Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020)
IEEE Xplore Part Number: CFP20P17-ART; ISBN: 978-1-7281-5821-1

Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract

Syada Tasmia Alvi
Dept. of CSE
Jagannath University
Dhaka, Bangladesh
tasmia.rng@gmail.com

Mohammed Nasir Uddin
Dept. of CSE
Jagannath University
Dhaka, Bangladesh
nasir@cse.jnu.ac.bd

Linta Islam
Dept. of CSE
Jagannath University
Dhaka, Bangladesh
linta@cse.jnu.ac.bd

***Abstract*—The voting method is the mechanism for implementing the people's view to better administer the system. Throughout recent years, conventional votes have pleased neither people nor government authorities. They are not entirely safe since ballots are simple to strike. It also challenges voter safety and transparency. Additionally, counting the votes takes too long. Modification of voting worldwide is an intriguing issue in current voting system. To solve these problems Digital technology is used in the voting phase for citizens in many nations. Digitalisation alone can not fix the issues fully. There are also many ways of manipulating or modifying digital technology and hindering voting. There should be fairness, independence and impartiality in the voting method. By analyzing the aforementioned problems, this research work combines the digitalisation with the blockchain technology to provide a voting mechanism. The main goals of our voting mechanism are to provide integrity, anonymity, privacy, and security of voters. With the use of markle tree and fingerprint hash, the data integrity and anonymity, privacy, security of the voters has been achieved in our proposed digital voting systems.**

***Index Terms*—Voting, Blockchain, Fingerprint Hash, Smart Contract, Mining, Markle tree**

I. Introduction

Democratic voting is a mechanism which is important and severe in every region. Conventional paper polling, mechanical devices and electronic ballot systems are the common way for countries to vote. However there is a need for new digital technologies. Digital voting involves the usage of electronic polling devices and in addition there are two forms of digital voting : E-voting and I-Voting. E-voting is where a device is used by the voters to place their votes at the voting center and I-voting is where a software interface is required for this reason. The main criteria for the integrity of the democratic process are precision, robustness to illegal behavior, efficiency, stability and transparency of the voting mechanism. Reliability, secrecy, integrity and reduce investment on manpower, supplies and technological equipment can be enhanced by Digital Voting systems. It simply guarantee that the casted votes and the final results are correct [1].

Digital Voting also has a number of limitations. Fake voting, expense savings, produce quicker outcomes etc. are some malicious practices throughout the voting process. In fact, a variety of intruders may damage smart or IoT (Internet of Things) systems by making a dramatic impact on the voting or calculation of voting to obtain their own profit. Certain protection measures must be in place which should gurantee about a consistent process of poling and counting. Different approaches has been suggested. However, such systems can also raise the complexity of network by increasing the expense of computation, bandwidth, space, and testing. Therefore, some improved protection systems or mechanisms are required that guarantee a stable voting or counting methods and preventing the aforementioned described problems [2].

Blockchain technology is a decentralized ledger that maintains a coherent understanding of truth. Blockchain has been used in cryptocurrencies such as Bitcoin [3] and Ethereum [4] which is a mutual, tamper-proof ledger and peer-to - peer networking platform. Here the public or private key identity protects user anonymity. There are several blockchain based model [5], [6], which provides security and privacy. While blockchain provide security, privacy, accountability and durability, the essential challenges of implementing Blockchain technology are related to speed and scalability [7].

Our objective is to design a Digital Voting architecture with the inclusion of a smart contract to reduce challenges generated during the adoption of blockchain with voting and provide authentication, transparency, anonymity, accuracy and autonomy, singularity, integrity, mobility. In our system, from the voters information a hash will be generated and stored in the chain. This will provide scalability and anonymity of voters as the information is stored in the blockchain as a hash. Any changes will be easily detected if the hash information is modified. Smart contract running in the chain ensure security and privacy. A miner is nominated by smart contract to improve the speed of the transaction. The nomination depends on different criteria such as data transmission, energy consumption. Counting process of vote is done in each block. At the end of voting, from the last block total vote can be easily analyzed. It reduce the time consumption for counting.

