Towards Developing a Secure and Robust Solution for E-Voting using Blockchain

Harsh Jain
Department of Information Technology
Dwarkadas J. Sanghvi College of Engineering
Mumbai, India

Rajvardhan Oak
School of Information
University of California
Berkeley, USA

Jay Bansal
Department of Computer Science & Engineering
M.B.M. Engineering College
Jodhpur, India

***Abstract*—Blockchain is one of the upcoming technologies in computing. It provides a tamper-proof distributed ledger which ensures integrity and authentication, as well as eliminates the need of a centralized trusted authority. This results in a secure and trusted system observed by the public. Although the blockchain was first applied to cryptocurrencies (which resulted in bitcoin), the features it provides are desirable for several other applications. In this paper, we develop a blockchain-based solution for securely digitizing the voting process. Election process is an important test of democracy and rigging the election may have disastrous consequences. Through our solution, we aim to provide a platform for voters to cast their vote securely online, from their home. The votes will be published in the blockchain, which will be observable by everyone. This would result in a tamper-proof ballot system which would be impossible to manipulate. The anonymity of voters will be maintained. We aim to apply this in the Indian context. We further show how our system meets the requirement of an online voting system, and how it resolves the issues present in current as well as proposed systems for the same.**

Keywords—Blockchain, Mining, E-Voting, Online Voting

I. INTRODUCTION

Blockchain [1][2] is an innovation which has proved to be very promising. The new blockchain technology is being applied in the domains of Healthcare [3], education [4], manufacturing [5], multimedia sharing [6] and several others.

At its core, blockchain provides us with a distributed ledger that can be seen and maintained by all the participants in the network. The ledger comprises of a number of 'blocks' (collection of transactions). The blockchain ledger is essentially a linked list where the links between various blocks are maintained using hash pointers. Every block includes the hash of the previous block it wishes to extend the chain on. Due to use of hash pointers, the blockchain is virtually tamper-proof. In order to change an existing transaction, one has to change the corresponding hash value. This would also mean changing the hash value of the next block and so on.

A schematic diagram of the blockchain network [1] is shown in Fig. 1. The blockchain functions on the principles of distributed consensus. Decisions about validity are taken collectively by all the participants. There is no central authority that has to be trusted. In a blockchain environment, all transactions are broadcast to the nodes in a P2P network. The nodes collect various transactions into a block and propose it as the next correct block by computing some value like proof of work [2]. This implies that more than 50% of the nodes must be malicious in order to subvert the process. Even then, it is quite difficult to attack the system.

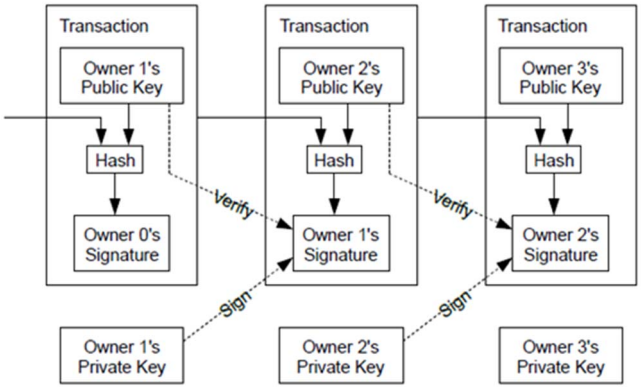

Fig. 1 Blockchain Network [1]

As the honest nodes always extend the longest existing chain, the probability that the attacker would succeed in catching up is very low [1].

Thus, a blockchain model is secure, transparent, decentralized and immutable. The most renowned use case of the blockchain is bitcoin [1], which also denotes the integration of the security properties (confidentiality, integrity and authentication) using digital signature schemes.

The properties of the blockchain discussed so far are extremely desirable for a voting system. The purpose of this research is to exploit the blockchain for digitizing the electoral process. If this is achieved, the entire election process will be transparent to the public. Everyone will be able to observe the ongoing progress, and the number of votes cast. Analogous to the "miners" in a bitcoin network, this model will have bots

978-1-5386-9166-3/19/$31.00 ©2019 IEEE

working as miners. Alternatively, this task may also be assigned to volunteers/election officials with some incentive [2].

