Transparent Blockchain-Based Electronic Voting System: A Smart Voting Using Ethereum

Chapter · February 2022

DOI: 10.1007/978-981-16-7167-8_7

5 authors, including:

Md Tarequl Islam
Khwaja Yunus Ali University
20 PUBLICATIONS **107** CITATIONS
SEE PROFILE

Abu Sayed Sikder
LCT Journal Publisher
25 PUBLICATIONS **63** CITATIONS
SEE PROFILE

Md. Selim Hossain
Hajee Mohammad Danesh Science and Technology University
56 PUBLICATIONS **410** CITATIONS
SEE PROFILE

Dr Mir Mohammad Azad
Hamdard University bangladesh
72 PUBLICATIONS **492** CITATIONS
SEE PROFILE

Transparent Blockchain-Based Electronic Voting System: A Smart Voting Using Ethereum

Md. Tarequl Islam[1*], Md. Sabbir Hasan[1], Abu Sayed Sikder[2], Md. Selim Hossain[3] and Mir Mohammad Azad[1]

[1] Department of Computer Science and Engineering, Khwaja Yunus Ali University, Enayetpur, Sirajganj-6751, Bangladesh
[2]School of Science and Engineering, Southeast University, Dhaka,Bangladesh
[3]Department of Computing and Information System, Daffodil International University (DIU), Dhaka, Bangladesh
tareq.cse@gmail.com

Abstract. The research work scrutinizes an e-voting concept that is on the platform Ethereum block-chain. Ethereum is a distributed computing platform that is free, open-source with the functionality of smart contracts. By utilizing this depiction, it is feasible to originate engrossing scientific prominence which enables the thoughtful in sober fact collaboration occurring in the block-chain. E-voting is the most accepted worldwide because it is a tool that every moment signifies the democracy of the election. Consequently, most of the countries persevere to experiment and development of the E-voting process. Block-chain technology is responsible for a decentralized design that designates advanced data simultaneously among the P2P network barring a central database. At last, the experiment addressed the debilitation of the existent E-voting method and successfully fruitful blockchain technology to unravel that feebleness.

Keywords: E-Voting, Blockchain, Ethereum, Smart Contract, Authorization, Decentralization, Security and Privacy.

1 Introduction

A Blockchain is a sempiternal progressive ledger[1][2][3] that remains an indestructible record of all the transactions that have occupied a place in a sheltered, chronological, and unchallengeable [4] way. A blockchain comprises a chain of blocks that take on information. Every block record all of the current transactions, and once completed goes into the blockchain as a perpetual database. Blockchain technology can be mobilized into abundant areas. The fundamental use of blockchain is as a distributed [5] ledger[6] for crypto-currencies. It displays the greatest pledge across a comprehensive range of business applications like Entertainment, Finance, Healthcare, Insurance, Media, Government and Banking, Retail, etc. Blockchain technology has become more accepted because of Unchangeable transactions, Reliability, Security, Collaboration, Time reduction, and decentralized. In 1991 Stuart Haber and W. Scott Stornetta have described this technology[7]. Electronic Voting Machine (EVM) is one of the most serious themes to dispute for political gatherings in point of fact from the last successive