The paper is organized as follows. In Section II, related works about voting based on EVM, E-Voting and Mobile Voting are discussed. In Section III, general architecture of the proposed blockchain based e-voting election system is explained. At the following section, Section IV, proposed system is analyzed from different aspects. Section V shows the comparison between existing systems and proposed system. In the final section, Section VI, future work on the system is

discussed and conclusions about the research have been made.

II. Related Work

A. EVM

A voting mechanism is introduced in [8]. Electronic voting machines are used by them for voting process. This system is centralized system. That way, voting information can be easily manipulated. There is no mechanism for the electors to validate whether or not their vote is recorded. [9] introduce an blockchain based voting algorithm where each EVMs are directly linked in a network. This system has three parts to ensure integrity: fingerprint authentication, peer verification transaction, and chain manipulation detection. It is susceptible to snoops and DoS (Denial-of-Service) attacks. It needs to be updated for several nodes.

B. E-Voting

Santhosh et.al. [10] present the concept of the online voting systems in which configuration of voting counter using internet is highlighted. In this process voters can cast vote through the Internet. This system is limited by the fact that a system failure is possible and voting information can be manipulated. In [11] they have designed a new sample of the Indian voting process. After performing authentication voter can cast vote from voting machine from anywhere. Confidentiality, credibility, privacy, fairness, simplicity and accountability of the technical and protection specifications of e-voting have not been discussed. [2] introduce a framework that focuses on improved security through Blockchain in the IoT-based e-voting platform. Throughout this program the user needs the voting id and other bio-metric approaches to create an account with successful verification on a smart device. Smart Contract is used for performing voting operation. Though it is highly safe and busy process, the device runs slowly because of workload.

C. Mobile Voting

A safe voting mechanism is introduced via SMS (Short Message Service) and smartphone application in [12] where mobile voting systems are used to vote safely for their candidate. It guarantees that the ballots can be stored secured until the election in their districts ends. Anyone having the phone in the absence of mobile owner can cast vote. So it is possible to vote wrongly. An m-voting platform [13] is recommended which utilizes blockchain technology to securely manage cast votes. This system use multi-factor authentication to authenticate voters while voting. No security research has been done by them. It may be vulnerable to a quantum attack, 51% attack, and so many.

III. Proposed Voting Mechanism

Most people don't have devices due to living in extreme poverty. Legitimate voters can therefore cast votes through their devices or from a specified voting station. The details of the voting mechanism showed in fig. 3 and fig. 4. Where fig. 3 shows the registration process and fig. 4 shows the casting and counting process.

A. Data Management of the system

In the time of election process enormous data volumes are created. So data should be recorded systematically. There are three type of storages used in our system as shown in fig. 1 :

1) **Election Commission's Database :** All the voters registration information, candidate registration information, party registration information and other election related information will be stored in database.
2) **Blockcahin Storage :** In Voting blockchain, a hash value which is generated from the voters information will be stored in the genesis block as a list of voter and each vote will be stored in chain as a block. To store the metadata of Election Commission's database another type of blockchain is used.
3) **Cloud** : A copy of Election Commissions database and voting information before and after election will be stored in cloud.

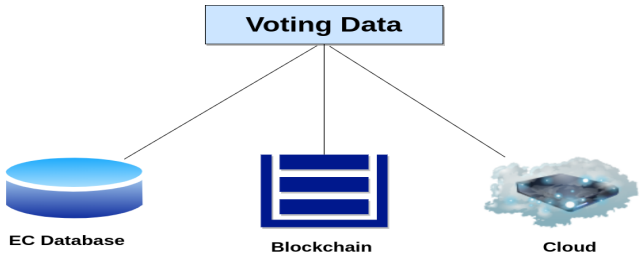

Fig. 1. Storage of the System

B. Voter Registration

Voters Registration Process showed in fig. 3 are explained below:

- To be a legitimate voter each person have to go to their local voter registration office and submit their appropriate details.
- For genrating a key pair of public key and private a key generation algorithm will be used.
- Public key is used as voter identification in the blockchain network. The private key is sent to mobile number of voters. Using this private key they can participate in the voting process and cast vote.
- A hash generation algorithm from fingerprint [14] is used to generate a hash from the submitted fingerprint of a voter. The full process of hash generation from voter submitted information is shown in fig 2.
- Generated hash will be combined with voters others information to generate another hash value .
- Final hash value will be stored in the genesis block of blockchain as a voter list.
  Where, hash value = proof-of-membership

C. Candidate Registration

Since Candidate is also a voter, their Registration process is just like the voter registration. The candidate number, party symbol and public key will be stored in the genesis block of blockchain.