The issues like rigging of the Electronic Voting Machines (EVM) will also be resolved. Each eligible voter will have a key pair. Thus, although the votes are published in the blockchain, the secrecy of the ballot is maintained as they will be encrypted.

Section II presents an overview of the current research regarding electronic voting and use of blockchain in voting. Section III describes our proposed model and underlying algorithms for the E-Voting system. Section IV discusses the results obtained and analysis of the system which includes the advantages and drawbacks of our system. The paper ends in Section V with conclusion and direction for future work.

II. Related Works

A. Online Voting Systems

E-Voting systems have been researched extensively over the past few years, especially after the dot com revolution. Estonia was the first country to adopt a fully digital election system in 2005 [7]. Switzerland has also begun work on a project called 'remote voting' [8][9]. According to our analysis, though the proposals outlined in [9] encourage participation of citizens in the election process, none of these are as secure and transparent as the blockchain. Such e-voting remains prone to malignant activity and hacking attacks [10][11].

In [12], a ranked choice e-voting system has been proposed that uses homomorphic encryption [13]. The algorithms used in this research are inspired by the approval voting algorithm. The homomorphic property makes it possible to poll all the ballots without decrypting them and viewing the content of any specific ballot.

The authors in [14] have described their E-Voting platform in which they implement image-based steganography along with standard cryptographic primitives. According to the authors, the most suitable approach to be used in this voter-verifiable voting scheme is F5 algorithm (image steganography with DCT coefficient technique). This scheme provides resistance against coercion to some extent.

Several other voting mechanisms have been proposed [15][16][17]. Although the models will simplify the election process, they still suffer from the same problems of security, integrity, immutability and lack of transparency as the traditional models. In addition, they assume that the central authority is trustworthy and will not tamper with the election process.

B. Blockchain-based Voting Systems

A huge amount of research has been performed in blockchain applications [3][4][5][6] since the introduction of blockchain and bitcoin. One such application is the E-Voting systems. In [18], a system has been designed which uses the blockchain to store the election and voting data. However, the blockchain advantages are not exploited. The system is still paper-based and is vulnerable to a number of attacks [18].

The work in [8] shows promising advances towards using blockchain for elections. In the research [8], the authors have used the Ethereum platform [19], which provides a framework to record any structural data into a blockchain. Smart contracts are used to enforce the rules of the election. As it is based on Ethereum, it also provides the feature of self-tallying [8][9].

In [20], another blockchain-based solution to E-Voting has been proposed. Instead of the standard Proof-of-Work [1][2], it uses turn rules. It uses a permissioned blockchain where the nodes of the blockchain are the voting centers.

Though online voting solutions (both with and without the use of blockchain) exist in the literature, they have some major issues described as follows:

- Most of the non-blockchain models face the problem of centralization, security, transparency and tampering.
- Some existing blockchain models are vulnerable to attacks [18]
- Some of the existing models, such as [8], require the voters to spend a small amount of the cryptocurrency.
- None of the existing models are fully online solutions.
- Some models are paper-based while some still require the voters to vote at a voting booth.

We aim to address these issues through our research.

III. Proposed System

The aim of this research is to develop a fully online and blockchain-based solution to the voting process. Elections are at the heart of a democracy, and thus fairness in elections is essential. Today, there is a lack of trust in the voting infrastructure due to rigging of voting machines, votes being changed internally by malpractices, etc. There is a need for a transparent and trustworthy system which can store the election data. This is the principal motivation behind this work.

The process of the proposed system has been described in Fig. 2.

