EasyChair Preprint

№ 7034

Secure E-Voting Using Blockchain Technology

Sonali Ridhorkar and Barkha Ramteke

November 11, 2021

SECURE E-VOTING USING BLOCKCHAIN TECHNOLOGY

Prof. Dr. Sonali Ridhorkar
Department of Computer Science and Engineering
G H RAISONI INSTITUTE OF ENGINNERING AND TECHNOLOGY, NAGPUR
sonali.ridhorkar@raisoni.net

Barkha Ramteke
Computer Science department
G H RAISONI INSTITUTE OF ENGINNERING AND TECHNOLOGY, NAGPUR
barkharamteke@gmail.com

***Abstract*- Modern electronic voting systems use blockchain as the underlying storage model to make the voting process more transparent and provide data immutability as blockchain technology grows in popularity. The transparent feature, on the other hand, may reveal sensitive information about a candidate because all system users have the same right to their data. Furthermore, the pseudo-anonymity of blockchain will expose voters' privacy, and third-parties involved in the voting process, such as registration institutions, will have the ability to tamper with data. We use an authority management technique in blockchain-based voting systems to overcome these challenges. We propose AMVchain, a fully decentralized and efficient blockchain-based voting system, in this paper. AMVchain offers a three-tier access control design, with smart contracts doing validation and granting rights at each layer. To protect ballot-privacy, a linkable ring signature is used in the voting process. By incorporating proxy nodes, AMVchain also imposes a compromise between efficiency and concurrency. The results of the studies reveal that our system meets the basic requirements in the presence of a large number of concurrent users.**

Keywords— Blockchain, AMVchain

I. INTRODUCTION

Advanced vote-based systems are based on voting a ballot, whether it is traditional artistic dance-based voting or electronic voting (e-voting a ballot). Voter apathy has been growing in recent months, especially among the younger PC/technically savvy generation [1]. E-voting is a strategy for meeting the demands of the youth [2, 3]. Blockchain technology is supported by a distributed network of thousands of interconnected hubs. "Each of these hubs has its own duplicate of the appropriated record, which contains the complete history of all trades handled by the system.". The system is not controlled by a single power. They acknowledge an exchange if the majority of the hubs agree [4-6]. This method allows clients to remain anonymous. An in-depth evaluation of the blockchain innovation (counting precise agreements) suggests that it is a valid explanation for e-voting a ballot and, moreover, that it has the potential to create e-voting a ballot more adequate and secure. [7-9].

The blockchain technology is supported by a distributed network of thousands of interconnected hubs. If the majority of the hubs agree, they accept the adjustment. This method allows clients to remain anonymous. An in-depth evaluation of the blockchain innovation (counting precise agreements) suggests that it is a valid cause for e-voting a ballot and that it has the potential to make e-voting a ballot more satisfying and reliable. "I) more openness as a result of open and appropriated records, ii) inalienable obscurity, iii) security and unwavering quality (especially against Denial-of-Service Attacks), and iv) changelessness (solid trustworthiness) [7-9]".

In the current paper and voting form voting a ballot procedure, the outcome examination of the political contest takes hours and occasionally days, and the results are rarely screwed up by human or computer error, resulting in the operation taking significantly longer. The blockchain concept envisions a world in which that specific flaw is removed from the equation and votes are immediately verified. Voters should cast a ballot in a regulated domain to meet the protection and security requirements for e-voting a ballot, as well as to ensure that the political decision system does not enable constrained voting. To achieve these goals, we suggest a hyper ledger private blockchain in our research. It employs a formula that expresses relatively short exchanges via an agreement component that is based on a stake in one's way of life.

