Online Voting System in Pakistan using Blockchain Technology

Tehmina Kausar[1], Aftab A. Malik[1],Waqar Azeem[1], Mujtaba Asad[2]

***Abstract*—The election system is one of the most endured issues in numerous nations. Control on votes, unsafe automated voting devices, altering of ballots, and balloting place apprehending are the alarming problems that are to be talked about in an existing balloting network. Blockchain innovation is the answer to defeat the above issues and to give a secure balloting network. This innovation is successful in providing an answer to problems like safety, reliability, and verification. Blockchain technology can be used to execute a secure and safe voting process. In this paper, an E-balloting system is suggested for Pakistan, which depends on the application of Blockchain, to make sure the secrecy of democratic procedure. A previously distributed ID (identity) and the secret password are included as an additional layer of security to avoid dual voting. A design is presented for the implementation of a blockchain-based technique for the voting system in Pakistan. The engineering and structure of the proposed framework are also presented. The suggested framework is tamperproof, and any attempt to change or alter the casted votes could be identified through unusual .hash lengths**

Keywords: **Automated, Blockchain, Authentication, Democratic, Framework & Innovation.**

INTRODUCTION

Democratic voting in any country is the most important event that allows its citizens to exercise their power by voting and electing the representatives. To protect the right of citizens to conduct fair elections is the basic prerequisite for any country [1]. A lot of time and money is spent to hold elections. Pakistan is one of the large democratic countries. Nearly 107.5 million people are registered voters [2] but still, an outdated voting system is used which is held by a central authority. In outdated voting schemes paper ballots are used to cast votes. Voter stamps on the paper ballot to mark their choice of candidate. Generally, these ballots were physically counted and that's why there is always a delay in the election process. There are a lot of disadvantages to the outdated voting system that as the chance of ballot filling, the use of adding ink to produce fake results, fake procedures, violation of privacy, planned errors in calculations, and slow counting [3]. An Ideal voting system has the properties such as comprehensive examination of the records, Secrecy Transparency, Coercion, and confrontation [4].

[1]Lahore Garrison University Lahore
[2] Shanghai Jiaotong University, China
Email: * tehmina.kauser@gmail.com

Unlike simple voting, the e-voting system gives the facility to the voter to vote according to their ease and from anywhere which maximizes user participation. It also provides Security, Accessibility Auditability, Efficiency, Reliability, Accuracy, and quick publication of results. Despite the advantages, there are many drawbacks to the existing system. Some of the common vulnerabilities are voter privacy; identity theft and Immutability [5, 6]. To overcome the above-mentioned vulnerabilities blockchain-based e-voting system is introduced. Blockchain technology got much consideration in recent years because of its higher resistance against hacking. Blockchain technology is base on the distribution principle many copies of the data are sent over the network, but all are replicas no one is the original file. It's a transparent technology so all the members of the network can see the transactions. It's a combination of cryptography mathematics and algorithms [7]. So due to the above-mentioned properties, a blockchain-based e-balloting system provides secrecy, correctness, and immutability [8, 9]. The blockchain-based e-balloting network is in practice in many countries and successfully working. The present research work proposed in an implementational way for a blockchain-based e-balloting systemin to improve the existing system. The proposed architecture depends on the ideas of Blockchain. This paper presents a technique to investigate the use of Blockchain technology to search for solutions to the problem in the voting system. Blockchain technology has a constructive influence on our social life. This framework will help increment the number of voters just as the trust of individuals in their legislature.

The paper is arranged as follows: section 2 illustrates the defects in the present system as motivation, section 3 portrays the relevant work, section 4 gives a short presentation on the blockchain innovation and the cryptographic hash work, section 5 explains the proposed system, section 6 shows the analysis of the proposed system and section 7 presents the conclusion.

