





Blockchain-Based Secure E-Voting with the Assistance of Smart Contract



Kazi Sadia , Md. Masuduzzaman , Rajib Kumar Paul ,
and Anik Islam 

Abstract Voting is a very important issue that can be beneficial in terms of choosing the right leader in an election. A good leader can bring prosperity to a country and also can lead the country in the right direction every time. However, elections are surrounded by ballot forgery, coercion, and multiple voting issues. Moreover, while giving votes, a person has to wait in a long queue and it is a very time-consuming process. Blockchain is a distributed database in which data are shared with the participant of the node and each participant holds the same copy of the data. Blockchain has properties like transparency, pseudonymity, and data integrity. In this paper, a fully decentralized e-voting system based on blockchain technology is proposed. This protocol utilizes smart contracts in the e-voting system to deal with security issues, accuracy, and voters' privacy during the vote. The protocol results in a transparent, non-editable, and independently verifiable procedure. The protocol discards all the intended fraudulent activities occurring during the election process by removing the least participation of the third party. Both transparency and coercion are obtained at the same time.

Keywords Blockchain · E-voting · Hash · Security · Smart contract

1 Introduction

1.1 Blockchain

Blockchain is essentially a distributed database of records or a public ledger of all transactions or digital events that have been occurred and shared among participating

K. Sadia · R. K. Paul

Department of Computer Science and Engineering, American International University-Bangladesh, Dhaka, Bangladesh

Md. Masuduzzaman · A. Islam (✉)

Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, South Korea

e-mail: anik.islam@kumoh.ac.kr

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer 161
Nature Singapore Pte Ltd. 2020

D. Patel et al. (eds.), *IC-BCT 2019*, Blockchain Technologies,
https://doi.org/10.1007/978-981-15-4542-9_14

parties connected within a network [1]. A blockchain is a chain of blocks where blocks are connected to hold data or information regarding any event [2]. Each transaction or activity within the blockchain is verified by consensus of a majority of the participants (i.e., without the approval of the majority network, no activity is acceptable) [3]. Once some data have been inserted into a blockchain, it becomes very difficult to change it due to having an immutability configuration [4]. To rewrite any data, dishonest miners must rewrite the previously broadcasted block and these changes have to be agreed by the other miners in the network [1].

In the blockchain, double spending is prevented by using “proof of work” that requires computer processing power to generate fingerprints to uniquely identify each block [1]. Blockchain technology uses cryptography which ensures the legitimacy of a transaction [5]. Third-party involvement is prevented by the peer-to-peer network validation. Therefore, cost and trust-related issues are resolved [6]. The structure of a block in the blockchain is described below.

Data—The data can be any type of information that is stored in the block.

Hash—The hash is a kind of fingerprint that uniquely identifies a block and is generated based on its contents.

Hash of the previous block—It refers the previous block to form the chain. Any change in data can change the hash of the block.

According to Fig. 1, when a participant intends to add a block to the chain, the peer nodes are responsible for validating the block. After the verification, if the majority agrees to add the block, then the block is added to the blockchain [7]. If the majority denies, then block is discarded.