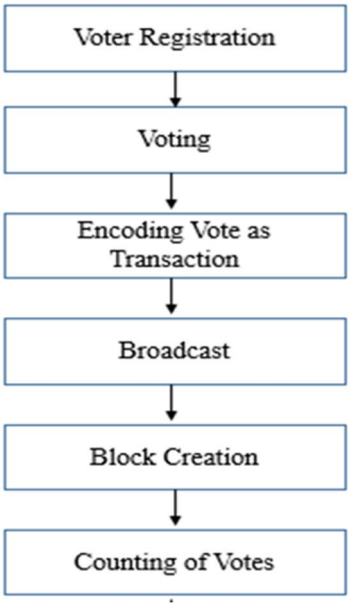

Fig. 2 Election Process

First, every voter will register for the election by generating a public key-private key pair. The process of registration gets completed before the election. On the election day, the voters will use their keys to cast votes. Then, every vote cast will be encoded into a specified transaction format. Miners (bots or incentive-driven individuals) will collect the transactions and subsequently publish it in the blockchain. This will be publicly visible, and anyone may observe the ongoing transactions.

Once the election gets completed, a common key-pair, used while encoding the votes into transactions, is made public for displaying the result.

Following is a detailed description of each step of the proposed system:

A. Voter Registration

The voters will have to register themselves prior to the election. They will generate their own public-private key pair online. For the registration, they will have to mention their Aadhaar card [15][16] and Voter ID details. Standard checks of eligibility to vote (age, citizenship) can be carried out using the Aadhaar UID Database. The voter will be verified using a One-Time-Password (OTP) sent to the registered contact number. As the Aadhaar cards are now linked to mobile numbers, this authentication is easy. One Aadhaar card may be linked to at most one mobile number; thus, every voter will have only one key pair. After successful registration, a key pair will be generated along with a registration ID which will denote the area code, constituency and other details. As a result of the registration ID, a voter will be able to vote only in the constituency in which he resides. This process has been described in Fig. 3.

An alternative to this registration process is physical and on-site registration. Voters will register using their Aadhaar details and biometrics and the key pair will be generated for them. This would prove to be useful for those who do not have access to, or are unable to use the internet and OTP mechanism.

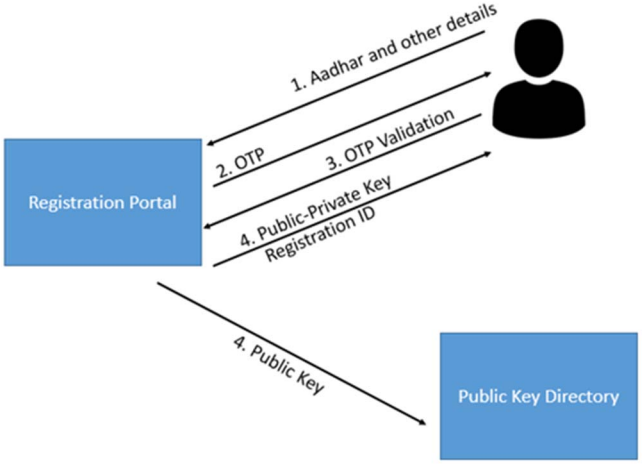

Fig. 3 Voter Registration

B. Voting

Voters will cast their vote online using a web portal or mobile application. First, the voter will enter his registration ID. Based on that, the portal will display the names of only those candidates, to whom the voter can vote. The voter will then vote for the preferred candidate. While doing so, what he will essentially be doing is creating a transaction with his public key and the hash value of the candidate (vote) and signing it with his private key. The vote, in the form of a transaction, is broadcast to a P2P network. The proposed transaction message format is shown in Fig. 4.

Transaction ID
Voter Public Key
Vote
Timestamp
Random Nonce
Digital Signature

Fig. 4 Transaction Format

In Fig. 4, the 'vote' field refers to the candidate for whom the voter has voted. The digital signature of each transaction will be encrypted using a common public-private key pair. The key-pair will be displayed on the portal after the elections get over. Once the key-pair is made public, all the blockchain users will be able to decrypt the signature and see each vote, which exhibits transparency.

After the transaction has been broadcast, the voter will be marked as having already voted, and will not be able to vote again. Even if some attacker somehow subverts this process, the duplicity will be visible in the blockchain, which is, of course, free to be examined by anyone. A point to be noted here is that since we publish only the public key and not the Aadhaar number of the voter, it is impossible to link a vote back to a specific individual.