MOTIVATION

Pakistan has a history of voting challenges. In the 2018 elections, numerous incidents of voting rigging were wide-open during a NADRA investigation. In the 2013 elections, a slew of violent incidents starting from kidnappings to bomb blasts created widespread fear and disrupted the voting environment on polling day [3]. All over the world Elections are expensive and Pakistan is not diverse on this count. A lot of time and money is spent to hold elections. Blockchain-

based elections can minimize the above danger by providing anonymity, allowing citizens to vote without fear of payback. Blockchain-based elections also allow for protected remote ballots, giving them the ability to the user to vote safely from their phones or computers. Blockchain-based elections reduce pressure, save time, easy to monitor and stop manipulations [8, 9]. Our principal inspiration in this venture is to give a safe democratic condition and show that dependable voting conspires are conceivable utilizing blockchain. Since, when voting is accessible for everybody who has a PC, or a cell phone, an assessment will be increasingly open and progressively available by legislators and directors. This will ultimately lead the human race to true democracy. It is also important because nowadays it's easy to corrupt or change the elections plus manual voting process is very expansive Additionally, the voters may be on a holiday, on work excursion, or distant for whatever other explanation, which will make it unthinkable for that specific voter to go to the political decision. This will increase the general participation of voters [10, 11].

LITERATURE REVIEW

Blockchain-based voting systems have been suggested in many research papers as a result of the existing challenges of online voting systems in simple online voting systems data is stored in a central server. Which is still not secure. These complications can be improved using a dispersed system in which each hub in the system has its copy of the information. To offer safety to the information kept in such a system, a blockchain-based safety mechanism is used. In [5]. Blockchain is used to store given votes and acts as a role as an indisputable database. This framework utilizes Secure HTTP. Blockchain voting system involve\s the stages such as (a) Logging in, (b) ID creation, (c) Re-logging, (d) Constituent Expert planning, (e)Balloting, and (f)Vote count. Candidates and their participants will acquire results as soon as the votes are received. In [7], EVM electronic democratic machine utilizes has been discussed with special unique mark distinguishing proof technique. A voter thumb impression is utilized for recognizing the voter. EVM is utilized to catch the fingerprints. Then one of a kind imprints is inspected and is sent for affirmation. That is matched with present database catalogs. The database catalogs are inserted safely with the support of blockchain. All the elector's intriguing distinctive verification nuances like name, age, address, DOB (Date of Birth), exceptional finger impression, and iris check are entrenched and established in the blockchain. At that point, this data is stored in the blockchain to check the votes. Examined stand-out interesting imprint tries to encourage with the present square where vote checks spared. Each time an entire procedure is a rehash if unique mark coordinate, at that point vote as in [3], Putting away the vote information in a decentralized system and making sure about the information utilizing a security instrument got from the blockchain structure (which is as of now utilized for making sure about cryptographic forms of money). The vote information is shared between all the gadgets in the system and distributed affirmation is done to affirm the legitimacy of the vote information. To successfully change the framework, the information put away in all the hubs was adjusted. This makes the framework increasingly compelling and reliable. In this paper, a calculation is also proposed, which depends on the ideas of blockchain, to make sure about the votes put away in an EVM. A unique finger impression confirmation framework is additionally included as an additional layer of security to forestall twofold democracy. In [12], the proposed framework utilizes blockchain confirmation to make an improved democratic cycle. Filtering the QR code on the elector's identity number, the database on identity number is acquired. This data is checked and confirmed. Regardless the elector is from the correct municipal, age is 18 or more, and whether the elector has just cast ballot. If the data is checked to be legitimate, the voter can project his ballot. This ballot is then recorded in a blockchain record. This cycle is rehashed for additional electors. This framework goes on to a private organization, where the head of the discretionary advisory group has the freedom to choose the initiating. Season of the democratic cycle. The cycle monitors a dispersal methodology such that any qualified resident can decide in favor of the ward from any place in the state.