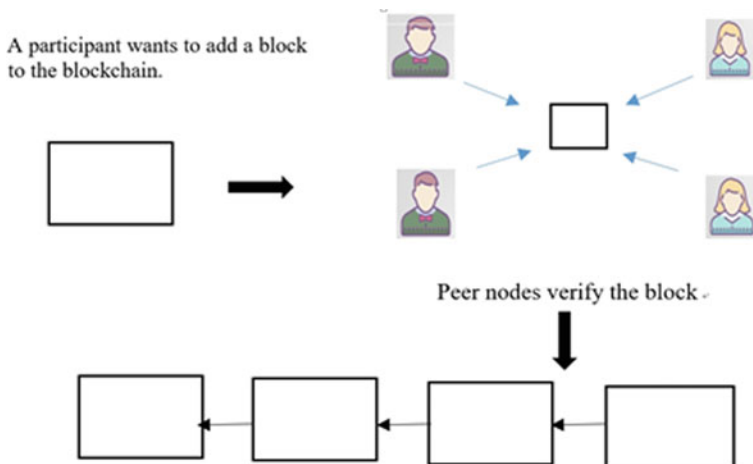


Fig. 1 Mechanisms of adding a block in blockchain

1.2 E-Voting

In democracy, the main important thing is to secure the election process for the national security and development of a nation. Ever since the candidates were needed to be elected through a democratic process, it was done by voting with pen and paper. Afterward, the result was counted manually and declared. The process of voting with paper ballot and pen required a lot of time and created hustle in maintaining a long queue. Also, the manual process ensues with ballot forgery, coercion, and multiple voting. Now, replacing the traditional process of voting by a new innovative process might be condemned in stopping any sort of duplicity and forgery [8].

E-voting is the new concept proposed to ensure fair and digitalized voting that promises to resolve all the issues related to the traditional voting process. By electronic voting, we generally mean the vote casting process with the help of any sort of computer or computerized voting equipment or the Internet. The tasks are conducted through systems to hereby reduce the involvement of manpower during the election process. Registering the voters, tally ballots, and recording of votes can also be easily done by this electronic system [9].

Electronic voting machine is neither a complex machine nor a harder one to operate. It can be easily understood and operated by both the election officer's in-charge and the voters. EVM has basically three units—control unit, display unit, and ballot unit. The main unit of EVM is a control unit that stores all the data and controls the basic function including voter information. Vote counting is assuredly conducted with possibly less time and accuracy.

1.3 Smart Contract

Previously, contracts between parties were held upon visual meetings. The smart contract is aimed to provide contracts between parties where both parties are given the priority and contracts are conducted upon establishing the conditions of both parties [4]. It is the executable code that runs on top of the blockchain to facilitate the terms required in an agreement of a contract between the two parties. The involvement of any third party is resolved as any medium between parties is not required as contracts are self-executed.

A smart contract is a legal application that runs on a blockchain network [4]. Smart contracts are much like legal contracts. The smart contract can be used in many different things. Banks, for example, could use it to issue a loan, worth for automatic payments, both e-commerce and music rights management can use this. An insurance company could use it for process claims; postal companies use it for payment on delivery and so on.

- No trust issue in a smart contract just like this vendor machine, as shown in Fig. 2. A person itself can put the coin into this and get the desired product.

Fig. 2 Example of smart contract



- No involvement of the third party: the same as this vendor machine. When a person itself involved with this matter can directly interact with it and get the desired product. Moreover, there is not any involvement of third party.
- As the smart contract is distributed in an open ledger, there is no chance of losing or hacking as in an open environment. It is difficult to involve in and manage to steal stuff.

The remaining sections of this paper are organized as follows: Sect. 2 represents related works. In Sect. 3, the proposed scheme is depicted. A security analysis based on different properties is outlined in Sect. 4. Finally, Sect. 5 draws a conclusion from this paper.

2 Related Work

There has been a lot of work on blockchain-based e-voting using cryptography, signatures, and other techniques. In such papers, minimal involvement of the third party observed is significantly less and a problem of coercion and transparency maintenance at the same time is also observed. Additionally, the balancing of transparency and coercion resistance was a possible future work in [10]. Reduction of third party is a major portion of work in an election process as the impact of third-party involvement can have a vulnerable effect on the whole procedure. Moreover, coercion resistance is a difficult task that is to be mapped with transparency.

Lewis et al. [1] described blockchain as an open, distributed ledger of historical records that uses cryptography and digital signatures. In his paper, he also mentioned the logic of blockchain and how does it work. Upon explaining the aftermath of resolving conflicts, he introduced an idea of not broadcasting a block intentionally. Two blocks can be created, and one can be left as being not broadcasted. The un-broadcasted block can be broadcasted when desired. In this paper, we have used this concept to keep the choices of nominees secured until result calculation.