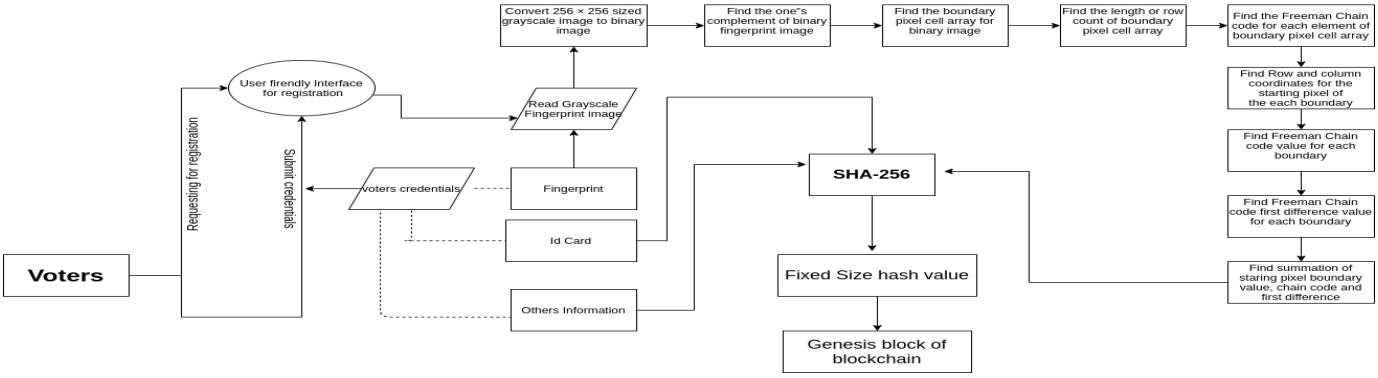

Fig. 2. Hash generation from voter credential

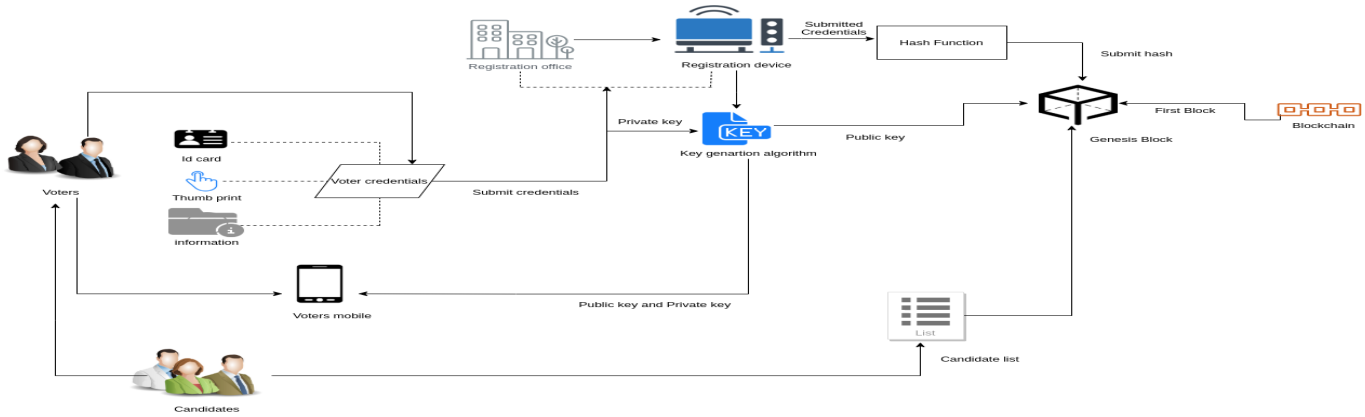

Fig. 3. Architecture Of Registration Process

D. Vote Casting using smart contract

The role of smart contract running in the blockchain are given below :