BLOCKCHAIN AND HASH FUNCTION

Blockchain is a chain of squares that contains information. This system was first portrayed by the authorities in 1991 and was at first proposed to timestamp electronic documents. Therefore, it's unreasonable to temper with them. Blockchain is a passed-on record that is thoroughly open to everybody. It has entrancing stuff once the data has been noted within the blockchain it turns out to be uncommonly difficult to transform it. Each block holds a couple of data the hash of the block and the hash of the past block. The information that is stored inside the block endless supply of blockchain; the bitcoin blockchain, for example, stores the exchange, sender, beneficiary, and coins. A square furthermore has a hash. The hash and fingerprints can be differentiated easily. It separates a block and its beginning and end of substance and it's reliably stand-out also as a one-of-a-kind finger impression. At the point when a block is made, its hash is resolved, modifying to some degree within the block will make the hash modify [13]. So, as such hashes are incredibly useful when users have to perceive the movements of blocks. In case the extraordinary characteristic of the block changes it never again is the comparative block. The third part inside each block is the hash of the past block. This strategy makes the blockchain so secure. Fig. 1 shows the generalized blockchain structure that can also be implemented for the voting system.

Blockchain has something which is called evidence of work. It's a component that hinders the formation of another block. This system makes it difficult to mess with the block in such a case that you mess with one block you have to recalculate

the evidence of work all the accompanying blocks. The security of blockchain originates from its imagination of hashing and its confirmation of work instruments [13]. There is one all the

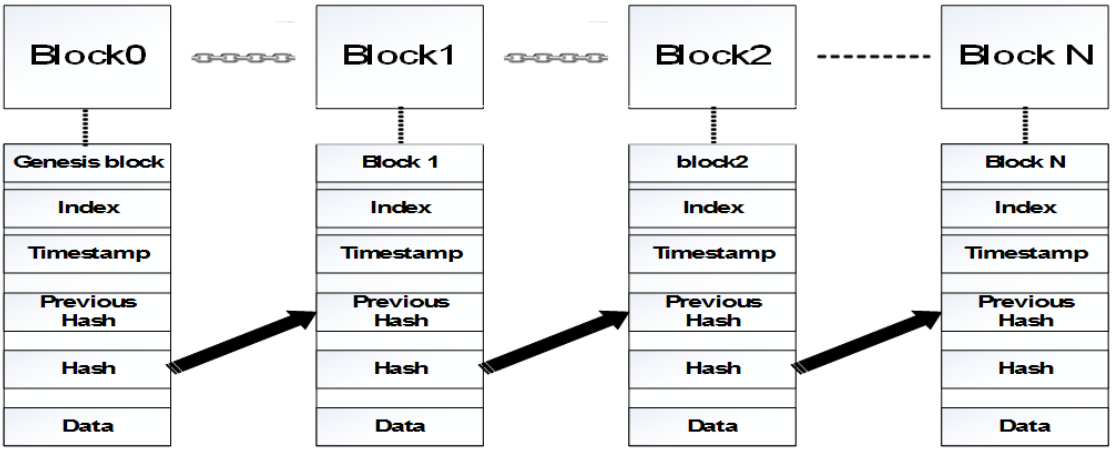

Fig. 1 shows the generalized blockchain structure

more way that blockchain made sure about itself and that is by being conveyed. Rather than utilizing a focal element to manage the chain, blockchain utilizes a P2P (Peer to Peer) system and everybody is permitted to join. In a P2P network, peers are the computers, connected via the Internet. Files are shared directly between systems on the network without requiring the need for a central server. At the point when somebody joins this system, he gets four duplicates of the blockchain. The hub can utilize this to check that everything is still all together.

Blockchain has many amazing things. (1) In blockchain for similar information, the users get similar hash esteem. (2) A little change in information can change the hash in an altogether different manner for example “hi world” hash will be changed from “Hi world”. (3) You can’t get a genuine contribution from the hash esteem that is the mean opposite is absurd. Hashing isn’t encryption because, in encryption, a node can get information back utilizing unscrambling however that is not the situation with hash. That is the reason in hashing, a lot of information could be lost. (4) For two unique messages, there are two diverse hash esteems, if messages have similar hash esteems it’s known as a clash [13-14].