Liu et al. [10] proposed a protocol where the choice was made safe using a random string and choice code. The length of the vote string varies depending on the election requirements. The choice code represents the voter's choice followed by a random string which is an indication of a well-formed vote. According to Liu et al. [10], the phases are pre-voting phase, voting phase, post-voting phase. In the pre-voting phase, the organizer Bob collected all valid ballots. After ending the voting time, Bob generates a set of all ballots which means all the ballots that have been received. Then Bob runs this algorithm 1:

Algorithm 1 To Obtain All Valid Ballots

Input: *AllBallots*: the set of all ballots Bob has received

Output: *ValidBallots*: the set of all valid ballots

```

1: for each  $b \in \text{Ballots}$  do
2:   if  $\text{isCorrectFormat}(b) \ \& \ \text{hasAllSignature}(b) \ \& \ \text{isCastOnTime}(b) \ \& \ \text{hasNotBeenCounted}(b)$  then
3:      $\text{ValidBallots} \leftarrow \text{ValidBallots} \cup \{b\}$ 
4:   end if
5: end for

```

This algorithm runs to gain a set of valid ballots which is set of all the valid ballots.

There are issues regarding an election. Therefore, voters' privacy must be assured. Thus, the concept of public and private keys is used in different papers but with a little modification. Anonymity was ensured by keeping voters' identity private [10, 11]. According to Liu et al. [10] and Hardwick et al. [11], one must authenticate oneself to the central authority (CA) and CA receives a token that proves one's eligibility to vote. In these papers, one central authority or an officer is responsible for initial verification.

The counting phase described in the protocol discussed by Hardwick et al. [11]. Hardwick et al. [11] deal with broadcasting a ballot opening message that contains a value which will represent the voter's choice and the voter's themselves broadcast this. Hardwick et al. [11] stored the information of the list of candidates and voters in the genesis block as the initial storage. The authors revealed the result at the end of the election using the concept of value representation of the voter choice. A voter can vote multiple times, and every time the previous vote was replaced by the current one. By this process, coercion is said to be totally removed. In both the papers, everyone can view the public blockchain and there is no centralized authority. In [12–17], they also proposed a voting mechanism which utilizes blockchain.

3 Proposed Methodology

3.1 Procedure

The basic functionalities of the proposed protocol are shown in Fig. 3. The code is executed on top of the blockchain. Therefore, verifying actions that were supposed to be performed by the third party are performed automatically. Moreover, the peer network connected is in-charge of further verification as mentioned. The figure introduces some unknown terms that are further described below.

Condition 1—Verify whether the voter is in group X and the flag of X is true. Also, check whether the voter is on the eligibility list or not.

Condition 2—Mathematical computation (proof of work) is done. Also, verify whether the voter has cast vote previously or not and check the ballot is in the correct format or not.

Organizer—In this protocol, the organizer is the only representative who is involved within the protocol but for a limited time. The role of the organizer is to arrange and collect the list of nominees, list of eligible voters, start date and time, end date, and time. The start and end (date and time) are decided and announced by the election commission. The list of eligible voters is collected through manual registration.

Ballot string—The string that contains the choice of nominee hidden around random numbers to avoid recognition.

Sibling block—A block that contains the arrangement of choice value.

st—ST—Start Time

et—ET—End Time

Hash (fingerprint)—a hash function that used on the binary value of the voter's fingerprint.