few years [4]. In the conventional scheme [8][9], the election commission has to print isolated ballot-paper for each voter[10]. A voter usages “seal and ink” to vote for their selected candidate.[11] And sometimes, many votes converted impractical for philanthropic the “seal” in unexpected constituencies. Again, piracy in voting [3][7] and “lack of clearness in numeration[1][3] are the major disqualifications of the outdated organization [7]. Typically, the voting system should be able to functions such as accredited voters should be capable to vote (the same convenience about accessibility and place). The voter can validate whether their vote has been counted, and the result is tally all around the voting process [4]. The election should be a reasonable cost. No one can mention their vote other than themselves. The voting process should be capable to validate by all participants. By meeting legislators' legal requirements, blockchain-based electronic voting systems improve voting integrity, optimize the voting process, and produce consistent voting results. It will also help to mitigate current challenges for a long time through the distributed ledger process. To steadfastness E-voting limitations, blockchain technology is an of incalculable value existence. The behavior of blockchain technology is a ledger that is incontrovertible, immutable, and distributed [4][9]. Omission the principal database. P2P networks that every node has the same block-chain but distributed that consequential in no single point of miscarriage[8]. When a new data or so-called block generates, the previous block will be referenced by the new block that fabricates an unchangeable chain that protects data from interfering [6][7]. “Control over half of the nodes (51%) in the net which made the system” [7] tremendously secured. “It is improbable to launch DDoS to multiple nodes in the network at the same time [8]. Moreover, Ethereum brings additional prolongation, while residuals the block-chain functionalities are: “Give authorization to the developer to program and customize block-chain (i.e., smart contracts)” [12]. “Least CPU possessing the cost in terms of performance” [13]. Furthermore, the decentralized architecture brings the security level higher with block-chain technology with its consensus algorithm than the centralized architecture (client-server).

2 Related work

In this part, we contemporary approximately the circumstances of the art pertinent e-voting schemes that usage blockchain as a service. “Agora”[14] designed a voting system that is an end-to-end verifiable [15] voting solution on “blockchain-based for governments and institutions” [16]. For the election, administrations, and organizations, acquisitions tokens for each qualified voter Agora uses these Token on the block-chain [14]. The current voting system has numerous flaws, including political power abuse, high costs, and a lengthy procedure, among others. To address these issues, we proposed a blockchain-based smart voting system. In the UK they provide digital voting to their voters to vote from their home district or by a web browser at home by using blockchain technology that is used in their current voting system [15][16].
A biometric online voting system is a web-based online voting system that improves the electoral process by providing fast, accurate, and secured election results. In this voting system, there will be two different users for the creation of data as admin each

with their privileges [12][13], one is an administrator and the other is a system user. An administrator creates the logs, inserts the candidate's information, creates voter data, party information, and closes the web application when done whereas the system user creates logs, creates voter data, and closes the web application only. For the registration of voters, the system accepts the voter's fingerprint for the verification process and if the fingerprint is matched to the database, then the system issues the PIN for the voter else the system will scan the finger for the matching fingerprint is not detected. After getting PIN voters can give the vote [5].

3 Proposed Concept along with Contribution

The foremost achievement of the paper is tabulated by the way:
1) It is anticipated a message endorsement and broadcasting apparatus which permits authorization to examine while conserving secrecy. The mechanism can take advantage of in various scenarios including vote, authority, result, candidates, and so on.
2) It has been decoupled the biometric Info and inspecting the method into three steps, correspondingly administered by the authority, the voters, and the Candidates' smart agreement.
3) In the simulation the comprehensive apparatus is implemented, containing reliable calculation skills founded on Ethereum.

4 Working Procedure

Algorithm1: Algorithm for Authentication
authorization: = initialization
If authorizations: = (voter_id, Biometric_Info)
Add: = Node{(node_id) & (authentication)}
Authority= certification {user credentials, certify (credentials, node_id, users_Info)}

Algorithhm2: Voting Algorithm
Vote (V): = vote (voter_id, candidate)
Block: =add (V, chain)
BC Info: = Update (voting machines)
changed the voter's linked arena to vote by Authority, vote (voter_id, user-list, true).

Algorithm 3: Counting Vote
Candidates are reached from an authority, candidates = get candidates (candidate_list).
Calculation: = votes and the conqueror of the territory is strong-minded,
results = count (chain, candidates).
End

Nowadays, we are working to designate our projected typical according to the algorithm. Ethereum based voting system includes us with a central database, where every

transaction is rechecked. “This procedure of transaction with the transaction is called a block. By following every set of rules, the transaction validation is checked. Solidarity software design is utilized to change the consent to get to the organization whether it private Ethereum based blockchain framework. Even however Ethereum remains an open and permissionless Blockchain framework, we will attempt to make the permission. In every step, it checks the voter identity to produce voter permission to vote.