The entire voting process has been depicted in Fig. 5

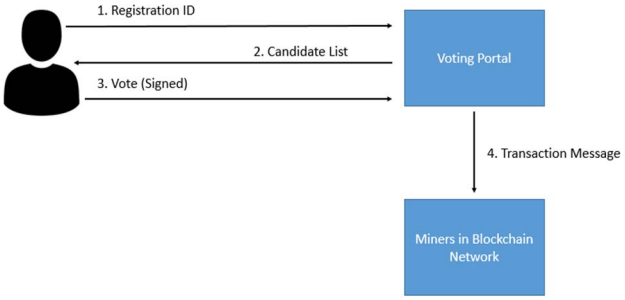

Fig. 5 Voting

C. Block Creation

In our system, the miners are bots who will compute the Proof-of-Work or some alternate proof [2] and create the blocks. A fixed number of transactions will be accumulated to create a single block. Miners will then compute the value for a random variable, called nonce, such that the hash value of the block achieves a predefined target. The structure of a block is shown in Fig. 6. This task, called mining, may also be outsourced to voluntary individuals and awarding them with some incentive, so that they remain honest and do not engage in malpractices. The quantity of transactions/votes in a block is a design choice. A blockchain will be formed by the blocks linked together via the hash pointers. Each block will include the hash of the previous block.

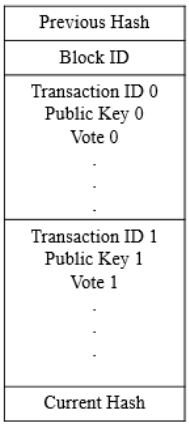

Fig. 6 Block Format

D. Vote Counting

As the votes will be counted programmatically from the public blockchain, it will not take a lot of time. A simple module will traverse the blockchain and count the votes for each candidate. The results will be released towards the end of the elections after the release of the common key-pair. This will also solve any problems of violence and subsequent coercion. Another option is to maintain a structure in each node of the Merkle Tree [1][2]as is done for the Proof-of-Reserve [2]. In addition, before announcing the results, some time may be allotted for individuals and third parties to independently examine the blockchain for double votes or incorrectly validated blocks. This step will further increase the confidence of the voters in the blockchain.

IV. Results And Discussions

The proposed model was implemented and tested for the functionality. RSA was used as the encryption scheme.

If the user attempts to register using an already registered Aadhaar number or Voter ID, it would be an unsuccessful registration attempt which is handled by the system as shown in Fig. 7 and Fig. 8.

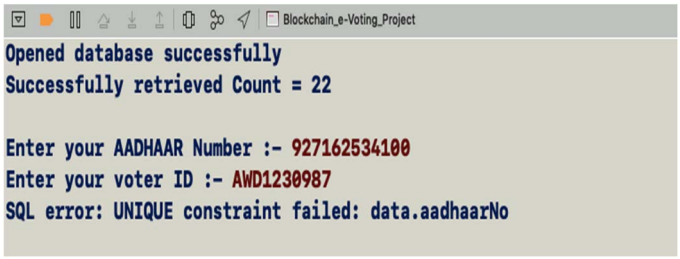

Fig. 7 Unsuccessful registration due to already registered Aadhaar number

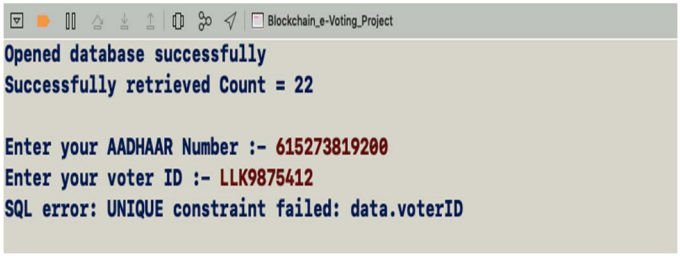

Fig. 8 Unsuccessful registration due to already registered voter ID

Fig. 9 depicts successful registration of a voter. Fig.10 shows the state of database after the successful registration.

