2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress

Towards A Privacy-Preserving Voting System Through Blockchain Technologies

Rabeya Bosri, Abdur Razzak Uzzal, Abdullah Al Omar*, A S M Touhidul Hasan, and
Department of Computer Science and Engineering
University of Asia Pacific
Dhaka, Bangladesh
Email: {rabeyabosri.cse, abdurrazzakuzzal.aru}@gmail.com, {omar.cs, touhid}@uap-bd.edu
Md. Zakirul Alam Bhuiyan
Department of Computer and Information Sciences
Fordham University
New York, NY 10458, USA
Email: mbhuiyan3@fordham.edu

***Abstract*—The voting system is the process to take the opinion of people to run the constitution properly. Fairness, independence, and unbiasedness should be present in the voting system. Hence, it must be a transparent and secured process so that everybody can express their own opinion freely. Worldwide vote manipulation is an intriguing problem in existing voting systems. Since people in different countries are using digital technology in the voting process (e.g., Optical Scan Voting system, Internet Voting system, Electronic Voting system) instead of traditional way (e.g., Ballot Box). Only digitization could not solve the issues completely. Because still there are numerous ways to manipulate or tamper digital technology and hamper the voting process. To build a secure electronic voting environment, we introduce an application of blockchain technology as a service for the distributed electronic voting system. With the use of blockchain, we achieve data integrity which is a necessary attribute of a voting environment. The anonymity of the voters, privacy, and security of the voting environment is the main goal of this work. Through the design of our system and with the help of blockchain we have solved all the security issues in the voting environment.**

***Index Terms*—Voting environment, Digitization, Anonymity, Blockchain, Privacy, Security, Secure electronic voting system**

I. Introduction

Election is the process by which people can elect their representative from a list of candidates; it is the most popular way to give peoples' pronouncement. To be a democratic country a fair election is a prerequisite which gives the citizens an opportunity to provide their consent to the way the democratic government has been working [1]. Only by providing fair election authorized body may retain peoples' trust in democracy. Worldwide several voting processes are being used for the election. In the time of digital information, many countries are still using a traditional paper-based voting system which is obstructing to provide a fair election. This traditional voting system has faced several issues e.g., booth capturing, ballot paper stealing, and unfair counting.

Since paper-based voting systems have already faced several security issues therefore, different countries (e.g., Argentina, Brazil, Philippines, Australia, Italy, United Kingdom) have already moved into electronic voting machine [2]. An electronic voting machine (EVM) is introduced with the facilities of each vote to be recorded and counted with legibility and impartially. EVM also provides the ease of tabulation of ballots into result, gives more accurate and faster outcome compared with traditional paper-based voting system [3].

Though EVM comes with the solution of the problems which are raised in the traditional voting system (e.g., booth capturing, invalid vote, ballot paper stealing). But EVM still suffers from universal acceptance issues as it fails to handle some security problems [4]. EVM can be re-programmed by any corrupted election insider who may include some algorithm to count the votes fraudulently [5]. In addition, EVM memory chip (storage) could be replaced with a manipulated memory chip, by an election insider who has access to the machines which can change the voting result. The most important issue with EVM is using a centralized database as it is easy to insert some malware into the machine which would tamper the database. Considering the political culture, it is undeniably a fact that any manufacturer or company hired for the production of the e-voting system will tailor the e-voting machines according to the needs of the current political party in power. Therefore, these machines are subjected to security, distrust, and inquiry through worldwide.

Anonymity and privacy of the voters in the voting system is always a big issue. The term privacy in information security refers to the fact that data of an individual will be collected, shared, and used in a way so that no entity other than the system or who are directly involved in the process will be able to know or crack the information. And anonymity means that the user will be unknown in between any data or information transaction in the system [6]. Nowadays, these two key terms are mostly absent in the voting systems though it is being claimed to be secured. Suppose, a voting system is designed to store the votes in a secured manner that they provide the highest level of security. No one may not be able to manipulate or tamper the votes in the system. But they may not ensure voter privacy and anonymity at all. In this type

*Corresponding Author

978-1-7281-3024-8/19/$31.00 ©2019 IEEE
DOI 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00116

of system, every candidate and the authorities are able to identify the voters who have voted for which candidate. It violates the two major factor of information security that is: **Anonymity and Privacy**. The systems may be secured to store the votes but somehow they fail to provide the voters' anonymity and privacy.