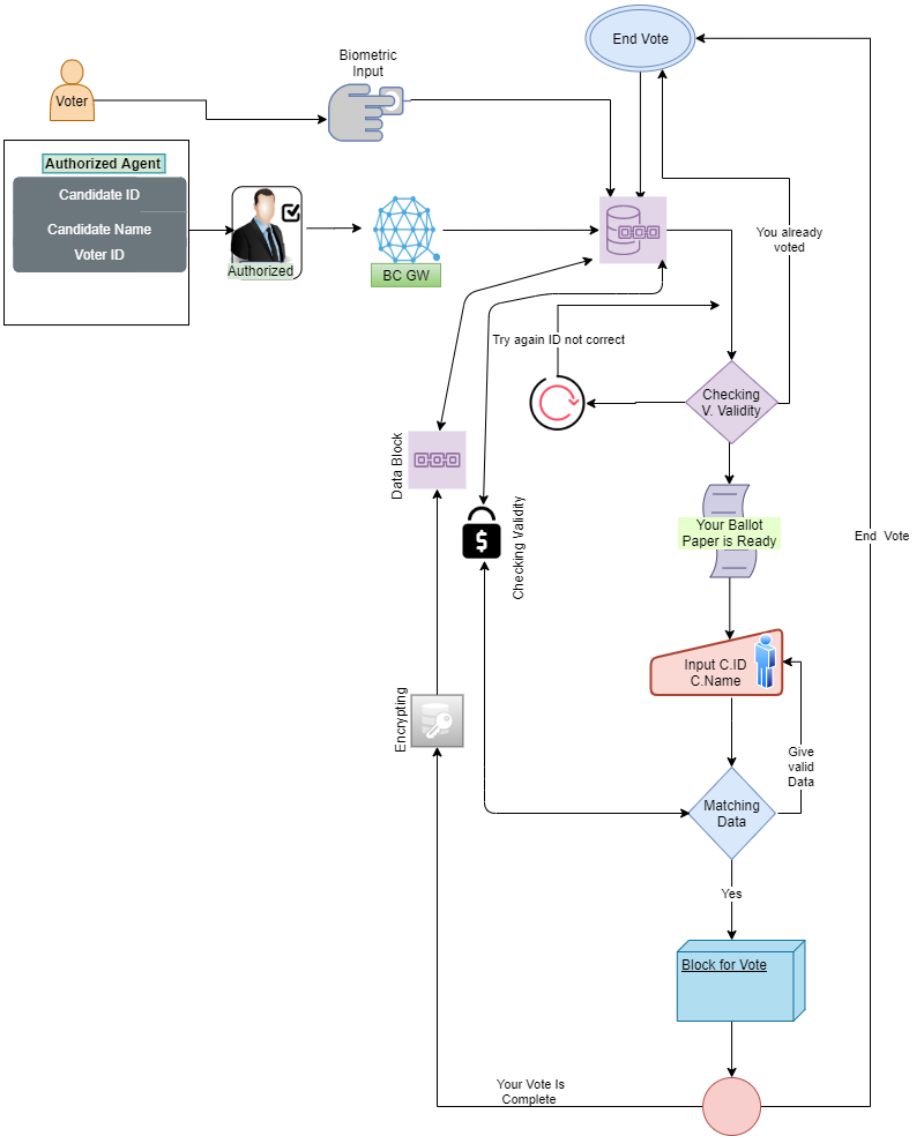

Fig 1. Proposed Block diagram of E-Voting System Using Blockchain

Since BC is a distributed ledger system, the data will be managed by decentralized manner. BG will be used to transfer the normal data into blockchain format. Here each block has a coordination with the previous block. There are 3 blocks in this proposed system. Each block is connected. When a person (Voter) comes to vote 1st his/her details are checked by the authority by biometric information then she/he can access the voting system. After verified electrical ballot paper showed in the display and voter choose the candidate when voter choose candidate this is also verified by the author again. At last, when all of is verified then the vote is count to the chosen candidate. Since we have a NID number against our biometrics fingerprint system. The NID number will be matched in equivalence to the fingerprint where it will be easily handled the data from database system.