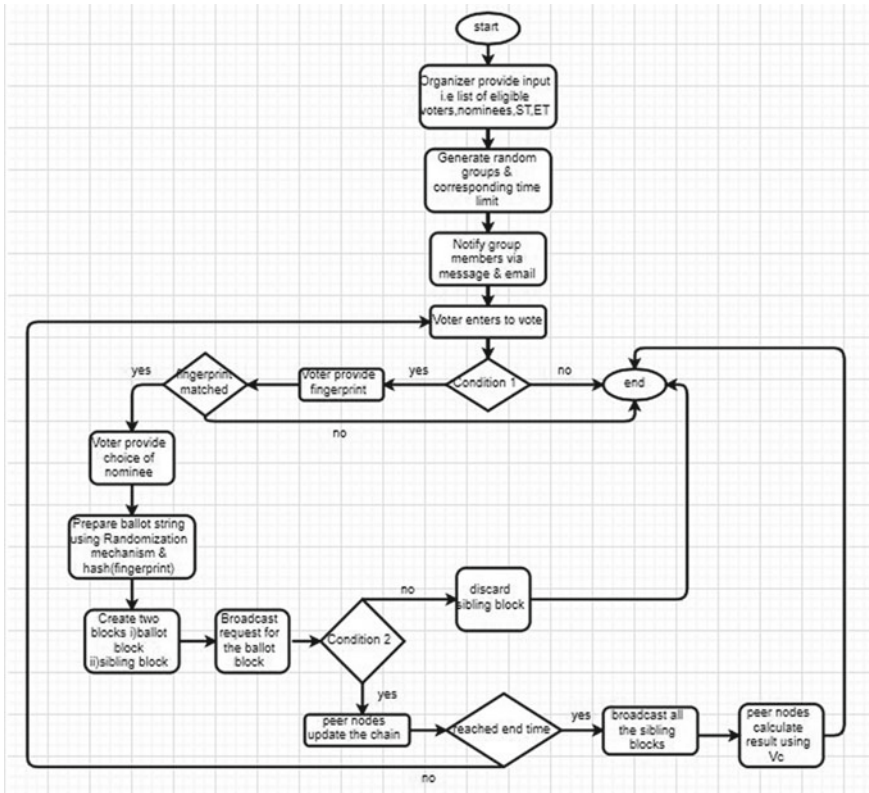


Fig. 3 Flowchart representation of the basic functionalities of the protocol

Note: The choice of nominee is hidden in the ballot string. The arrangement of the choice is hidden in the variable V_c . The arrangement is prepared by random number generation. Thus, nobody has any idea of the voter’s choice until the end of the election.

3.2 The Phases of the Proposed Protocol

The protocol is categorized into three phases, in which each phase is dependent upon another. Following are the three phases:

1. Pre-voting phase.
2. Voting phase.
3. Post-voting phase.

1. Pre-voting phase

The organizer is responsible for collecting the list of the eligible voters and nominees based on the desired condition (if any). The list of the voters should contain voters' names, national identification numbers (NID), fingerprint, and any other information based on the direction of the election commission. Organizer provides the list of eligible voters, and their fingerprint coordinates along with the binary value, nominees, start date–time, and end date–time as an input on the genesis block. In the case of people having a problem, an alternative option is considered. A priority list is maintained. In the priority list, the thumb is given the priority and people deprived of thumb can use the grooming finger. For worst case, message verification process can be used. In that process, a pin code is sent to the particular contact number of the voter and the voter has to provide the pin to verify himself as an alternative of the fingerprint. Genesis block is the parent block or the first block of the blockchain. The start date–time and end date–time are mentioned earlier by the election commission. The role of the organizer ends here; as per the result of the code execution, the procedure is carried out. The program (code) is previously integrated within the blockchain as per the concept of smart contract. On reaching the start date–time, one of the pre-defined conditions fulfills (i.e., {if (DateTime.Now==st) start ();}; a function is called which invokes the election procedure to start and corresponding activities are performed). Voters are grouped randomly based on the number of eligible voters. Moreover, other conditions are also provided and random time is generated for each group. Each group holds distinct timing; overlapping is not taken into consideration. Voters of specific groups are notified via email and message; a time limit is set for each group.

<p>Group-A</p> <p>Time: - 10:00 am – 12:00 pm</p> <p>flag=true</p>

[After 12:00 pm, the flag automatically becomes false, so further voting from that group is not acceptable.]

The flag is a Boolean property of a group. The flag remains true until the time limit of the specified group expires. The duration of each group is also decided by the election authority. The voting duration for each group must be adjusted in such a way that none of the voters skip to vote due to load/traffic on the network. No one is allowed to vote after the flag becomes false (i.e., the time limit exceeds). The flag becomes false automatically once all the voters within the group are done with their voting which provides further security.