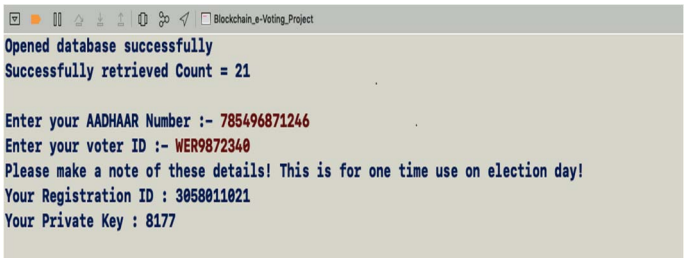

Fig. 9 Successful registration

	regID	aadhaarNo	voterID	d	n	votedFlag
	Filter	Filter	Filter	Filter	Filter	Filter
2	3058011001	882937162344	AWS1239287	67	13733	0
3	3058011002	192837526345	PAW1291827	101	5549	0
4	3058011003	627888291092	WQP9281723	71	2449	0
5	3058011004	928881723615	WEK8917200	41	6107	0
6	3058011005	927162534100	QMN9102836	101	8153	0
7	3058011006	266371892007	KKA1291928	89	9517	0
8	3058011007	354213465879	RIP0004587	47	4681	0
9	3058011008	745986321450	KKO4789563	37	8339	0
10	3058011009	887649815436	ASD7897894	37	8711	0
11	3058011010	455658789652	AQW7778542	11	3007	0
12	3058011011	448596321400	LLK9875412	53	16771	0
13	3058011012	775469821033	DDE7845210	71	4867	0
14	3058011013	741025896301	POL7845126	23	15469	0
15	3058011014	452100230012	POL7755330	19	341	0
16	3058011015	985665899856	MNO7410896	67	7471	0
17	3058011016	445102020100	QQW1594832	11	4309	0
18	3058011017	567887654321	AQW3456789	67	5611	0
19	3058011018	212354568789	UIO2125478	53	527	0
20	3058011019	129384756002	SDF1256439	13	13423	0
21	3058011020	455478879652	ASE4786932	43	7099	0
22	3058011021	785496871246	WER9872340	53	14477	0

Fig. 10 Database after successful registration

If the user attempts to vote using incorrect private key or tries to vote again using the same registration id, it would be an

unsuccessful voting attempt which is handled by the system as shown in Fig. 11 and Fig. 12.

```
Opened database successfully

Enter registration id :- 3058011009

These are the candidates for your zone :-
1. Jay Bansal
2. Harsh Jain
3. Rajvardhan Oak
4. Paul Thomas

Select your choice (1-4) :- 2

You are going to vote "Harsh Jain"

Enter your private key :- 8172

Invalid Reg. Number/Private Key combination!
```

Fig. 11 Unsuccessful voting due to incorrect private key

```
Opened database successfully

Enter registration id :- 3058011021


This registration ID has already voted!
```

Fig. 12 Repeated voting denied

The successful voting procedure is shown in Fig. 13. The state of database after successful voting is shown in Fig. 14.

```
Opened database successfully

Enter registration id :- 3058011021

These are the candidates for your zone :-
1. Jay Bansal
2. Harsh Jain
3. Rajvardhan Oak
4. Paul Thomas

Select your choice (1-4) :- 3

You are going to vote "Rajvardhan Oak"

Enter your private key :- 8177

Voted "Rajvardhan Oak" through Reg. number 3058011021 successfully!
```