4.1 Transaction Table

The elector's data is kept secure utilizing the "SHA3-512-bit hashing algorithm and to keep citizens' democratic inclination un-uncovered just elector id and political decision id is put away in the information base which doesn't uncover whom they have cast a ballot."[17][18] Some other exchange yields are given underneath every exchange distinguishing proof:

Table 1. Transaction Details

No	Election_ID	Election_Name	Number of Candidates
1	0xCA35b7d915458EF540aD e6068dFe2F44E8fa733c	Select Candidate	3

Table 2. Voting Transaction Table

No	Voter ID	Candidate ID	Status	Time	Gas Cost
1	0x583031d1113ad 414f02576bd6afa bfb302140225	0xca35b7d91545 8ef540ade6068df e2f44e8fa733c	Vote Successful	7-12-2020 18:54:05	50139
2	0xdd870fa1b7c47 00f2bd7f4423882 1c26f7392148	0x14723a09acff6 d2a60dcdf7aa4af f308fddc160c	Vote Successful	7-12-2020 18:54:07	62560
3	0x63fdf702493a3 5c653e9a1a851da 1cc6aff16c33	0x4b0897b0513f dc7c541b6d9d7e 929c4e5364d2db	Vote Successful	7-12-2020 18:56:15	59564
4	0x560565799dc6a 92c6fc494c58835c d01fa2b7b81	0xca35b7d91545 8ef540ade6068df e2f44e8fa733c	Vote Successful	7-12-2020 18:58:05	50139
5	0x2e2ae5091cb39 71389bb92b5dd1 428ad81491baf	0x4b0897b0513f dc7c541b6d9d7e 929c4e5364d2db	Vote Successful	7-12-2020 19:00:05	69665

6	0x0a4cdb536739782cff6bd6f3c7a0ebf6cae8efa3	0xca35b7d915458ef540ade6068dfe2f44e8fa733c	Vote Successful	7-12-2020 19:04:09	50139
7	0xc27a944e35f9b9b06f4c83e785353ce1a460d919	0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db	Vote Successful	7-12-2020 19:10:55	61435

Table 3. Output of a Transaction

statues	0x1 Transaction mined and execution succeed
transaction hash	0x8593e5277dd25ffd6261d1db16f709f8e96e9231decb44b55049d7e6cb7d773e
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	50139 gas
execution cost	27523 gas
hash	0x8593e5277dd25ffd6261d1db16f709f8e96e9231decb44b55049d7e6cb7d773e
input	0x462...00000
decoded input	0x0DCd2F752394c41875e259e00bb44fd505297caF
decoded output	[]
logs	[][]
value	0 wei

The framework checks the all-out votes got by every competitor in every single diverse political decision, what's more, stores them in the information base. Also, the eventual outcome has appeared on the overseer site. The accompanying figures show the number of up-and-comers in all decisions and got votes of every competitor in each various race.

5 Result Analysis

We are describing delay time between 2 voters when a voter voted then another voter need to wait to complete the transaction. Since an organization set up that the program would not be transmission however would make some short time delay amassed into the transmission to allow.
For example, we take 10 voters to vote in a network. Here if every voter takes 10-15ms time after completing his/he transaction then the delay of time goes to:

Table 4. Delay of time for voters

Voters	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th
D.Time	10	22	28	40	50	60.50	73	85	90	103.45