A) Working

A Blockchain is a record or worksheet containing information about transactions. Each transaction makes a hash. A hash is an evolution of figures and alphabets. Trades go in the solicitation where they happened. The solicitation is difficult. The hash is dependent on the transaction just as on the past transaction hash. Undoubtedly, even a small modification in return makes an undeniably new hash. The center points check to guarantee a trade has not been changed by evaluating the hash. In case a trade is supported by a lot of the centers, then it is formed into a square. Each square insinuates the previous square and makes the Blockchain. A Blockchain is conclusive as it is spread over numerous Machines, all of which have a copy of the Blockchain. The PCs are called center points. The Blockchain resuscitates itself at customary stretches [15-17]. Fig. 2 shows the working of various blockchain nodes to complete a transaction

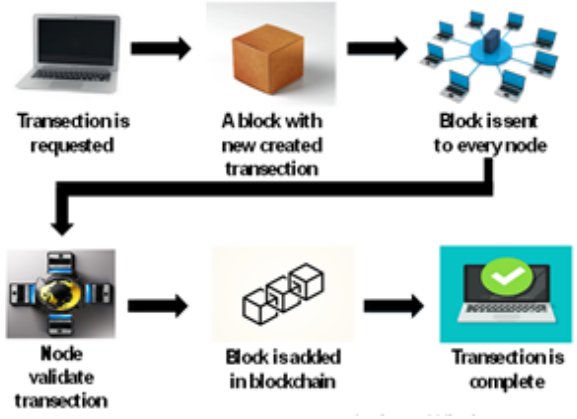

Fig. 2. Working of Block Chain [22].

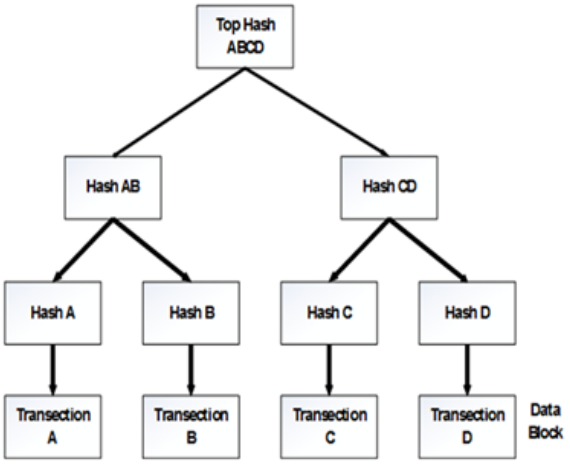

Fig. 3. The Merkle Tree Structure [23].

B) ***The Merkle Root***

Another concept that is used in our proposed system is the Merkle root. A Merkle root is the hash of the apparent multitude of hashes of the apparent multitude of exchanges that are essential for a square in a blockchain network. It is a basic numerical approach to confirm the information on a Merkle tree. There are various exchanges put away on a specific square, all the exchange hashes in the square are additionally hashed, which brings about a Merkle root. The hashing begins at the most minimal level hubs, and every one of the four hashes is remembered for the hash of hubs that are connected to it at level one. Thus, hashing proceeds at level one, which prompts hashes of hashes coming to more elevated levels, until it arrives at the single top root hash. Fig. 3 shows the root hash flowchart, that root hash is known as the Merkle root [18-22].

PROPOSED SYSTEM

This section depicts the engineering, plan, and arrangement point of view of blockchain-based elections. The model was structured and worked as a delineation of the confirmation of the idea that blockchain innovation could without a doubt be utilized to conduct the election. The model can't be straightforwardly received as an undeniable voting framework. It would require a few customizations and changes to be fused that are by the democratic procedure.