2. Voting phase

As the voter approaches to voting providing his/her public keys, it is verified (within the code) whether the voter is in the group with a flag value of true and whether the voter is in the eligibility list. As a smart contract performs an executable code, it is verified through the code by the call of a function that checks whether the voter

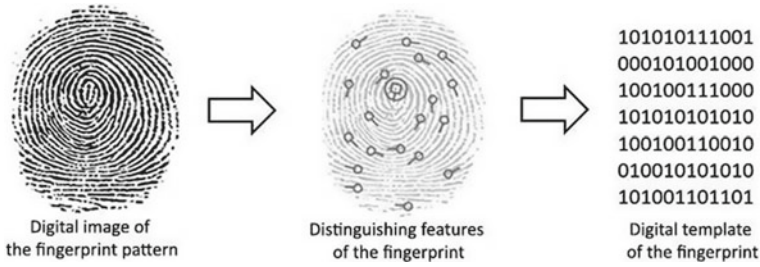


Fig. 4 Conversion of the fingerprint pattern to the binary value

entered is eligible or not. Given that, the eligibility lists of the voters are stored on the genesis block. As the voter has proved him/her as eligible, and also, the voter is in the specified group (the group to serve currently); the voter is then to provide his/her private key (fingerprint which is converted to binary data, as shown in Fig. 4); as a need of verification that no other people except the voter is casting his/her vote. This reduces the chance of anyone knowing one’s public keys and using the public key to cast vote in the name of the voter. This is the second phase of verification of voters. The fingerprint is matched with the one provided along with the eligibility list in the genesis block. The fingerprint sensor is used to figure out the coordinates of particular voters. The coordinates are then matched with the coordinates provided in the genesis block. If it matches then, according to Fig. 4, the binary value of the coordinates is obtained from the provided list in the genesis block. Conversion of the coordinates into the binary value during the voting process will require time and memory consumption. Thus, this procedure is performed. The hash of the binary value is the unique voter identification in the ballot within the block. Direct voter’s identity is avoided to ensure the voter’s security. The hash ($\text{fingerprint}_{\text{binary}}$) value is the representation of the voter in the block. SHA-256 is used as the secured hash function, $\text{hash}(\text{fingerprint}_{\text{binary}})$ that cannot be reversed. According to some research, fingerprint is one of the most secure metadata of a person. Thus, fingerprint is used instead of any other metadata in this protocol.

The voter is then provided with the list of nominees each represented by a logo. The voter then selects his/her choice of nominee. The nominees are represented by their representative logo. The logos have a binary value which is basically selected and worked with when chosen. The calculations and workings are done upon distinct binary values. Figure 5 shows an example of the representation. The number of 1’s and 0’s in representing the nominees must be the same. Otherwise, it is possible to guess the choice of nominee in the ballot string. Upon several workings, it has been seen that an unequal number of 0’s and 1’s for every nominee may result in the prediction of the selection of a nominee. As a result, the progress of the election is made visible. If the representations do not remain consistent or if it is not possible to allocate different representations of nominee within (N) bits, then increase the number of bits to get different representations for equal numbers of 0’s and 1’s. For example, three bits with two 1’s and a 0 will have representations—110,011,101.

Fig. 5 Binary representation of nominee logos

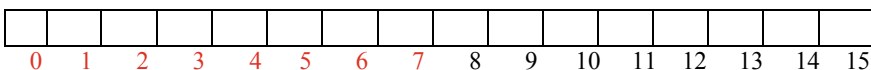


Therefore, three logos can be represented by these in other words three nominees can be represented.

On choosing the nominee, the preparation of the ballot takes place. A ballot is designed to have a ballot number in it. The ballot consists of the voters’ hash ($\text{fingerprint}_{\text{binary}}$) and the ballot string. The ballot string is prepared by the execution of a function inside the code with the concept of smart contract. The ballot string must be different for every voter. The ballot string has two substrings, such as choice string and the random string. The choice string consists of the nominee choice hidden within other randomly generated values. The random string is randomly generated 0/1 values. These techniques are used to prevent viewers from recognizing the choice of nominee. A nominee might get multiple votes. Therefore, to distinguish every ballot strings the concept of random string is used. Generation of the random string results in unique ballot string formation. The ballot string is prepared in two phases, and the following are:

Note: The total number of bits has no restriction. 16-bit is just an example. Greater number of bits is more secure as chances of similar generation of random number decrease. The decision of the number of bits must be taken into consideration before making the decision.