- **Verification of a voter :**
  - Voter logs in to the voting system using private key through an internet-connected device.
  - Submit NID,fingerprint and other information.
  - Smart contracts built in the blockchain check the legitimate voters information in the genesis block with the submitted information.
  - If the information matches, it provides a candidate list to the voter.
- **Create Block for Casted Vote:**
  - Voter choose one of the candidates from the list of candidates and cast vote.
  - Sign the vote with digital signature and a send a transactions to the SC.
  - SC generates a VID(Vote ID) for the vote of that voter.
  - Increment the vote of the choosed candidate.
  - Make a block with transactions collected from the voter including the VID and Candidate Vote number.
- **Miner Selection:**
  - The SC executes a Miner Selection Algorithm and
  - Nominate a Miner to generate the target Hash of the block.
- **Generate Hash:**
  - The Miner who is nominated by SC updates the block by adding the hash of the current mined block and increasing the nonce into the Block.
  - The miner begins generating a desired hash with a number of prominent zeros (known as Proof of Work) by increasing a variable which is called nonce of the block.
  - The Miner produces the intended hash and then transmits the block to the Blockchain network and get financial compensation for it.

  In Bitcoin, Proof of Work in digital cryptocurrency requires tremendous computing resources as all the miners race to be the first to produce the block's goal hash to avoid record interference. It has been proposed to select a Miner in the proposed voting architecture on the basis of heuristic extracted from achievements by a Miner.The SC gathers mentioned in [15] criteria including latency, energy usage and node capacity.
- **Verify Block :**
  - All the nodes in Blockchain verify the block and add the block to the current Blockchain.The block

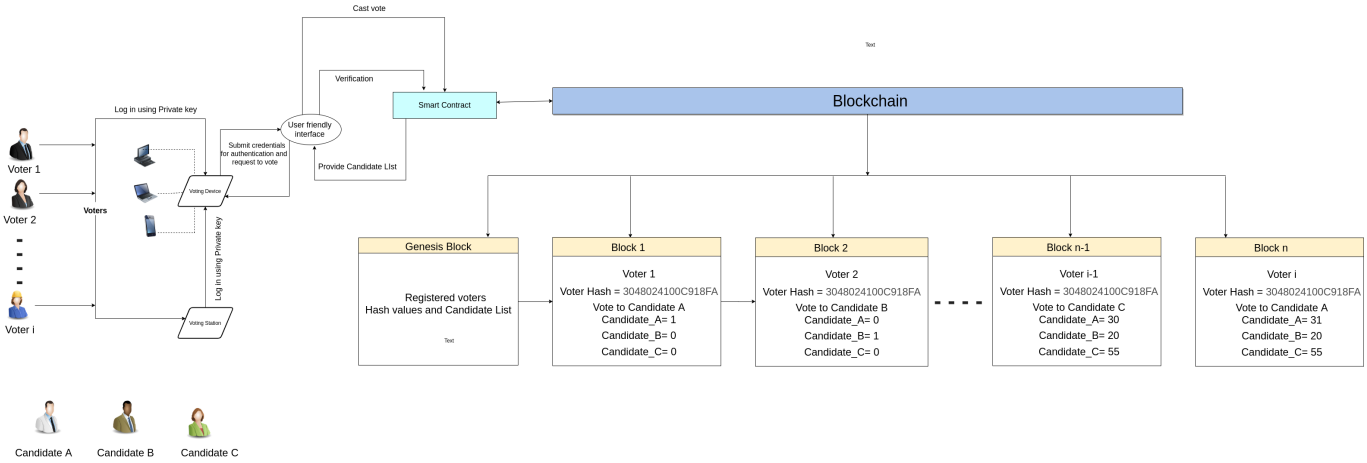

Fig. 4. Architecture Of Vote Casting and Counting

structure is shown in fig. 5.