To solve these above-mentioned problems, we proposed a blockchain based voting system using ethereum network. Ethereum [7] is an open blockchain platform that permits anyone to build and use decentralized applications. Blockchain is a data structure which holds encrypted ledgers with the properties: immutability, append-only, ordered, open, secure, and transparent [8]. It may call chain of blocks where blocks are denoted by digital information. Every block is made up with digital pieces of data i.e., information about transactions, who are participating in the transaction, and a unique piece of code which is called hash and every transaction is recorded on the blockchain without any third party [9]. The first blockchain was introduced in the bitcoin cryptocurrency by Satoshi Nakamoto in 2008. Proof-of-Work [10] and Proof-of-Stake [11] are the two primary ways to validate the transaction on the blockchain. In a public blockchain anyone can join and in a private blockchain (i.e., ethereum) only permitted users' can join. We incorporate the ethereum network to run the distributed voting system to store the votes. Permissioned blockchain is faster, legal and trusted [12].

In the proposed system, the election commission will create the ethereum account corresponding to the voters and their details will be stored in the ethereum network[1]. Every voter from developing countries like Bangladesh, India, Pakistan, etc. are not affordable to have a smartphone or an ethereum wallet. Therefore, it is not an optimal way to design a voting system which can only be accessible by a smartphone or an ethereum wallet. To simplify the voting process, we integrate either that means voters may cast vote from their smartphone or voters may cast vote from a designated voting center. By the smartphone, voters may easily log into their account and after the authentication process, they can cast their vote. Or, the voters who cannot afford a smartphone they can go to the voting center and after the biometric [13] authentication process they can cast their vote. In the proposed system, every voter will get a chance to change their vote before the final submission if they did any mistake. Moreover, we compromise two steps of verification before the vote is added into the blockchain, first step by the voter and second step by the consensus [14] observers by the election candidates. If any uncertain situation arises such as booth capturing, the observers may decline the vote confirmation request and no vote will be added into the blockchain. In this way, we solve the privacy and security related problems of the voting system and introduce a novel design in voting.
In this paper, a secure voting system using blockchain technology is proposed which ensures a fair election process. The main idea of our work is to keep the votes secure which are not accessible by anyone though accessing the blockchain and also maintain no voter will be able to cast a duplicate vote. Our system provides voters anonymity and privacy of voter's information, maintain the security of casted votes and accountability.

[1]Ethereum account for each voter will be provided by the constitutional body in our system. Voters need not maintain an Ethereum wallet by their selves.

Paper Organization: The remainder of the paper is organized as follows: Related work described in Section II, Section III explains our methodology and Section IV shows the working scenario of our platform. The security analysis of our system has been described in Section V and concluding remarks in Section VI.

II. Related work

Peoples interest is increasing rapidly on the blockchain with the properties of authentication and authorization on an automated information system [15]–[17]. Authentication is to identify a user of a system. On the other hand, authorization is allowing the user to perform a task, more formally it is the validation of the user permission. Blockchain becomes more popular in bitcoin cryptocurrency [18], it provides authentication and authorization in the digital currency system. Blockchain is a chain of blocks and each block contains digital information including cryptographic hashes corresponding to the previous and current block to ensure continuity and immutability of the chain [19].

Some countries currently have introduced e-voting [20] using EVM and a few countries introduced the online voting system to make the voting system easier. Other countries are planning to switch into e-voting system. A lot of research has been done to make voting systems more secure and reliable. Most of the works introduced blockchain technology as a decentralized database for online or e-voting system [21]–[24].

Yavuz et al. tried to build a secure environment for the e-voting system with ethereum network [25]. In their system, voters submit their votes through a smartphone or from their ethereum wallets. But it is very difficult to develop such a system in a developing country like Bangladesh where every voter is not able to afford a smartphone or an ethereum wallet. Shukla et al. also implemented a system by using the ethereum blockchain network [26]. In their application voters must sign up by submitting the required information and log in using the details that they gave while signing up. Voters may cast their vote only once after login. This is an issue of this system. If a voter did a mistake like vote for an unexpected candidate while voting there is no chance to rectify his/her vote. However, it does not make sure the voters' privacy as well.