II. RELATED WORK

E-voting a ballot that self-counts. In scholarly study, e-voting a ballot is a thriving and unfading point. A focal authority is often incorporated in traditional brought together e-voting a ballot convention for sorting out the political decision and checking the votes. Kiayias et al [8] suggested the idea of self- tallying voting a ballot to achieve better grounded voter security, which is another perspective in decentralized evoting systems. In self-counting systems,

counting is an open system in which any group, including voters and observers, can check the authenticity of each polling form and compute the final voting result after collecting all of the substantial voting forms. They made the most significant breakthrough by using a release board, which assures flawless voting form security and debate freedom Growth et al. [7] "suggested a less complicated plan that would be more beneficial for every voter." They also created an unknown communication channel with perfect message mystery at the expense of the convention's increased round unpredictability, which requires n + 1 rounds for n voters." "Proposed a self- counting voting a ballot convention depending on a two-round mystery veto convention," according to Hao et al. [6]. (AVnet). Their convention has similar security features, but it is more successful in terms of round unpredictability." Bitcoin, Khader et al. "guaranteed that is neither vigorous nor reasonable, and they propelled the convention by introducing a responsibility step and a recovery round." To strengthen voter protection, Takabatake et al. [3] developed a voting convention based on Zerocoin. In 2017, McCorry et al. "introduced Open Vote Network 8 9 as the primary application of a decentralized self- counting e-voting a ballot convention based on Blockchain. "The dedication in is the hash of the vote, which is hopeless if a voter will not cast his voting form in the voting stage." Shahzad B et al "exhibited a reliable evoting system in to alter the square makes and seals by changing the hash work in the blockchain to accomplish the validity and decency of the political decision. In the DATE proposed by Lai et al., the decency of the e-voting a ballot and the security assurance for voters were acknowledged by utilizing the blockchain and ring mark innovation. Simultaneously, it likewise made them count highlight. Tragically, on the grounds that there is no outsider expert on the plan, it can't be reviewed. In an e-voting a ballot system dependent on blockchain and ring mark set forward" by Wu et al**,** straightforwardness and security were settled.

Wei-Jr Lai et al "proposed a proficient decentralized unknown voting system. The system depended on the Ethernet and utilized the ring mark plan to guarantee the straightforwardness and protection of the system. It accomplished the objective of high proficiency and speed through equal activity in the checking stage. Along these lines, Freya Sheer Hardwick offered a blockchain e-voting a ballot convention, which accomplished obscurity and straightforwardness as well as expanded the modifiability of the polling form by using blind mark and duty innovation in the blockchain. This has additionally become another course in the investigation of e-voting a ballot system".

Pd McCorry and colleagues. "In, proposed a blockchain-based shrewd agreement for board races, which is the main scheme that does not rely on any trusted in power to tally and assure voter security. From then on, Adiputra CK proposed "A Proposal of Blockchain-Based Electronic Voting System" in 2018, which addressed the general unquestionable status issue of blockchain electronic voting plans while ignoring the security issue of e-voting a ballot.".

III. PROBLEMSTATEMENT

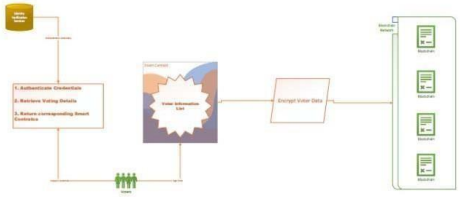
Because the blockchain maintains an unchangeable square of their vote and their character, voters are not allowed to vote more than once. Because the blockchain is irreversible, erasing a vote is absurd. Controllers or reviewers can efficiently verify the votes at any time and from any location. The e-voting a ballot programming application can provide considerable benefits to both balloters and EC (Electoral Commission) officials. However, at the same time, the proposes e-voting a ballot application provides a wide range of risks to political decision security and honesty, and fundamentally alters the spirit of political race transparency and inquiry. E-Voting has a Relatively Favorable rating; at the end of the day, Comparative Benefit is assigned when an improvement is deemed superior to the previous voting form-based voting procedure; therefore e-Voting is superior to the manual voting system. The e-voting a ballot programming application can provide considerable benefits to both balloters and EC (Electoral Commission) officials. However, at the same time, the proposes e-voting a ballot application provides a wide range of risks to political decision security and honesty, and fundamentally alters the spirit of political race transparency and inquiry. E-Voting has a Relatively Favorable rating; at the end of the day, Comparative Benefit is assigned when an improvement is deemed superior to the previous voting form- based voting procedure; therefore e-Voting is superior to the manual voting system.