Fig. 13 Successful Voting

	regID	aadhaarNo	voterID	d	n	votedFlag
	Filter	Filter	Filter	Filter	Filter	Filter
1	3058011000	928786323400	AWS9102999	19	8401	0
2	3058011001	882937162344	AWS1239287	67	13733	0
3	3058011002	192837526345	PAW1291827	101	5549	0
4	3058011003	627888291092	WQP9281723	71	2449	0
5	3058011004	928881723615	WEK8917200	41	6107	0
6	3058011005	927162534100	QMN9102836	101	8153	0
7	3058011006	266371892007	KKA1291928	89	9517	0
8	3058011007	354213465879	RIP0004587	47	4681	0
9	3058011008	745986321450	KKO4789563	37	8339	0
10	3058011009	887649815436	ASD7897894	37	8711	0
11	3058011010	455658789652	AQW7778542	11	3007	0
12	3058011011	448596321400	LLK9875412	53	16771	0
13	3058011012	775469821033	DDE7845210	71	4867	0
14	3058011013	741025896301	POL7845126	23	15469	0
15	3058011014	452100230012	POL7755330	19	341	0
16	3058011015	985665899856	MNO7410896	67	7471	0
17	3058011016	445102020100	QQW1594832	11	4309	0
18	3058011017	567887654321	AQW3456789	67	5611	0
19	3058011018	212354568789	UIO2125478	53	527	0
20	3058011019	129384756002	SDF1256439	13	13423	0
21	3058011020	455478879652	ASE4786932	43	7099	0
22	3058011021	785496871246	WER9872340	53	14477	1

Fig. 14 Database state after successful voting

The performance of the system was analyzed as per the parameters outlined in [21][22][23] for any voting system to work properly.

- **Eligibility**: Only legitimate voters are able to cast a vote. Our system ensures this constraint, as non-eligible voters will not be able to register and obtain a key pair.
- **Multiple Voting Detection**: All voters should be permitted to cast only one vote. This is checked in our system, as every voter has a flag indicating the voting status.
- **Privacy of Voters**: The secrecy of the ballot is maintained. Although in our system, the public key of the voter would be visible, it is impossible to tie this to the real-world identity.
- **Integrity**: No one should be able to change a previously cast vote. This is enforced as our data is being published in the blockchain. Since every block includes the hash of the preceding block, a change in a single vote would lead to the hash pointers not matching up and will require very high computing power to recalculate all the changed hashes.
- **Correctness of Result**: Only verified and valid ballots should be counted. In our case, only valid votes shall be present in the blockchain and the vote count would be automatic.

Our system has several advantages as compared to the traditional electoral models as well as many of the online voting systems.

- **Security:** The votes are secure due to the use of strong encryption algorithms.
- **Fast Results:** The vote counting will be extremely speedy. Furthermore, anyone may examine the blockchain and verify the results.
- **Digitization:** With a fully digital system, individuals may cast their vote online. There is no need of election booths.
- **Transparency:** With the use of the blockchain, the entire voting will be essentially public, and at the same time maintaining the secrecy of ballots. As the citizens can see the blockchain, statistics like the final result and the percentage of voters, who cast their vote will be publicly verifiable.
- **Paperless Voting:** Our system is entirely digital, and requires no paper ballots. In addition, as voting will be done by each individual online, the need of associated paperwork also decreases.
- **Cost and Resource Saving:** The expense incurred in the security of the booths, personnel required for booth management, voting machines will be reduced. As the entities required to maintain the integrity of the system are miners (bots), the only expense will be the computation power required to run the miners.

A comparison of our model with the existing methodologies is shown in Table I

TABLE I

Sr. No	Parameter	Existing Models	Proposed Model
1.	Transparency	None	Fully transparent and observable
2.	Fully Digital	No	Yes
3.	Speed of Result	Low	High
4.	Privacy	Less, as voters need to visit the voting booths	High, as voting is done from home
5.	Risk due to EVM rigging	High	None

V. Conclusion And Future Scope

Blockchain provides us with a distributed, tamper-proof ledger which is ideal for the election process. We have proposed a novel model in which the blockchain is exploited to develop a secure, transparent and fully digital voting system. We have allocated a unique key pair to every individual, and votes are recorded in the blockchain. This results in a fully transparent system. Due to use of the existing Aadhaar infrastructure, the implementation is feasible.

There is tremendous scope for future research and improvement in this system. The system will be further improved if we are able to design a simple, yet secure puzzle instead of the proof of work. The system will become more secure if we are able to solve the coercion resistance problem. An improvement in the underlying cryptographic algorithms will also make this system resistant against various attacks as well as quantum computing. We aim to address these issues in future research work.

Acknowledgment

We acknowledge the contribution of Dr. Abhijit R Joshi and Dr. Neepa Shah for their useful suggestions and for proof-reading the paper.