McCorry et al. proposed a self-tallying voting protocol for boardroom voting in The Open Vote Network [27]. It does not rely on any trusted persons to calculate the tally. Besides, voters can control the privacy of their own vote but all voting data is publicly available. In the Open

Vote Network, anyone can register and cast their vote but it is not effective for the parliamentary voting system. Because in the parliamentary system only pre-registered and verified voters can cast their vote within a particular election zone. They cannot cast their vote in other election zones.

Shahzad et al. provide a solution on a secure e-voting system with ethereum network which deals with a hashing based system builds upon the blockchain technology [28]. In the proposed system, they did not substitute the EVM based voting system rather replace the centralized database into a distributed database by using blockchain. However, the proposed system cannot deal with the problem of booth capturing. It will be a problem if the voting center is occupied by the fraud people and they could force the voters to vote for a particular candidate. Their system provides secure storage for storing the votes but do not provide a secure environment for vote casting.

III. Methodology

In this section, we present the architecture as well as the design view of the mechanism.

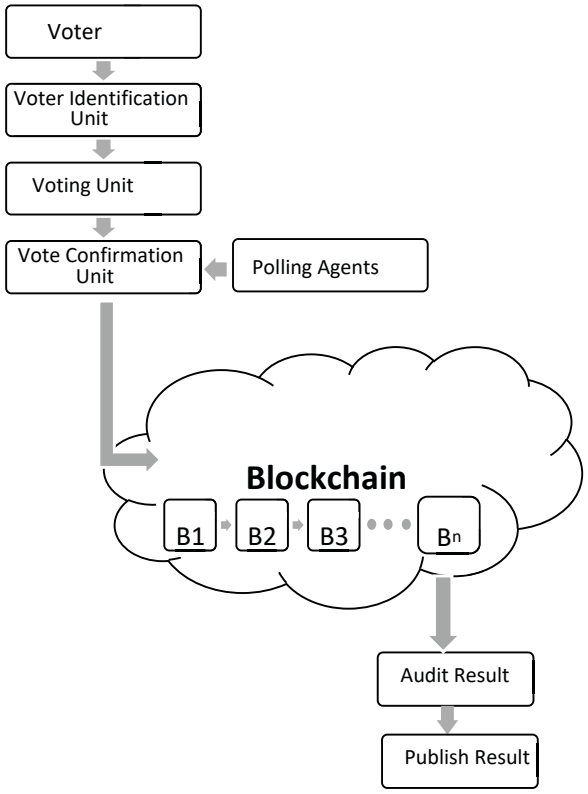

Figure 1. A secure voting environment based on blockchain

A. Entities of voting protocol

In the proposed system, we consider Bangladesh as a case study. The voting process is executed in a way that it deploys many electoral personnel at different levels. Table I describes the notations used in this paper. Figure 1 illustrates the entities of the voting process are described here:

TABLE I
Terminology table

Notation	Description
V	Set of Voter
EC	Election Commission
AU	Voter Authentication Unit
VU	Voting Unit
VVU	Vote Verification Unit
A	Set of Polling Agent
BC	Blockchain
P	One Time Password

*a) **Election Commission** (EC):* Election commission manages the life-cycle of the election. Election commission is defined as EC. EC creates election, activate the election and close the election after a fixed time period. During the voting process, EC observes the whole voting process and publishes the result after the election is over. Another important task of EC is to create the voter list through a voter registration process before the election. EC stores v_i's personal information. EC is considered as a trusted entity in the proposed system who ensures the v_i's details to be tamper proof. EC adopts different personnel from the polling station to the constituency (e.g., the returning officer, the assistant returning officer, presiding officer, an assistant presiding officer, and polling officer).

i. Returning officer: They collect the voting machines from the EC before the election starts. Returning officer consigns the voting tools to the assistant returning officer.

ii. Presiding officer: Each polling station is administrated by the presiding officer who is assisted by an assistant and some other staffs. The assistant returning officer provides all voting tools and the v_is' list to the presiding officer.