IV. EXISTING SYSTEM

The cutting-edge majority rule governments are expanding on voting a ballot, whether it is the traditional creative dance based or electronic voting (e-voting a ballot). Voter apathy has been growing in recent years, especially among the younger PC/educated generation. Evoting is being promoted as a possible solution for attracting younger voters. Various functional and security requirements are defined for a robust e-voting a ballot plan, including transparency, accuracy, auditability, system and information uprightness, mystery/protection, accessibility, and power dissemination. The present system is based on the blockchain. The current system operates in a secure electronic voting system that provides the decency and security of existing voting plans while also providing the simplicity and adaptability of electronic systems has been put to the test for quite some time. The current method makes use of blockchain to aid in the execution of distributed electronic voting systems.

4.1 DISADVANTAGES OF THE EXISTING SYSTEM

- No straightforwardness
- No Immutability
- No Remote Voting



Voters should cast a ballot in a controlled environment to meet the protection and security requirements for e-voting a ballot, as well as to ensure that the political race system does not enable confined voting. In our effort, we set up a Hyperledger private blockchain to achieve these goals. It makes use of a calculation that allows for equally swift exchanges through an agreement instrument that is based on a stake in one's way of life. It explains why Hyperledger is used in the blockchain system. Speak with each voter in the area where the ballot will be cast. Each locality hub has a product specialist who independently interacts with the "boot node" and manages the keen agreement's existence pattern on that hub. When the political race leader makes a political choice, a vote form smart agreement is circulated and transmitted to the corresponding location hub. When the polling form smart agreements are produced, each of the contrasting location hubs is given permission to associate with their relating contract. When a voter takes a decision based on her savvy contract, the vote information is certified by the majority of the comparing area hubs, and each vote they accept is recorded on the blockchain. The political decision process has the accompanying jobs:

1. A political decision manager is someone who manages the lifespan of a political campaign. This project could involve a number of different faith-based organizations and organizations. The political decision managers are in charge of making the political decision, registering voters, determining the duration of the decision, and appointing permissioned hubs.

2. A voter is a person who is eligible to vote. After making a political decision, voters can validate their identity, load political race voting forms, make their choice, and check their vote.

4.2 PROPOSED SYSTEM

The simple rationalization could be a ‘chain’ of blocks. A block is associate degree mass set of information. knowledge square measure collected and method to suit in an exceedingly block through a process known as mining. every block may be known employing a science hash (also referred to as a digital fingerprint). The block shaped can contain a hash of the previous block, so blocks will kind a sequence from the primary block ever (known because the Genesis Block) to the shaped block. during this method, all the information may be connected via a connected list structure.

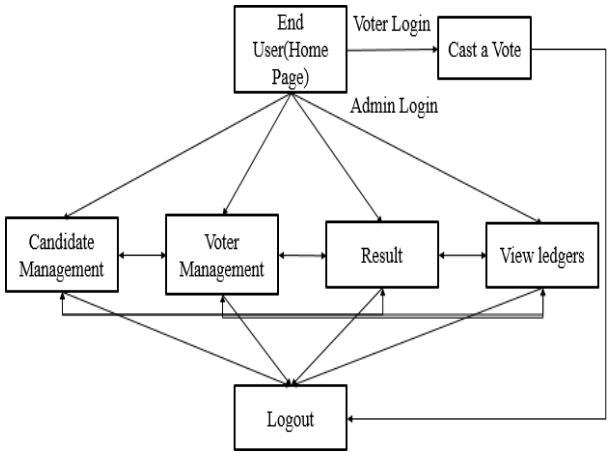
4.2.1 Analysis/Framework/Algorithm

1. Deterministic: This means that no matter how many times we enter the same input we will get the same result.
2. Quick Computation: This means that the result is generated quickly and this leads to an increase in the system efficiency.
3. Pre-Image resistance: Suppose we are rolling a dot (1-6) and instead of getting a specific number we get the hash value. Now we calculate the hash value of each number and then compare it with the result. And for a larger data sets it is possible to break pre-Image resistance by brute force method and this takes too long that it does not matter.
4. Small changes in Input change the whole Output: A minor change in the input significantly changes the whole output.
5. Collision Resistant: Every input will have a unique hash value.
6. Puzzle friendly: The combination of two values gives the hash value of new variable.