References

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Online: https://bitcoin.org/bitcoin.pdf, accessed on 16th June 2018.

[2] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, “Bitcoin and Cryptocurrency Technologies” Available at:https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1, accessed on 16th June 2018

[3] Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu, Danyi Li, “Integrating blockchain for data sharing and collaboration in mobile Healthcare applications”, 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)

[4] S. Streng , R. Atterer, "Non-Invasive Collaboration Aids: Supporting Group Learning With Pervasive and Ambient Technologies, 2008 International Conference on Computer Science and Software Engineering, 2008.

[5] R. Latif, H. Abbas, and S. Assar, “Distributed denial of service (DDoS) attack in cloud- assisted wireless body area networks: a systematic literature review,” Journal of Medical Systems, vol. 38, Article 128, 2014.

[6] Deepayan Bhowmik; Tian Feng, “The multimedia blockchain: A distributed and tamper-proof media transaction framework”, 2017 22nd International Conference on Digital Signal Processing (DSP).

[7] F. Ho, P.Y.A. Ryan, Real-World Electronic Voting: Design, Analysis and Deplyment, CRC Press, pp. 143-170, 2017.

[8] Emre Yavuz; Ali Kaan Koç; Umut Can Çabuk; Gökhan Dalkılıç, “Towards secure e-voting using ethereum blockchain”, 2018 6th International Symposium on Digital Forensic and Security (ISDFS)

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

[10] M. Gregory, Electronic Voting May be Faster but Carries Security Risks, 2016, [online] Available: http://www.theaustralian.com.au/business/technology/opinion/electronic-voting-may-be-faster-but-carries-security-risks/news-story/f0b6b44844214605e3860ef1887b2bb9.

[11] J. Lavelle, D. Kozaki, Electronic Voting has Advantages but Remains Vulnerable to Security Software Problems, 2016, [online] Available: http://www.abc.net.au/news/2016-07-11/electronic-voting-has-support-but-security-fears-remain/7587366.

[12] Xuechao Yang; Xun Yi; Surya Nepal; Andrei Kelarev; Fengling Han, “A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption”, IEEE Access ,Year: 2018, Volume: 6, Pages: 20506 - 20519

[13] X. Yi, R. Paulet, E. Bertino, Homomorphic Encryption and Applications, New York, NY, USA: Springer, 2014.

[14] Z.A. Usmani ; Kaif Patanwala ; Mukesh Panigrahi ; Ajay Nair, “Multi-purpose platform independent online voting system”, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)

[15] Vishal; Vibhu Chinmay; Risabh Garg; Poonam Yadav, “Online voting system linked with AADHAAR”, 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)

[16] Himanshu Agarwal; G. N. Pandey, “Online voting system for India based on AADHAAR ID”, 2013 Eleventh International Conference on ICT and Knowledge Engineering

[17] Srivatsan Sridharan, “Implementation of authenticated and secure online voting system”, 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)

[18] Safdar Hussain Shaheen, Muhammad Yousaf, Mudassar Jalil, “Temper Proof Data Distribution for Universal Verifiability and Accuracy in Electoral Process Using Blockchain”, 2017 13th International Conference on Emerging Technologies (ICET)

[19] G. Wood, "Ethereum: a secure decentralized generalized transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[20] Rifa Hanifatunnisa; Budi Rahardjo, “Blockchain based e-voting recording system design”, 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)

[21] X. Yang et al., “A verifiable ranked choice Internet voting system," in Proc. Int. Conf. Web Inf. Syst. Eng. (WISE), 2017, pp. 490-501.

[22] J. Dreier, P. Lafourcade, and Y. Lakhnech, “Defining privacy for weighted votes, single and multi-voter coercion”, Proc. Eur. Symp. Res. Comput.Secur. (ESORICS), 2012, pp. 451-468.

[23] A. O. Santin, R. G. Costa, and C. A. Maziero, “A three-ballot-based secure electronic voting system," IEEE Security Privacy, vol. 6, no. 3, pp. 14-21, May 2008.