*b) **Voter** (v_i):* Voter set is defined as V. v_i is a person who has the legal right to vote and also included in the v_i list of his particular area. v_is list is provided and updated by the EC.

$$V \subset [v_1, v_2, v_2, ..., v_i]$$

In the system, v_i can cast their vote either by going to the voting center or online using the internet. For online voting v_i need to authenticate themselves first, then load election ballots, cast their vote and finally espy the result after the election is over. On the other hand, v_is who wants to cast their vote from a voting center, they must go to the voting center with his/her National Identity (NID) Card and after passing the authentication process they can go through the voting process.

*c) **Voter Authentication Unit** (AU):* v_i authentication unit is a trusted entity in the system and defined as AU who authenticates the v_is. To cast a vote v_i must authenticate himself as a real v_i who is included in the v_i list of his election area. This authentication process is done by the AU. Two different types of authentication process are used for online and offline voting. In the voting center biometric authentication system is used to authenticate the

v_is. And for online voting v_is are authenticated by logging into the voting system using their username and password. All the v_is authentication information are provided by the EC to the AU.

*d) **Voting Unit** (VU):* VU provides the voting phase with the v_is and it is defined as VU. Every real v_i is able to cast his vote into this unit. VU is not able to add the votes into BC, it sends the vote verification request to VVU.

*e) **Blockchain** (BC):* In the system blockchain is defined as BC. Only permitted v_is can use their ethereum accounts which are created by the EC, to cast their votes.

*f) **Polling Agents** (A):* Polling agents are the representatives of the candidates who are connected with VVU. In the system, agents are fully anonymous to the v_is and are not identifiable except EC, and v_is are also anonymous to the agents. Agents set is defined as A and their job is to verify the votes.

$$A \subset [a_1, a_2, a_3, ..., a_i]$$

A are verified by the EC and their profile is designed with their party symbol. If a particular A continuously rejects the real votes then that particular A will be blocked by VVU that means, that A will not ask for vote verification anymore.

*g) **Vote Verification Unit** (VVU):* Vote verification unit is defined as VVU. A and VU are connected with VVU. The main job of this unit is; forwards the vote verification request from VU to the a_i, and confirmed votes are added into BC by this unit. To deal with the problem when a_i rejects a vote, VVU establishes a connection with the presiding officer. After receiving the feedback from the officer, VVU makes the decision either the vote is added into BC or not.

IV. Formal description

Figure 2 demonstrates how the proposed system works. The whole voting process is divided into three units; VU, AU, and VVU. While the authentication process is going on, AU have introduced electoral personnel and during the vote verification process, VVU has introduced A with the system. We are assuming that electoral personnel is fair and aware of their duties and EC monitors the election from the start to the end. At every voting center, presiding officer plays an important role, to identify the v_i when any a_i rejects the vote confirmation request.

1) Voter authentication and vote casting: v_i's authentication is done in two different ways for two different categories online and offline voting.
Figure 3 presents the online v_i authentication process. The v_is who are unable to go to the voting center they can easily cast their votes using an smartphone from their suitable place. To cast a vote v_i must log into the voting system using their corresponding username and P which are provided by the EC. Unique username for every v_i is their NID number and Ps are generated

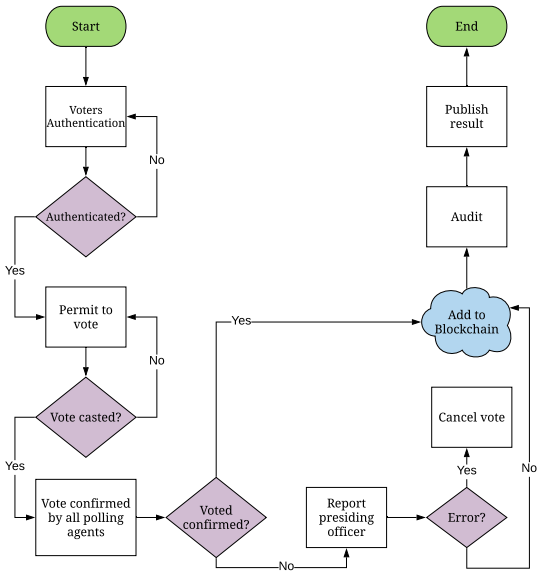

Figure 2. Overall voting process in flow diagram

using a random function. Ps are sent to every v_i's corresponding mobile number before the election starts.