The need of hashing in blockchain:

- The blockchain is a sequence of blocks that contain data.
- Each block has a hash pointer that contains previous block’s data.
- So, if a hacker tries to attack a particular block, the changes will be reflected to the entire chain of blocks.
- Therefore, the blockchain concept is so revolutionary.

Fig The Proposed System/System Architecture

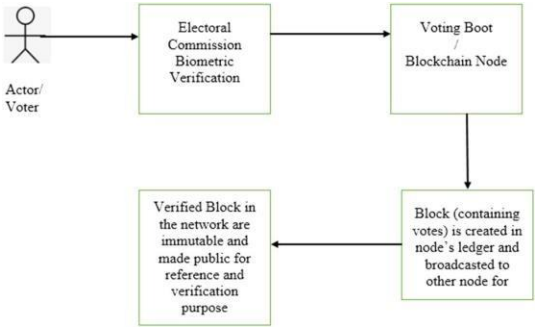


4.2.2 Workflow of the proposed system

In Fig. 1 we propose the basic workflow on working procedure for how the proposed system will work. The Actor signifies the voter, the voter arrives at the polling booth for verification and authentication. Electoral commission of each nation should be able to keep and update a comprehensive biometric record of its citizen, a dedicated bio- metric ID should be generated for each citizen, for example the biometric verification number (BVN) used in the financial system of Nigeria. This can partly be integrated into the proposed system, allowing voters that have been verified once for a particular vote session, unable to participate in another session elsewhere unless another voting category is selected. After verification of the biometric information of voter follows authentication during this phase voter's biometric ID is entered in the voting machine where voter will be allowed to vote for their candidate of choice. This biometric ID is again screened for the second time, if it exists in any node of the blockchain network, then voter will be restricted access to vote as it signifies voter's vote had already been counted somewhere. Successful authentication allows voter to continue with their voting process and vote casted are made public on the ledger across all nodes in network.

Figures 2 and 3 describes the first phase and second phase work of electoral commission respectively that how the proposed system will carry out their task phase wise