- After successfully adding the vote in chain the Sc will remove the hash value from list of voter
- Add it to another list named Already voted to prevent double vote casting.
- Return VID to the voter to verify thier vote in the blockchain

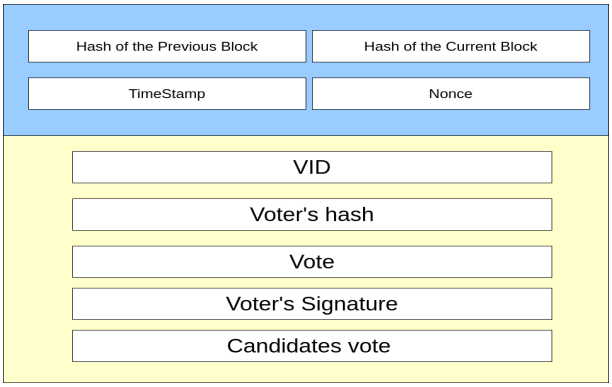

Fig. 5. Block Structure

E. Vote Counting

The smart contract will count the number of votes in each block. Once the vote submitted, the vote is counted immediately, and there is no chance of voting manipulation and fraud voting.

Table 1 illustarate the collection of voting result for different region.

IV. Experimental Analysis

A. CONCUSSES IN THE BLOCKCHAIN

With decentralized frameworks, particularly in blockchain based e-voting method, a concussion problem can arise. This is happened when various voters cast their votes around the same time. This will be connected when a voter casts a vote

TABLE I
Result Publication

Region	Candidate A	Candidate B	Candidate C	Winner
X1	2000	3000	1000	Candidate B
X2	2040	1000	3000	Candidate C
X3	5000	1000	500	Candidate A
X4	2000	3000	1000	Candidate B
X5	2000	3000	1000	Candidate B
X6	2000	3000	1000	Candidate B
X7	2040	1000	3000	Candidate C
X8	5000	1000	500	Candidate A
X9	2000	3000	1000	Candidate B
X10	2000	3000	1000	Candidate B

linked to the last vote to build an unmistakable or unmistakable line [16]. In our system there is no concusses problem as the voting transaction is first submitted to Smart contract. So each block's information will be sent to the miner after a certain time interval as shown in fig. 6.

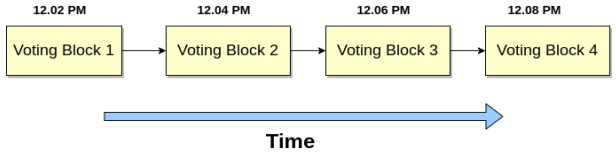

Fig. 6. Solution of Concuss Problem

B. Integrity

Merkle tree is implemented using blockchain technologies to guarantee data integrity [17]. Throughout ethereum, the Merkle tree principle was developed so as to provide a lightweight and effective proof that guarantees a transaction in a node.The Merkle tree includes hashes of all the transactions in a block. If a node needs to check that a transaction is modified or not, the nodes just have to create a markle tree in the transaction. This makes validating or invalidating a vote very easy [18]. To ensure the integrity of election process

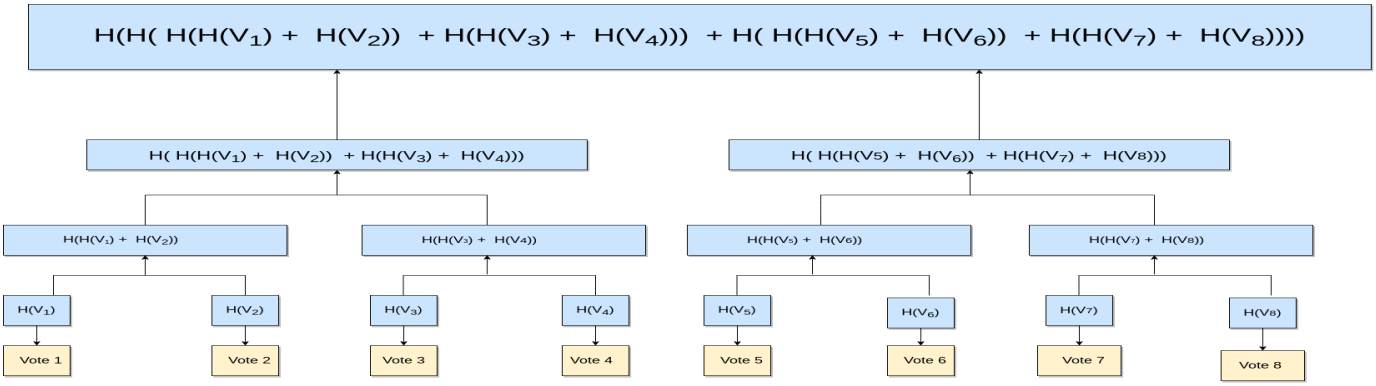

Fig. 7. Markle tree of full election process

markle tree is used in our system which is shown in fig. 7 .