$$\text{Random}(v_i)=P$$

After entering v_i's username and P, AU will ask for a secret code from the v_i. The secret code is generated by the AU and send to the v_i's mobile number after entering his/her username and P. v_i can enter to the system only if he/she provides the correct code. AU identifies the v_i as a real v_i and open a new block to get himself/herself into the voting phase.

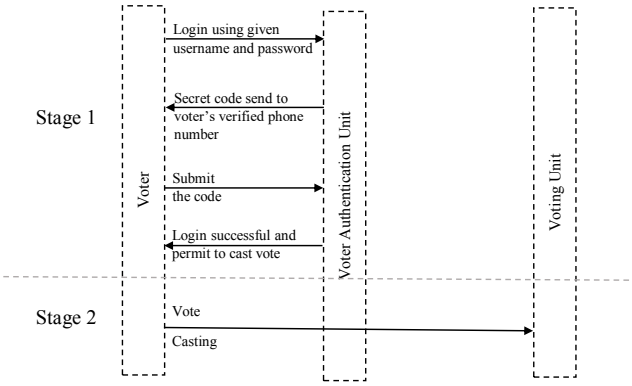

Figure 3. Low level view of online voter authentication and vote casting

Figure 4 illustrates the offline voter authentication process. The offline v_i authentication process is done with the electoral personnel. In the first step, v_i is requested to show his/her NID card to the assistant presiding officer then assistant presiding officer will check the v_i's details with the database. After checking the details v_i gets the permission for a biometric authentication process. In the proposed voting system, we are using v_i's fingerprint for the biometric authentication. If the v_i passes this

authentication stage, then he/she will be able to get into the voting phase. More formally, while the fingerprint matches with the database, a new block will open for the corresponding v_i to cast his/her vote.

The authentication process for online and offline voting is different but the voting process is the same for both. The voting page is designed with the candidates' name along with the party's symbol and the v_i is able to cast the vote at their will. Before submitting a vote, v_i will be asked for a confirmation of the vote. If v_i makes any mistake to select the favorite candidate, in this stage v_i can rectify it and do the final submission.

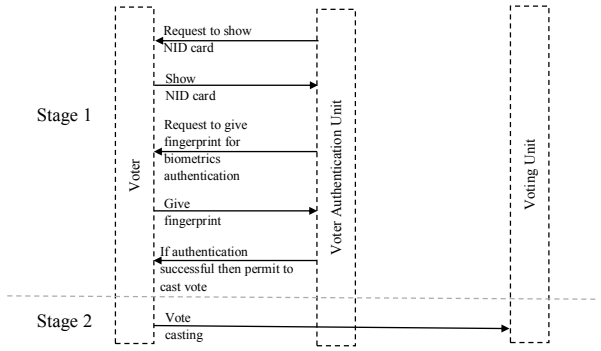

Figure 4. Low level view of offline vote authentication and vote casting

2) Vote verification and vote adding into Blockchain: Before adding the vote into BC it must be verified by the a_i. To ensure that the voting center is free from any unauthorized activities a_i verifies the votes. When a v_i submits the vote it will not be appended into BC directly. To record the vote into BC, the vote needs an acknowledgment from A. Verification request is sent to every a_i from VVU after every vote. When each a_i accept the request only then the vote will be appended into BC. When a real v_i submits his vote, there may occur two cases, i. all a_is accept the confirmation request, ii. a dishonest a_i reject the confirmation request.

Figure 5 shows the low-level view of vote verification and vote adding on the BC. VU ask for verification from VVU. VVU forwards the request to every a_i.When each of the a_i confirms the request then the vote will be added into BC. More formally, VVU seal the block and it will be added into the chain.