Let us consider a 16-bit ballot string of which 8 bits are choice string (i.e., the red ones) and 8 bits are random string (i.e., the black ones). The ballot string is equally divided into these two parts.



- (i) If n bits are representing each logo, then n random numbers are generated from 0 to 7 as the choice string is between 0 and 7. The binary value of the logo is arranged in the generated random value indexes of the ballot string (i.e., Alice chooses the nominee with a binary value of 1100 and the binary value consists of four bits. Thus, four random numbers are generated to hide the choice of Alice).

Number of bits is representing each logo—4
 Random numbers—4,5,7,0 (4)— V_c —opening value

Nominee choice—a binary value of logo—1100

Therefore, the four randomly generated numbers—4,5,7,0 are the indexes to hide the binary value of the nominee’s choice. The value is assigned sequentially.

0				1	1		0								
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

- (ii) Generate another number between 1 and 0. Fill that number in the other four indexes. Example-1

0	1	1	1	1	1	1	1	1	0						
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

The other indexes of the choice string are assigned with either 1 or 0. However, all the other indexes of the choice string must have the same value to avoid recognition of the choice.

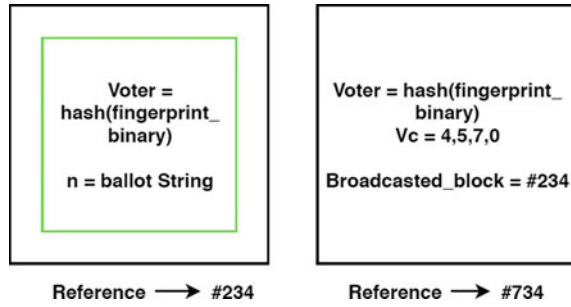
- (iii) Generate random numbers randomly between 1 and 0 and put on the indexes (8–15) suppose—11001010

0	1	1	1	1	1	1	1	0	1	1	0	0	1	0	1
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

As 8–15 is the random string part of the ballot string, eight random numbers either 1 or 0 are generated and assigned sequentially to distinguish each ballot string. The ballot string is prepared, and the choice is hidden inside the string. The choice is recognized by the V_c only. Dispose of the V_c can only be result in the consideration of the vote. One block is created containing the ballot, and another sibling block is created that consists of the voters’ hash (fingerprint_{binary}), the reference number of the broadcasted block, its own reference number, and the opening value of the choice (i.e., in this case—4, 5, 7, 0). Figure 6 shows the arrangement.

As the voter casts the vote (i.e., the voter broadcasts the ballot containing block), the ballot containing block is requested to add in the chain, whereas the sibling block remains un-broadcasted. The peer nodes start to work for the proof of work for the block. The one, who complete the puzzle, verifies whether the voter has cast vote earlier and whether the ballot is in a correct format. After all the verification, the ballot contained block is added in the blockchain and other peer nodes verify and update their chain. Majority is taken into consideration. If majority disagrees, then the block is discarded.

Fig. 6 Blocks in the blockchain



3. Post-voting phase

Once the ending time is reached, it is checked whether all the voters have voted or not. If not, then they are shortly given a notification to complete their voting within the specified time. Their voting is performed similarly as per the voting phase; but if they fail to do so, then no consideration is taken to be granted. If all the voters are done with their voting, then as instructed in the contract, all the sibling blocks are broadcasted one by one sequentially. Once all the sibling blocks are broadcasted, the peer nodes start to calculate the result referencing the blocks and using the V_c to extract the choice of nominee for every block. Here, all the nodes are supposed to come up with the same result as no blocks are discarded unnecessarily in between and the blockchain supports no changes. Therefore, the voters, in other words, the peer nodes themselves count the votes and broadcast the result preventing the need for counting using third party. The blockchain is transparent, and the accuracy is ensured as everything is made visible.