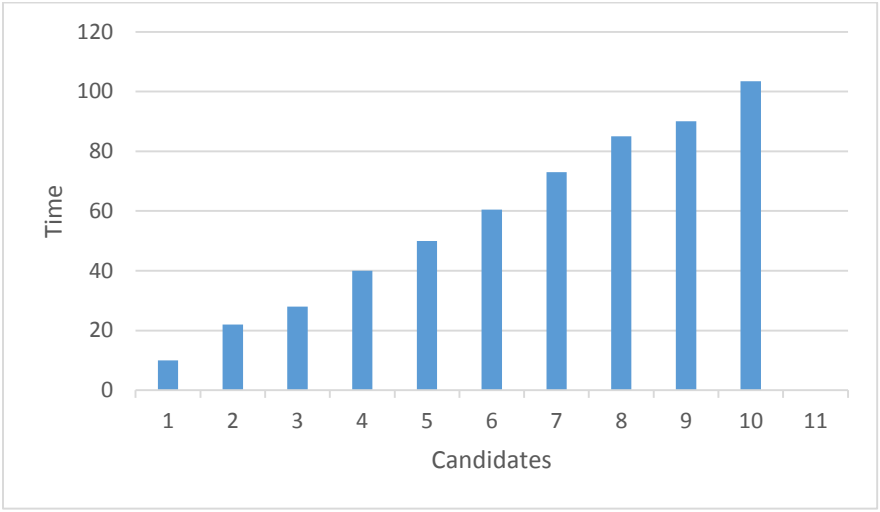

Fig 2. Chart of Delay Time

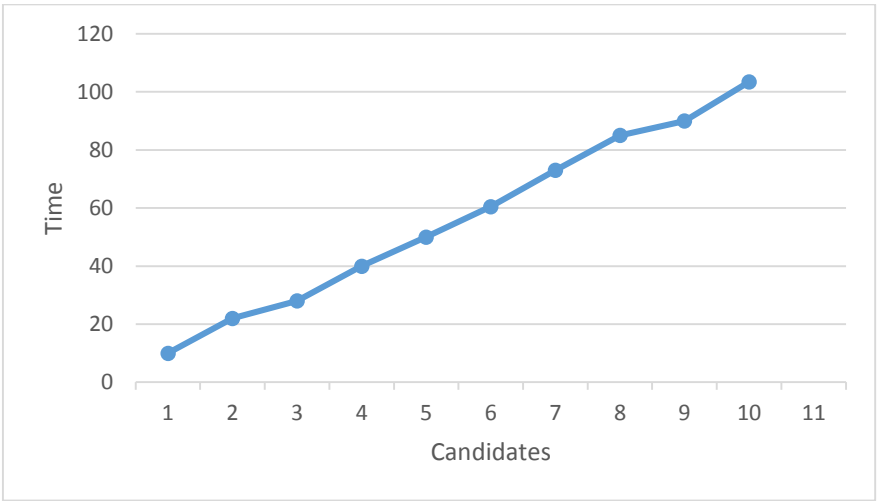

Fig 3. Curve of Continuous Delay Time

6 Security Issue

At first, we deliberate the security of smart agreements and e-voting on the block-chain. Which is the foremost apprehension that essential be occupied. Since supposing if the

citizens are not guaranteed of their security, they won't get engaged in the procedure [3]. There are confident safety areas that can be pleased with our projected practice. Inconspicuousness, Voters Privacy, Confidentiality, Ballot manipulation, Transparency.

7 Limitations of the Proposed System

In the Ethereum based Blockchain (EBB) innovation, the exchange will happen in a cryptologic way wherever logs are not open and can't be adjusted. It is not possible to get the log data of this EBB exchange. Smart Conventions started with the comparative pay of changelessness as Blockchain. Indeed, even minimal blunder in cryptograms can end up being costly and tedious to precise once when the keen arrangement is situated to execute. While the annihilation of third-social events stays a theory that receipts set for Blockchain and unique agreement that is no real way to dispose of them.