Figure 6 presents the low-level view of the rejection of a vote by a dishonest a_i when the v_i is a real. In this case, VVU sends a notification to the presiding officer. After receiving the notification, the presiding officer will check the v_i credential again and sends an acknowledgment along with the v_i to the VVU. VVU add the vote into BC as it receives an acknowledgment from presiding officer. On the other hand, when every a_i rejects the vote, the vote will be canceled automatically.

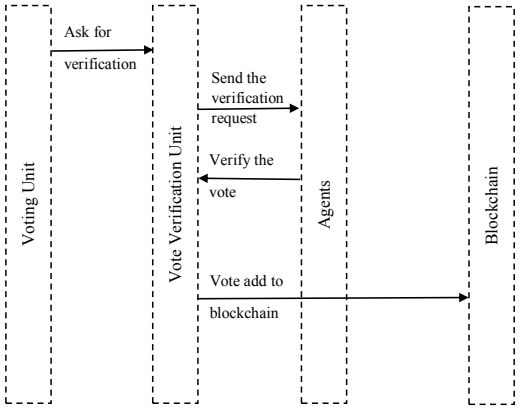

Figure 5. Low level view of vote verification and vote adding to Blockchain

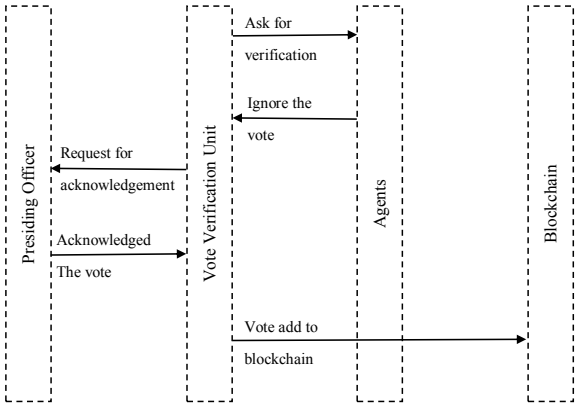

Figure 6. Low level view of vote verification and vote adding to Blockchain

V. Security Analysis

Integrity: Integrity for this system is to preserve the accuracy and ensure consistency of votes throughout its life cycle (voting period). In order to achieve integrity, the scheme uses blockchain to store the votes. Blockchain technology introduces Merkle tree to ensures data integrity [29]. The concept of Merkle tree has been introduced in ethereum to allow a compact and efficient verifiable proof which ensures that a transaction is included in a block. Every block in ethereum contains three Merkle trees for three kinds of objects; transaction, receipts (pieces of data showing the effect of each transaction), and state. In this data structure, hashes of child nodes are combined together into the parent node's header. This technique of combining the child nodes' headers and adding it to the header of the parent node continues iteratively until it reaches the final node, right at the top, the root node. Thus, the root node will contain information about all of the nodes present in the tree. Hash of all the transactions in a block is stored in the Merkle tree. Therefore, if a node wants to verify whether or not a transaction has been changed, the nodes

need to only build the Markle tree using all the transaction of the block. This makes it very simple to validate or invalidate a transaction. This proposed system is using BC as a storage therefore, this scheme ensure data integrity.

Security: The proposed system provides security by protecting the votes from unauthorized access and manipulation. Due to the immutable attribute of BC; it is quite impossible to manipulate the information (votes) which are recorded on BC [30]. If anyone changes a transaction, he will have to re-mine all the blocks' information from that block till the current block. Every block contains a unique hash using a hash function and the hash of the previous block. Since one wants to manipulate the data of a block, this change will result in a different hash value. New hash value will conflict with the value which is stored in the next block. Thus, the next block will also have to be re-mined. The same process of re-mining is needed for all the blocks in the chain. While the miner is busy in re-mining old blocks, there will be new blocks getting added to the chain, which makes the data manipulation of a single block extremely difficult. The computation power required to achieve this is enormous and close to impossible in real life. Blockchain ensures us, votes are tamper proof and it is quite impossible to manipulate the votes in our system.