4 Security Analysis

In e-voting, security is the main concern that must be taken into consideration at first because if the voters are not assured of their safety, then they are not going to involve in the protocol. The following are the certain security goals that can be satisfied with our proposed methodology.

4.1 Anonymity

This protocol uses public and private keys of a voter during the process execution. On the blockchain, only the voter's public key is broadcasted which is hashed previously. Therefore, by excluding the voter's actual identity, no one will be able to recognize any voters within the blockchain. The only identity of voters is the hash of fingerprint that is the binary values of the coordinates.

4.2 Voters' Privacy

Voters are not aware of their timing to vote. Therefore, the chances of manipulation and coercion by fraudulent supporters are reduced. The timing of the voters' voting is only kept within the randomly generated time against each group in the code executed. As a result, manipulators or the party-specific public cannot blackmail or threaten voters.

4.3 Confidentiality

Confidentiality is equivalent to part of privacy. The prevention of sensitive information from reaching unauthorized users while making sure that the right people are aware of it. The most common method ensuring confidentiality is a data encryption, and in this protocol, the data are the voter's identity and the ballot string which is encrypted and can only be made visible to all the participants once the election process is over. Being concerned about the voter's identity, only the voter themselves are aware of their identity and choice. The ballot string is prepared in such a way that without the V_c , and the choice is not understandable. Once the sibling block is broadcasted, the choices are visible to all the peer nodes within the network.

4.4 Ballot Manipulation

In this protocol, inappropriate ballots (i.e., one voter voting more than once) is prohibited by the rejection of the approval of the peer nodes. Upon verifying, the peer nodes reject the ballot and are not further added to the block. Ballots without correct format are also discarded, and it is made sure that the sibling block of the rejected block is discarded simultaneously. Ballots are contained in blocks that is why the modification is not possible. A single change in a block leads to changing the other blocks linked with it.

4.5 Transparency

Blockchain is an open and distributed ledger where each transaction and activity is made transparent for peer verification, validation, and visibility. As things are kept visible, this ensures no fraudulent activities to take place secretly. The fairness and accuracy are obtained through the blockchain's property of being transparent.

4.6 Public Verifiability and Individual Verifiability

Our protocol provides the opportunity to publicly verify activities or the voting process as it is kept transparent with the help of blockchain. Peer nodes or anyone can monitor activities of the participant of the network. Moreover, voters themselves can make sure whether their vote is taken into consideration or not. If the block containing voter's identity is broadcasted, then this ensures that the voter's vote is going to be taken into consideration. Individual verifiability is satisfied through the protocol.

4.7 Auditability

Results are calculated after the ending of the election process, and the whole process is auditable as blockchain keeps the record of the whole thing. The rejected blocks and ballots can be monitored at later stages to have an idea of how often fraudulent activities were intended. Smart contract codes cannot be modified since it is permanently written on the blockchain.

4.8 Consistency and Accuracy

All the peer nodes will have the same record, and at the end, the same result will be obtained by all the participants. For every activity, a consensus mechanism is carried out to satisfy the consistency. Meanwhile, no changes are incurred, and the consensus mechanism makes the protocol accurate.

4.9 Non-repudiation

The process of non-repudiation is that someone cannot deny something. Therefore, the result obtained cannot be claimed as being unfair or of fraudulent activities as every activity is made transparent and verifiable by the majority network. It is not possible to mess with the majority honest network. Activities are performed by the execution of code where there is no possibility of unfair means.