A) System Design

The suggested system design is contemplated for an electronic balloting design in Pakistan. In Pakistan, there are four provinces. Each province holds several cities and each city holds many union councils (UC). The whole system model is presented in Fig. 4. Now, the election commission of Pakistan wants to conduct polls. Each province starts the balloting procedure. Each vote under the union council makes a block and each block combines to create a blockchain. At the end of balloting, the blockchain of every union council of a city combines to create a city blockchain. Then city blockchain combines to make a provincial blockchain and at last, provincial-level blockchain combines to make a country blockchain. The Election Commission of Pakistan will use this solitary blockchain for the ballot sum.it is accepted that the Election commission of Pakistan (ECP) is directing these elections with the cooperation of NADRA. Fig. 4 shows a generalized electoral system of Pakistan.

Fig. 4. Country system model for electronic balloting system

B) Framework of Electronic Balloting Design

The suggested framework utilizes blockchain innovation. The framework is dependent on 2 ideas: encryption and hashing. The framework holds the accompanying segments: participants= {Voters}, organizers= {Union council}, inspector= {Election Commission of Pakistan}, encryption algorithm are DES & AES, Hash algorithm is SHA-256 and balloting server. The accompanying advances are included when an elector needs to cast the vote in the balloting period. Details of the proposed electronic balloting system are given in the following algorithm and in Fig. 5 and 6.

C) Algorithm: Electronic Balloting Structure

1: Input :(User Id, user Password)
2: Output: blockchain base ballot
3: START

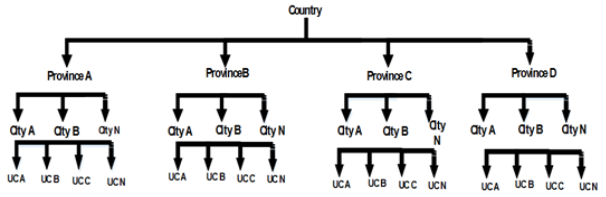

Fig. 4. Country system model for electronic balloting system

4: voter is already registered in the balloting system.
5: if (user ID == registered user Id) and (ID is not in database) then
6: Login (Enter personal information)
7: else
8: Non-registered voter + Block id after five attempts
9: if (information is correct + Not in database) then
9: choose the candidate and submit the vote
10: else
11: again, enter information
12: Encryption of balloting information - (V)
13: Signing the encrypted information - ((V))
14: Creation of the block - BLOCK (header + encrypted data)
15: Total votes-==
Where p = provinces, c =cities in a specific province, UC = union councils in a specific city.
16: END

Pre-balloting steps

a) The proposed model requires that all the registered voters already have an id and password given by the election commission of Pakistan.

Balloting steps

a) For the duration of the election, firstly voter needs to login into the system using voter ID and password. The first layer of security stops non-register voters to vote as mentioned above only register voters which have unique IDs and passwords can vote. If a user tries to login through a fake id and password after 5 attempts system will automatically block the ID. The system will check in the database through an ID that the user is voting the first time if NO id will move on the "hash 5 attempts" stage.

b) If the elector is authorized for casting the vote, at that moment the 2nd page opens, where the user will enter personal information. This stage provides a second layer of security. When users will enter personal information like name, DOB (Date of Birth), gender, and CNIC, the system will check through CNIC that the same information is already in the database if the YES, system will give the message" cast vote" if NO then the user will choose a political party and submit vote.

c) The vote is scrambled by utilizing the public key of the Election Commission of Pakistan.

d) The scrambled ballot is signed up by the elector's private key.

e) Presently, the produced elector data is kept in the elector server using the Internet. This is the primary block of the blockchain.

f) Steps 3 to 6 repeat to create blocks until the voting time is over.

Post-balloting steps

a) At the end of voting, the blockchain of every union council is combined for making a city blockchain.

b) The blockchain of every city is combined for making a provincial blockchain.

c) Now blockchain of every province is combined for making country blockchain.

d) Now, the election commission crisscrosses all the ballots from the blockchain and announces the final result of the balloting.