Anonymity and Privacy: The proposed system offers anonymity and privacy to the v_i. In the voting system, v_is' entry into the VU is done in an anonymous manner. The AU and VU are two different units. After the authentication, permission for creating a block is granted. After adding the vote into the block, no one can track back to find out the user who has created the block. In the system, from the block creation to the vote adding all are done by the v_i, no other entities in our system (e.g., presiding officer, agent, returning officer) are capable to find out the v_i, who created the block. In zero knowledge transaction, the EC and other parties only know that a valid vote has taken place, but nothing about the voter choice of selection [31]. Another important issue is; A are also anonymous. In many countries A are beaten or threatened by the dishonest political peoples but in the proposed system A are anonymous. A are verified by the EC and only the candidates know the details about their A.

VI. Conclusion

Maintaining security in the voting system is a big challenge for many countries. To ensure a fair election people are moving from paper-based voting system to the electronic voting system, on the other hand, many countries have already lost their trust from electronic voting. In our proposed system, we introduced a blockchain based voting system which provides a secure and trusted election while guaranteeing voters privacy. The main problem in the existing voting systems is using a centralized database, instead of a centralized database we introduced blockchain as a de-centralized database which is more secure and reliable. Our system also deals with the problems which are raised in EVM.

References

[1] O. Cetinkaya and D. Cetinkaya, "Verification and validation issues in electronic voting." *Electronic journal of e-government*, vol. 5, no. 2, 2007.

[2] S. Kumar and E. Walia, "Analysis of electronic voting system in various countries," *International Journal on Computer Science and Engineering*, vol. 3, no. 5, pp. 1825–1830, 2011.

[3] D. A. Kumar and T. U. S. Begum, "Electronic voting machine—a review," in *International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012)*. IEEE, 2012, pp. 41–48.

[4] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp, "Security analysis of india's electronic voting machines," in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010, pp. 1–14.

[5] D. F. Aranha, M. M. Karam, A. de Miranda, and F. B. Scarel, "Software vulnerabilities in the brazilian voting machine," in *Design, development, and use of secure electronic voting systems*. IGI Global, 2014, pp. 149–175.

[6] A. Hasan, Q. Jiang, H. Chen, and S. Wang, "A new approach to privacy-preserving multiple independent data publishing," *Applied Sciences*, vol. 8, no. 5, p. 783, 2018.

[7] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[8] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, pp. 6–10, 2016.

[9] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[11] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, 2012.

[12] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, 2016.

[13] D. A. Kumar and T. U. S. Begum, "A comparative study on fingerprint matching algorithms for evm," *Journal of Computer Sciences and Applications*, vol. 1, no. 4, pp. 55–60, 2013.

[14] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.

[15] M. A. Tasnim, A. Al Omar, M. S. Rahman, and M. Z. A. Bhuiyan, "Crab: Blockchain based criminal record management system," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*. Springer, 2018, pp. 294–303.

[16] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *International conference on security, privacy and anonymity in computation, communication and storage*. Springer, 2017, pp. 534–543.

[17] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Generation Computer Systems*, vol. 95, pp. 511–521, 2019.

[18] M. Iwamura, Y. Kitamura, T. Matsumoto, and K. Saito, "Can we stabilize the price of a cryptocurrency?: Understanding the design of bitcoin and its potential to compete with central bank money," 2014.

[19] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

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

[21] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," *International Journal of Network Security & Its Applications*, vol. 9, no. 3, pp. 01–09, 2017.

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

[23] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based e-voting system," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, 2018, pp. 983–986.

[24] J. Li, X. Wang, Z. Huang, L. Wang, and Y. Xiang, "Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing," *Journal of Parallel and Distributed Computing*, 2019.

[25] E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. IEEE, 2018, pp. 1–7.

[26] S. Shukla, A. Thasmiya, D. Shashank, and H. Mamatha, "Online voting application using ethereum blockchain," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2018, pp. 873–880.

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

[28] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE ACCESS*, vol. 7, pp. 24 477–24 488, 2019.

[29] B. Rogers, S. Chhabra, M. Prvulovic, and Y. Solihin, "Using address independent seed encryption and bonsai merkle trees to make secure processors os-and performance-friendly," in *Proceedings of the 40th Annual IEEE/ACM International Symposium on Microarchitecture*. IEEE Computer Society, 2007, pp. 183–196.

[30] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.

[31] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.