5 Conclusions

E-voting is an emerging concept or solution of voting to carry out activities with accuracy and reliability. Moreover, blockchain is an interesting and attractive technology that provides transparency of data and is a topic of high demand. As the process of election must be handled with care to avoid unusual circumstances and occurring, this protocol reduces the constraints of manual voting and other e-voting systems based on blockchain. Also, the reduction of the third party is proof of a healthy election which is enabled with the assistance of a smart contract. The coercion is also prevented by the concept of random generation of groups using a smart contract. The techniques used in the protocol are quite simpler and easily understandable. Moreover, this protocol is designed to reduce memory and time consumption to make tasks faster. Thus, this protocol fulfills all the previously defined properties of the referred paper along with the prevention of coercion with transparency. The voters can monitor the whole process, and their privacy is also maintained to avoid any sort of privacy issues. Moreover, a replacement of the metadata can be taken into consideration to make this protocol widely used in all areas.

References

1. Islam A, Shin SY (2019) BUS: a blockchain-enabled data acquisition scheme with the assistance of UAV swarm in internet of things. *IEEE Access* 7:103231–103249. <https://doi.org/10.1109/ACCESS.2019.2930774>
2. Islam A, Shin SY (2018) Blockchain technology in networking: a survey of the state-of-the-art. In: *Proceedings of symposium of the Korean Institute of communications and information sciences*, pp 321–322, June 2018
3. Islam A, Uddin MB, Kader MF, Shin SY (2018) Blockchain based secure data handover scheme in non-orthogonal multiple access. In: *2018 4th international conference on wireless and telematics (ICWT)*, Nusa Dua, 2018, pp 1–5. <https://doi.org/10.1109/icwt.2018.8527732>
4. Islam A, Shin SY (2019) BUAV: a blockchain based secure UAV-assisted data acquisition scheme in internet of things. *J Commun Netw* 21(5):491–502. <https://doi.org/10.1109/JCN.2019.000050>
5. Islam A, Chae S, Shin SY (2018) Social Internet of Things (SIoT) and blockchain: research opportunities and challenges. In: *Proceedings of symposium of the Korean Institute of communications and information sciences*, pp 326–327, January 2018
6. Islam A, Kader MF, Shin SY (2019) BSSSQS: a blockchain-based smart and secured scheme for question sharing in the smart education system. *J Inform Commun Converg Eng* 17(3):174–184. <https://doi.org/10.6109/JICCE.2019.17.3.174>
7. Islam A, Shin SY (2019) BHMUS: blockchain based secure outdoor health monitoring scheme using UAV in smart city. In: *2019 7th International Conference on Information and Communication Technology (ICOICT)*, Kuala Lumpur, Malaysia, 2019, pp 1–6. <https://doi.org/10.1109/icoict.2019.8835373>
8. Weaver N (2016) Secure the vote today. *Lawfare Blog*, Washington, D.C.
9. General framework of electronic voting and implementation thereof at national elections in Estonia. Document: IVXV-ÜK-0.99, 12 January 2017
10. Liu Y, Wang Q (2017) An E-voting protocol based on blockchain, October 2017

11. Hardwick FS, Gioulis A, Naeem Akram R, Markantonakis K (2018) E-voting with blockchain: an E-voting protocol with decentralization and voter privacy. [arXiv:1805.10258](https://arxiv.org/abs/1805.10258) [cs.CR], 3 July 2018
12. Cranor LF (2001) Electronic voting. *Encyclopedia of Computers and Computer History*, Fitzroy Dearborn
13. Kumar DA, Begumn TUS (2012) Electronic voting machine—a review. In: *International conference on pattern recognition, informatics and medical engineering*, March 21–23, 2012
14. Hanifatunnisa R, Rahardjo B (2017) Blockchain based e-voting recording system design. In: *11th International conference on telecommunication systems services and applications (TSSA)*, 2017
15. Hjalmarsson FP, Hreioarsson GK, Hamdaq M, Hjalmtýsson G (2018) Blockchain-based E-voting system. In: *2018 IEEE 11th international conference on cloud computing (CLOUD)*, San Francisco, CA, USA, 2018, pp 983–986
16. Hoque MdM (2014) A simplified electronic voting machine system. *Int J Adv Sci Technol* 62:97–102
17. Yavuz E, Koc AK, Yavuz E, Cabuk UC, Dalkilik G (2018) Towards secure E-voting using ethereum blockchain. In: *6th International Symposium on Digital Forensic and Security (ISDFS) 2018*