C. Anonymity and Privacy

The proposed system offers anonymity and privacy to the voters. In the voting system, voters entry into the blockchain is done in an anonymous manner. Public key is used as the voters identity and the hash value which is generated during registration process is used as voters information in the blockchain network which preserved voters anonymity and privacy as shown in fig 8.

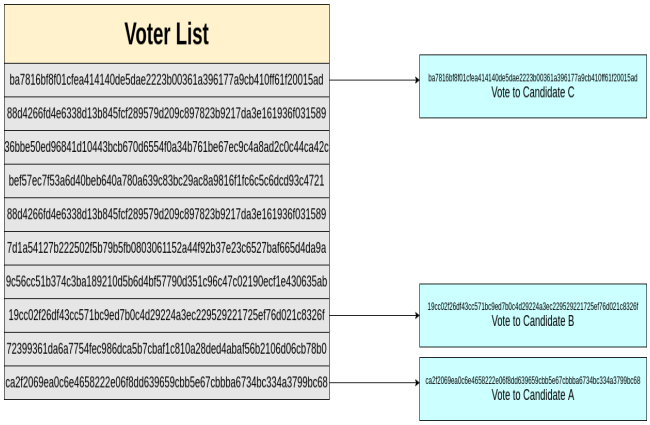

Fig. 8. Anonymity of Voter

D. Verifiability

Each vote is added as a block in the chain. Whenever a voting block generates, the Smart Contract (SC) return the voters a VID (Voter ID) and the location of the block to verify if their vote is added and counted in the chain without any modification. The vote verification process is shown in fig. 9.

E. Security Analysis

Some of the attacks that have been mitigated by our model are as follows:

- Sybil attack is used against centralized networks, where an person generates a vast number of nodes in an effort to interrupt network activity by hijacking or falling messages [19]. In our system only registered user can cast vote in this system and the hash value of each voter is unique so no individual has the access to create one.
- It solves the 51% attack [20] a major weakness in Bitcoin and Ethereum based blockchains. From [21], randomly selection of miner nodes solves the 51% attack.

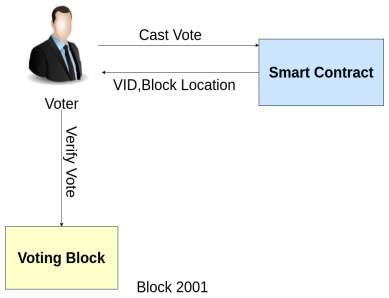

Fig. 9. Verification of Vote

V. Comparative Analysis

TABLE II
Comparison between Related and Proposed Works

Properties	[8]	[9]	[10]	[2]	[12]	[13]	Ours
Anonymity	×	✓	×	✓	×	✓	✓
Integrity	×	✓	×	×	×	✓	✓
Privacy	×	✓	×	×	×	✓	✓
Security	✓	✓	×	✓	×	✓	✓
Verifiability	×	×	×	×	×	×	✓
Decenralization	×	✓	×	✓	×	✓	✓
Singularity	✓	✓	×	✓	✓	×	✓
Authentication	✓	✓	✓	✓	×	×	✓

Table 2 shows the comparison between the existing works and our proposed mechanisms. From this comparison, it is observed that [8], [10], [12] do not provide anonymity, integrity, privacy, verifiability, decentralization. [2] doesn't provide inttgrity, privacy, verifiability. [9] and [13] do not provide verifiability. [10] and [12] do not provide security. [9] and [13] do not provide singularity. Authentication process

is missing in [12]. From the analysis of section IV, it is observed that, the proposed system provides anonymity, integrity, privacy, security, verifiability, decentralization, singularity and authentication.