PROOF OF WORK

Proof of work (POW) includes making a substantial block hash that can be immediately confirmed by different clients on the organization. A useable hash happens only if the mathematical clarification of the hash is lesser than a prearranged trouble. The hash must be littler than the trouble to be acknowledged in the blockchain. Authenticating the hash of a block is very much unpretentious and rapid to do, where it can be assumed that a hash is already created. The encrypted vote data is entered in an unpretentious formulation to create a figure and later compare it with block hash. If the hash is lesser, the block is acknowledged, if the hash is greater, the hash is not valid. The following are the variables that are used for block generation. As already explained each block has a unique hash which is generated with the help of variable bytes.

Variable	Bytes	Description
ID	4	voter ID given by ECP
Timestamp	4	block creation time since 00:00 UTC
Signature	32	sign for encrypted data
PrevHash	20	previous block hash
Merkl Root	20	hash tree with SHA 256
Encryp vote	4	Encrypted vote data in compressed form

Suppose the hash of a block is

Hash

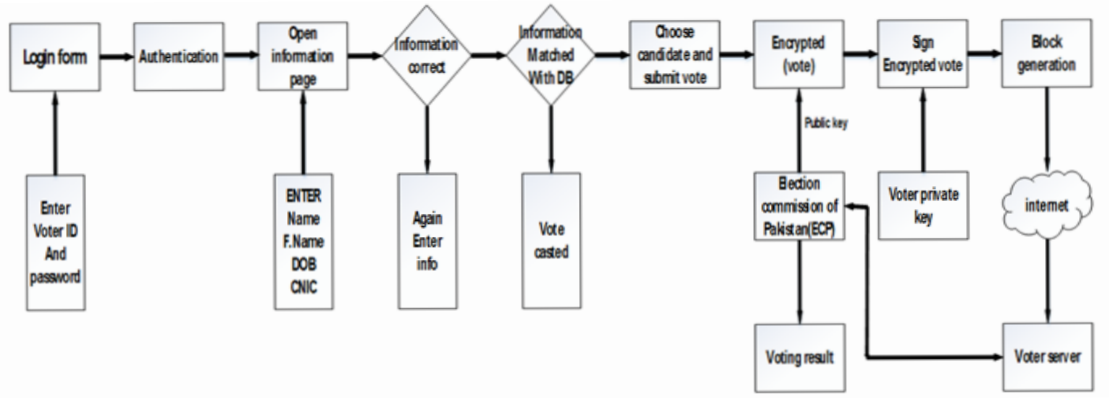

Fig. 5. Framework of the proposed electronic balloting system

000000000000000033d76d1979cbf908abb-
d9e94a5a7a84aedc51dd3aa0d022
a. For example, take a hash to check and encrypted vote data to compare it;

Hash=
000000000000000033d76d1979cbf908abb-
d9e94a5a7a84aedc51dd3aa0d022
Encrypted vote data = 1806b99f
b. use encrypted vote data, first byte as EXPONENT and the leftover as the MANTISSA.
EXPONENT == 18
MANTISSA == 06b99f
c. Put the figures in formula to get result;
Result == (0x) mantissa * 2^ (8 * ((0x) exponent - 3))
Result == 0x06b99f * 2^ (8 * (0x18 - 3))
Result == 0000000000000000006b99f00000
0000000000000000000000000000000000000000
EXPONENT-3 refers to the number of bytes on the right side of the MANTISSA
d. Is the hash lesser or equivalent to the trouble?