8 Conclusion and Future Work

From the earlier discussion, E-voting is an unindustrialized thought or clarification of voting to convey out operations with exactness and authenticity. We proposed a voting system in the research work which is based on Ethereum Blockchain contained a decentralized platform. The foremost influence of this work is the Biometric input of the Ethereum network on the e-voting system. But the whole work is done in simulation software and Ethereum online IDE. Paillier cryptosystem as a library in solidity is implemented here. With this system cryptography of solidity, the library could largely improve our ballot verifiability. BC system will be also applicable in NFT market place, real time IoT monitoring, personal identity security, supply chain, banking sector etc. In the future, it will be tried to implement a Blockchain-based E-voting system in real life.

References

[1] S. Agathiyan, S. Latha, and J. Menaka, "A NEW APPROACH OF SOLAR POWERED ELECTRONIC VOTING MACHINE WITH AUTHENTICATION SYSTEM AND FOR BLIND PEOPLE," *Adv. Innov. Res.*, p. 36, 2019.

[2] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Futur. Gener. Comput. Syst.*, vol. 105, pp. 13–26, 2020.

[3] 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)*, 2018, pp. 1–7.

[4] M. S. Hossain and M. T. Islam, "An Extension of Vigenere Technique to Enhance the Security of Communication," *2018 Int. Conf. Innov. Sci. Eng. Technol. ICISET 2018*,

no. October, pp. 79–85, 2018, doi: 10.1109/ICISET.2018.8745638.

[5] 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)*, 2018, pp. 983–986.

[6] A. Rahman, M. S. Hossain, Z. Rahman, and S. K. A. Shezan, "Performance enhancement of the internet of things with the integrated blockchain technology using RSK sidechain," *Int. J. Adv. Technol. Eng. Explor.*, vol. 6, no. 61, pp. 257–266, 2019.

[7] A. Zahan, M. S. Hossain, Z. Rahman, and S. K. A. Shezan, "Smart home IoT use case with elliptic curve based digital signature: an evaluation on security and performance analysis," *Int. J. Adv. Technol. Eng. Explor.*, vol. 7, no. 62, pp. 11–19, 2020.

[8] M. S. I. Sarker, Z. Rahman, S. K. A. Shezan, M. S. Hossain, and M. Mahabub, "Security Assumptions for Ubiquitous Secure Smart Grid Infrastructure using 2 Way Peg Blockchain and Fuzzy Specifications."

[9] M. M. Alhammad and A. M. Moreno, "Gamification in software engineering education: A systematic mapping," *J. Syst. Softw.*, vol. 141, pp. 131–150, 2018.

[10] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, 2019.

[11] Y. Kurt Peker, X. Rodriguez, J. Ericsson, S. J. Lee, and A. J. Perez, "A cost analysis of internet of things sensor data storage on blockchain via smart contracts," *Electronics*, vol. 9, no. 2, p. 244, 2020.

[12] S. Hossain, S. Waheed, Z. Rahman, S. K. A. Shezan, and M. Hossain, "Blockchain for the Security of Internet of Things: A Smart Home use Case using Ethereum," *Int. J. Recent Technol. Eng.*, vol. 8, no. 5, pp. 4601–4608, 2020, doi: 10.35940/ijrte.e6861.018520.

[13] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4. Institute of Electrical and Electronics Engineers Inc., pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[14] Y. Wang *et al.*, "Formal verification of workflow policies for smart contracts in azure blockchain," in *Working Conference on Verified Software: Theories, Tools, and Experiments*, 2019, pp. 87–106.

[15] T. Chen, X. Li, X. Luo, and X. Zhang, "Under-optimized smart contracts devour your money," in *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, 2017, pp. 442–446.

[16] K. Patidar and S. Jain, "Decentralized e-voting portal using blockchain," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019, pp. 1–4.

[17] L. Vo-Cao-Thuy, K. Cao-Minh, C. Dang-Le-Bao, and T. A. Nguyen, "Votereum: An Ethereum-Based E-Voting System," in *2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF)*, 2019, pp. 1–6.

[18] M. T. Islam, M. K. Nasir, M. M. Hasan, M. G. G. Faruque, M. S. Hossain, and M. M. Azad, "Blockchain-Based Decentralized Digital Self-Sovereign Identity Wallet for Secure Transaction."