Fig. 1 Basic workflow idea



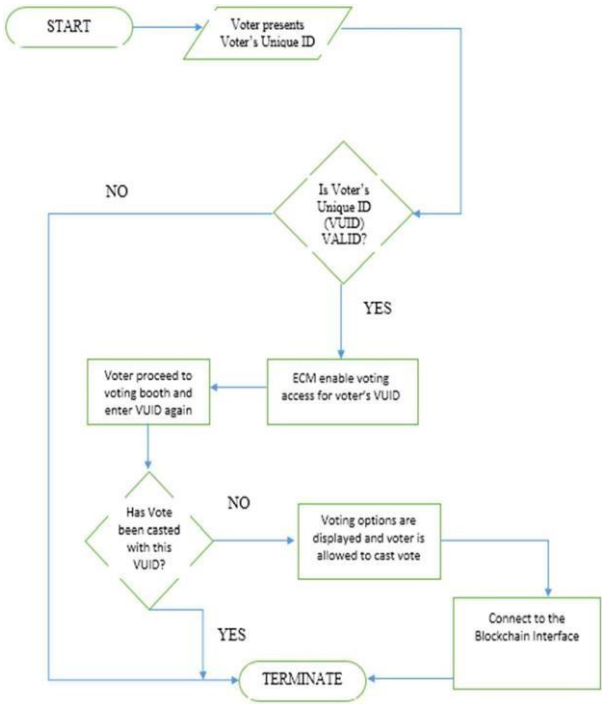


Fig. 2 Flowchart: first phase of electoral commission

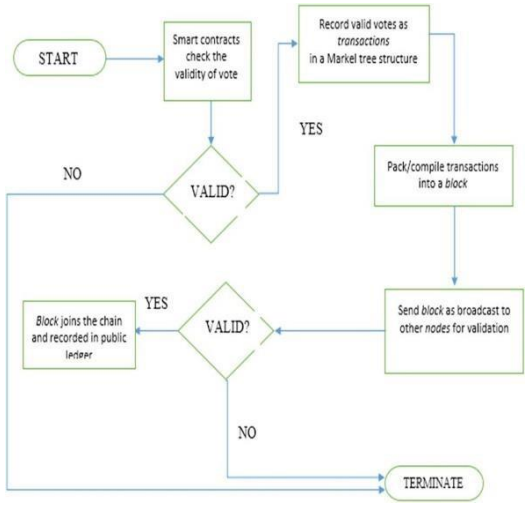


Fig. 3. The Proposed System/System Architecture

4.2.3 Architecture of the proposed system

This briefly explains the interaction within the blockchain network and some external actors. Permitted actors such as voters, external electoral observers, etc. can participate in the network from desired node and will have full participating feature according to their permissioned role in the network. Ledger as we know stores chunks of verified blocks, each block holds certain number of transactions (votes).[11] Every node in the network has an exact copy of the ledger, and each ledger can be accessed by any permissioned actor in that node. Consensus mechanism ensures that communication and exchange of data within nodes are valid as it should be or discard otherwise.

ADVANATAGES OF THE PROPOSEDSYSTEM

- *Greater straightforwardness because of open and dispersed records,*
- *Inherent namelessness in the blockchain systems,*
- *Security and unwavering quality*

VI MODULE DESCRIPTION

4.3 CONTESTANT MODULE

When a political choice is taken, the political race chairmen must create a predetermined list of qualifying candidates. This may necessitate a portion for a personality confirmation administration to safely authenticate and approve qualified individuals. Using such a service is necessary to meet the requirement of secure validation, which isn't guaranteed when using a blockchain basis. A character wallet would be produced for each qualifying candidate in our work. Every challenger is given a one-of-a-kind wallet for each political campaign in which they are qualified to run.

4.4 VOTER MODULE

At this point, the ageing of the large number of keys held by the voters begins, with the expectation that all of the panel and witness keys will have been raised by the time this stage begins. At this point, here's a rough outline. This is the stage that voters will go through as the political campaign unfolds, starting with entering the airport and ending with exiting the terminal, where the political decision is made. That must be decoded using their unique voter private key. Following the completion of the selection phase, a structured succession of information will be framed. The end result of this political race process is that each voter will receive a hash that can be used to check the results of the election. It is typical that each decision terminal does not have the same hash incentive for different voters.

4.5 ELECTION COMMISSION MODULE

The three sections that make up a savvy agreement are (1) recognizing the jobs that are associated with the understanding (in our case, the political race understanding), (2) the understanding procedure (i.e., political decision procedure), and (3) the exchanges (i.e., voting a ballot exchange) that are used in the savvy contract. 1) Election jobs: In a keen agreement, the election jobs include the gatherings that need to be included in the understanding. The following jobs are associated with the political election process: (I) Election overseer: Responsible for the entire life cycle of a political campaign. This project could involve a number of thought foundations and organizations. The leaders of political races make political decisions, register voters, set the duration of the political decision, and reassign permissioned hubs. Political race leaders create political decision polling forms using a careful agreement in which the chairman characterizes a rundown of alternatives for each voting region. The smart contracts are then put together on the block chain, where area hubs can link to their corresponding brilliant contract.

4.6 BLOCKCHAIN MODULE

Cryptography is the process of concealing and disclosing information by complicated number crunching, often known as scrambling and unscrambling. This implies that the e-voting ballot voter information must only be seen by the designated recipients.

The approach entails taking decoded data, such as voting ballot data, and encoding it with a logical estimation called a figure. This sends a ciphertext, which is a piece of e-voting ballot data that is completely meaningless until it is decoded. Symmetric-key cryptography is the name given to this encryption technique. Cryptography is used in blockchain development to ensure that e-voting a ballot trade are done safely, while also confirming all e-voting a ballot information and reserves of critical value.[13] As a result, everyone utilizing blockchain may be assured that once e- voting ballot information is stored on a blockchain, it is done so honestly and in a way that does not compromise security.