Hash=
000000000000000033d76d1979cbf908abb-
d9e94a5a7a84aedc51dd3aa0d022
Result = 0000000000000000006b99f0000000
0000000000000000000000000000000000000000
Hash < Result (hash is valid).r

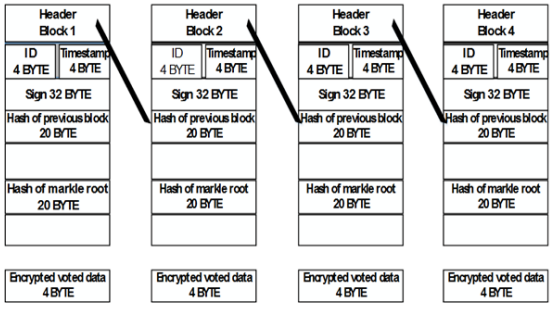

Fig. 6. Proposed Blockchain structure

System analysis

In this segment, design regarding safety, protection, and assaults were investigated. The proposed system has two ends frontend and backend. The frontend is a web page that works as a (GUI)Graphical User Interface that is constructed using HTML, CSS, and PHP. While Backend works as database (blockchain) is built using python

DATA TRANSMISSION PRIVACY

As indicated by the proposed framework, the country blockchain will be put away in the server. During the information broadcast, all the linked data is put away in the square and this square is protected against various assaults and dangers. In one way or another, if any client gets the squares, the assailant can't get any important data since all the information will introduce in a hash and encoded structure.

Elector secrecy

To give secrecy to the elector, like encryption and hash algorithm SHA-256 is used. Vote-related data is kept in an encoded structure. Due to the encoded structure, it is impossible to modify a block, that's why an attacker can't know about the vote. Along these lines, this method keeps up elector secrecy.

Doubling and Imitation in the System

A blockchain has been made o overthrow the imitation and doubling cases during the elections. To ensure that nobody will vote twice or more, a different unique ID is used. Our blockchain consists of three things Markle root hash, earlier block hash and signature. The signature gives validity and reliability to the transaction information.in blockchain, information reliability is sustained by using prior block hash. The root of the elector information is given by Markle root. Subsequently, our suggested e-balloting framework opposes the doubling and phony problem.

Storage space

The recreation of the suggested framework is done on the framework level. The thought of the necessary extra storage space for balloting is assuming a significant part in certifiable situations. During the balloting, for the capacity of one ballot exchange, that need 84 bytes. In these 84 bytes, the square contains citizen ID, timestamp, signature, a hash of past information, Merkle root hash, and scrambled ballot exchange information.

Comparison and validations

Table 1 shows comparisons and validation of the presented voting system with other blockchain-based applications. By managing the time stamps the electronic voting system can not only be made secure but could also provide transparency if required. The transaction fee for both Bitcoin and Ethereum coin is volatile and depends on multiple factors. Moreover, in the blockchain-based voting system transaction fee may not be required.

CONCLUSION

Blockchain innovation can be one response to deal with the issues that oftentimes occur in the balloting system. This research proposes an e-casting ballot architecture using blockchain technology to appropriately encourage digitalized decisions keeping up election and elector security even though forestalling extortion. The important steps of the design, specifically, log in through elector ID and password, elector information gathering, voting, and election tallying through blockchain are presented in this blockchain-based voting system.

In this system, there is zero chance of controlling or including

extra phony ballots. It is protected and secure and expands the accommodation of clients. Checking votes doesn't take tremendous time. It is a spending plan cordial. The proposed framework guarantees every vote is checked and gives straightforwardness to the electorates. This framework is protected and addresses an answer for the present democratic framework issues. It is one-time speculation and is what's to come.

REFERENCES

[1] Al-Rawy, M.& Elci.A., "A Design for Blockchain-Based Digital Voting System", in Springer Nature Switzerland AG, 2019.

[2] Malathi, M., Pavithra, S., Preakshanashree, S., Praveen Kumar, S., & Tamilarashan, N., "Rendering Untampered E-Votes Using Blockchain Technology", Department of Information Technology, Sri Krishna College of Technology, Coimbatore, India, 2020.

[3] Sudharsan, B., Nidhish Krishna MP, and M. Alagappan. "Secured electronic voting system using the concepts of blockchain." 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2019.

