der Meer, "In what we trust? A multi-level study into trust in parliament as an evaluation of state characteristics," Int. Rev. Administ. Sci., vol. 76, no. 3, pp. 517–536, 2010.

[11]. D. Basin, H. Gersbach, A. Mamageishvili, L. Schmid, and O. Tejada, "Election security and economics: It's all about eve," in Proc. Int. Joint Conf. Electron. Voting, 2017, pp. 1–28.

[12]. P. Bevelander and R. Pendakur, "Electoral participation as a measure of social inclusion for natives, immigrants and descendants in Sweden," Tech. Rep., 2008, p. 33

[13]. S. Wolchok et al., "Security analysis of India's electronic voting machines," in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 1–14.
[14]. J. Stern. Votem—Voting for a Mobile World. Accessed: Jul. 31, 2018. [Online]. Available: https://votem.com/
[15]. M. Pilkington, "11 Blockchain technology: Principles and applications," in Research Handbook on Digital Transformations. 2016, p. 225.

Cite this article as :

N Jeenath Laila, Sathya M, Sathya M Mariappan, "Blockchain Based Electronic Voting System", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 3, pp. 361-371, May-June 2023. Available at doi : https://doi.org/10.32628/IJSRSET52310218
Journal URL : https://ijsrset.com/IJSRSET52310218