Using an open blockchain to store and exchange trade e-voting ballot information introduces serious security risks: all data recorded in the record is in clear text, as is customary. Data mystery cannot be guaranteed because each center has an exact copy of the record. The private blockchain is recommended to overcome the difficulties in the open blockchain. The opposite of open blockchain is private blockchain. It's because certain limitations that are exposed to everybody on an open blockchain aren't open to all here.

V CONCLUSION

The blockchain technology offers yet another option to get over electronic voting's limitations and reception barriers, preserving the security and honesty of political decisions while also establishing the groundwork for transparency. With a Hyper record private blockchain, it is feasible to submit several exchanges per second into the block chain, with each component of the brilliant agreement assisting the heap on the blockchain. Extra steps should be taken to assist larger countries in achieving a higher throughput of exchanges per second.

References

[1] Al-Hamadi, Hamid, and Ray Chen. " Trust -based decision making for health IoT systems." IEEE Internet of Things Journal, vol. 4, no. 5
(2017): 1408-1419.

[2] V. Santos, J. P. Barraca, and D. Gomes. "Secure Decentralized IoT Infrastructure". In Wireless Days, IEEE, pp. 173 -175, 2017.

[3] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani,
M. Imran and M. Guizani, "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges". IEEE wireless communications, vol. 24, no.3, pp. 10 -16, 2017.

[4] S. Huh, S. Cho and S. Kim. "Managing IoT devices using blockchain platform." In Advanced Communication Technology (ICACT), 2017 19 th International Conference on, pp. 464 -467. IEEE, 2017.

[5] P. McCorry, S.F. Shahandashti and F. Hao. "A smart contract for boardroom voting with maximum voter privacy". International Conference on Financial Cryptography and Data Security. Springer, Cham, pp. 357 - 375, 2017.

[6] F. Hao, P.Y.A. Ryan and P. Zieli??ski. "Anonymous voting by two- round public discussion". IET Information Security, vol. 4, no. 2, pp. 62-67, 2010.

[7] J. Groth. "Efficient maximal privacy in boardroom voting and anonymous broadcast". In International Conference on Financial Cryptography. Springer, Berlin, Heidelberg, pp. 90-104, 2004.

[8] A. Kiayias and M. Yung. "Self-tallying elections and perfect ballot secrecy". In International Workshop on Public Key Cryptography,Springer, Berlin, Heidelberg, pp. 141-158, 2002.

[9] D. Khader, B. Smyth, P. Ryan and F. Hao. " A fair and robust voting system by broadcast". Lecture Notes in Informatics (LNI), ProceedingsSeries of the Gesellschaft fur Informatik (GI), pp. 285 - 299, 2012.

[10] T. C. Hsiao et al., "Electronic voting systems for defending free will and resisting bribery and coercion based on ring anonymous signcryption scheme," Advances in Mechanical Engineering., 2017, 9(1): 1687814016687194

[11] Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). "Star-vote: A se- cure, transparent, auditable, and reliable voting sys- tem.", in 2013 Electronic Voting Technology Work-
shop/Workshop on Trustworthy Elections (EVT/WOTE
13). Washington, D.C.: USENIX Association, 2013.

[12] Dalia, K., Ben, R. , Peter Y. A, and Feng, H. (2012). "A fair and robust voting system." by broadcast, 5th International Conference on E-voting, 2012.

[13] Adida, B.; 'Helios (2008). "Web-based open-audit voting.", in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335348.

[14] Chaum, D., Essex, A., Carback, R., Clark, J.,
Popoveniuc, S., Sherman, A. and Vora, P. (2008). "Scantegrity: End-to-end voter-veriable optical- scan voting." , IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.

[15] Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). "Bingo voting: Secure and coercion- free voting us- ing a trusted random number generator.", in Pro- ceedings of the 1st International Conference on E- voting and Identity, ser. VOTE-ID'07. Berlin, Heidel- berg: Springer-Verlag, 2007, pp. 111-124