[4] Navya, A., R. Roopini, and B. Prabhu. "Electronic voting machine based on Blockchain technology and Aadhar verification." International Journal of Advance Research, Ideas and Innovations in Technology 4.2, 2018.

[5] Pandey, N. & Singh, N., Blockchain-Based Voting System Can Better the Way of Elections in India.

[6] Iftikhar A. Khan, "Number of voters across Pakistan tops 107.5m", Published in Dawn, April 10, 2019, Accessed on: Nov. 3, 2020. [Online]. Available: https://www.dawn.com/news/1475072.

[7] Pathak, Ankush, et al. "Design and implementation of a secure and robust voting system based on blockchain.", Int. J. Adv. Res. Ideas Innov. Technol 4, 2018: 869-875.

[8] Bogan, S., Jose, B., Bhushkute, G., Gawade, V., Shirodker, S., Gonsalves, A. & Varak, A., "Digital voting system using blockchain technology", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN(P): 2249-6831; ISSN(E): 2249-7943 Vol. 9, Issue 2, Dec 2019, 1-6.

[9] Hsiao, Jen-Ho, et al. "Decentralized E-voting systems based on the blockchain technology." Advances in Computer Science and Ubiquitous Computing. Springer, Singapore, 2017. 305-309.

[10] Santhosh, k., Shree, l., & Sridhar, "Online voting system using blockchain", International Journal of Advance Research, Ideas and Innovations in Technology, Volume 5, and Issue 2, 2019.

[11] Yavuz, Emre, et al. "Towards secure e-voting using ethereum blockchain." 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018.

[12] Meka, N., Lavu, A., Chowdary, D., Nallamothu, Veeravilli, S., Erigela, G., & Abuzaghleh, O., "Providing security, immutability and transparency to voting system using blockchain technology", Department of Computer Science and Computer Engineering University of Bridgeport, Bridgeport, CT, 2019.

[13] Kumar, S., Darshini, Saxena. S., "Voteeth: An E-Voting System Using Blockchain", International Research Journal of Computer Science (IRJCS), ISSN: 2393-9842 Issue 06, Volume 6, June 2019.

[14] Hjálmarsson, Friðrik Þ., et al. "Blockchain-based e-voting system." 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018.

[15] Khan, Kashif Mehboob, Junaid Arshad, and Muhammad Mubashir Khan. "Secure digital voting system based on blockchain technology." International Journal of Electronic Government Research (IJEGR) 14.1, 2018: 53-62.

[16] Fusco, M. & Lunesu, M.Crypto-voting, a Blockchain based e-Voting System, KMIS. 2018.

[17] Bulut, Rumeysa, et al. "Blockchain-based electronic voting system for elections in turkey." 2019 4th International Conference on Computer Science and Engineering (UBMK). IEEE, 2019.

[18] Rakhe, R., Kale, R., & Bisht, P.(2019) E-Voting System using Blockchain Technology for Distributed Environment, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 8, Issue 5, May 2019.

[19] Pakistani general election violence, Accessed on: Nov. 4, 2020. [Online]. Available: https://en.wikipedia.org/wiki/2018_Pakistani_general_election_violence

[20] Singh, A., Chatterjee, K., "Secure Electronic Voting System Using Blockchain Technology", International Conference on Computing, Power and Communication Technologies (GUCON) Galgotias University, Greater Noida, UP, India, 2018.

[21] Blockchain technology basics, Accessed on: Nov. 2, 2020 [Online], Available: https://www.spheregen.com/blockchain-technology-basics/

[22] Nadeem, S., Rizwan, M., Ahmad, F., & Manzoor, J. "Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture". International Journal of Advanced Computer Science and Applications, 10(1), 288-295, 2019.

[23] Bosamia, M., & Patel, D. "Current Trends and Future Implementation Possibilities of the Merkel Tree". International Journal of Computer Sciences and Engineering, 6(8), 294-301, 2018.