VI. Conclusions and Future Work

Many countries face significant difficulties in protecting security in the voting framework. To ensure the participation and legitimacy of the voter, the integrity of the vote data and the counting of votes without manipulation, a blockchain based voting system using smart contract has been proposed. This mechanism where the SC performs the authentication process of voter and plays a role in selecting a Miner in the Blockchain to reduce the computational cost. It also counts the vote immediately which reduce the time consumption of election process. This mechanism provides the environment to the citizens to cast their vote using smart devices from anywhere. This will help to improve the amount voters in order to achieve any country's democracy. This research work intends to build an encryption technique in future to boost our system 's security.

References

[1] Roberto Casado-Vara and Juan Corchado Rodríguez. Blockchain for democratic voting: How blockchain could cast of voter fraud. *Oriental journal of computer science and technology*, 11, 03 2018.

[2] R.Krishnamurthy, Geetanjali Rathee, and Naveen Jaglan. An enhanced security mechanism through blockchain for e-polling/counting process using iot devices. *Wireless Networks*, 08 2019.

[3] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[4] Vitalik Buterin. A next-generation smart contract and decentralized application platform. 2015.

[5] V. Suma. Security and privacy mechanism using blockchain. *Journal of Ubiquitous Computing and Communication Technologies*, 01:45–54, 09 2019.

[6] Sivaganesan D. Block chain enabled internet of things. *Journal of Information Technology and Digital World*, 01:1–8, 09 2019.

[7] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian. A decentralized patient agent controlled blockchain for remote patient monitoring. In *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 1–8, 2019.

[8] Sandeep Kumar Kone Srikrishnaswetha and Md. Rashid Mahmood. A study on smart electronics voting machine using face recognition and aadhar verification with iot. In *In Innovations in Electronics and Communication Engineering, Singapore, 2019.*, pages 87–95. Springer, 2019.

[9] S. B, R. T. V, N. Krishna M P, B. R. J, S. Arvindh M, and D. M. Alagappan. Secured electronic voting system using the concepts of blockchain. In *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 0675–0681, 2019.

[10] .R.Keerthana .L.Suganya .S.Krishnakumar M.Santhosh, S.Kavitha. Electronic voting machine using internet. *International Journal of Communication and Computer Technologies*, 03 2016.

[11] Pooja Patil3 Nilisha Raut4 Prof. Swati Gawhale, Vishal Mulik. Iot based e-voting system. *International Journal for Research in Applied Science Engineering Technology (IJRASET)*, 5, 05 2017.

[12] X. I. Selvarani, M. Shruthi, R. Geethanjali, R. Syamala, and S. Pavithra. Secure voting system through sms and using smart phone application. In *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, pages 1–3, 2017.

[13] Temidayo Abayomi-Zannu, Isaac Odun-Ayo, and Barka Fori. A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication. *Journal of Physics: Conference Series*, 1378:032104, 12 2019.

[14] Sreeramana Aithal and Krishna Prasad Karani. A study on fingerprint hash code generation based on md5 algorithm and freeman chain code. *International Journal of Computational Research and Development (IJCRD)*, 3:13–22, 01 2018.

[15] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. An efficient selective miner consensus protocol in blockchain oriented iot smart monitoring, 11 2018.

[16] Ahmed Ben Ayed. A conceptual secure blockchain based electronic voting system. *International Journal of Network Security Its Applications*, 9:01–09, 2017.

[17] 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 *40th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO 2007)*, pages 183–196, 2007.

[18] R. Bosri, A. R. Uzzal, A. A. Omar, A. S. M. T. Hasan, and M. Z. A. Bhuiyan. Towards a privacy-preserving voting system through blockchain technologies. In *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 (DASC/PiCom/CBDCom/CyberSciTech)*, pages 602–608, 2019.

[19] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. volume 8, 10 2000.

[20] I.-C Lin and T.-C Liao. A survey of blockchain security issues and challenges. *International Journal of Network Security*, 19:653–659, 09 2017.

[21] R. Bulut, A. Kantarcı, S. Keskin, and Ş. Bahtiyar. Blockchain-based electronic voting system for elections in turkey. In *2019 4th International Conference on Computer Science and Engineering (UBMK)*, pages 183–188, 2019.