A New Perceptive of E-Voting with Blockchain

Shalini Jindal, Tarun Kumar Garg, Ajeet Singh

***Abstract**: Electronic voting is most growing field in the area of voting system. Digital users are growing with the expo-national growth in every country. In the country like India where mobile or internet user are 391 million, e-voting system reduce a huge amount of current voting methods. But in this current scenario e-voting system are vulnerable and not threat proof. Blockchain is new emerging field in security and for distributed systems. Only few methods are applied in the past where E-Voting system used the blockchain technology. So, the objective of this research is to review the different algorithms applied in e-voting using blockchain through various parameters to help researchers working to provide more security using blockchain.*

***Keywords**: E-voting, Blockchain, Security, attacks, SHA algorithm, distributed system.*

I. INTRODUCTION

In recent years, electronic voting has emerged in many countries to reduce the cost and effort required for conducting an election. It also focusses on ensuring election integrity by monitoring various aspects such as security, privacy, software and hardware requirements. It has been followed in several countries of the world. It was started in Estonia [1], followed by Switzerland [2] and Norway [3]. With the emergence of electronic voting, traditional ballot system and paper voting has become significantly outdated. E-voting has several advantages that it reduces the cost, effort and provide ease to cast a vote from anywhere in the world. In a survey conducted in 2019 the total number of internet user are in world are 4479 million and increasing day by day. No of digital user are in world is shown in fig1.

Still significant number of people cannot trust electronic voting due to authenticity, security and integrity of the machine used. Security is a major threat in e-voting system and but successfully implementation reduce human effort and cost.

To reduce the security and authenticity issues of e-voting, blockchain has emerged as a new solution to construct more secure and decentralized systems. Blockchain is gaining popularity as it is a simple method that provides authentication and maintains integrity in several domains such as bitcoin, payment systems and domain systems in government and non-government organization [4].

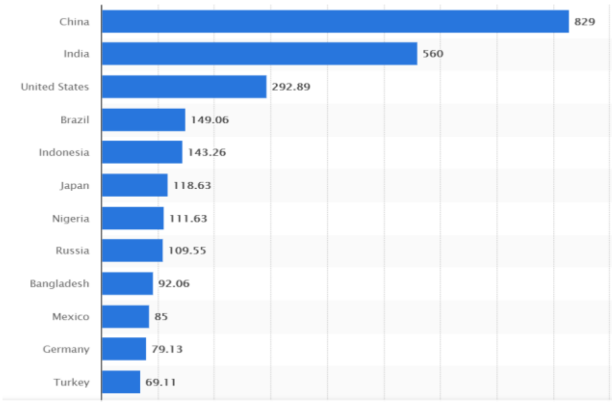

Fig 1 No of internet user in world

Blockchain is first implemented by Santoshi in 2008 [5]. It is a digital platform for various assets such as cryptocurrency and electronic votes. It is a distributed ledger technology which ensures several critical features such as Immutability, authenticity, verifiability, security, integrity and others. In this work, several technologies and methodologies used by various researchers in the field of e-voting with blockchain has been reviewed. The conducted review depicts that blockchain is the new improved solution for electronic voting ensuring all critical features. Although it does not provide anonymity, still various intelligence organizations are relying on blockchain technology all over the world[6]. There are mainly three systems where e-voting is successfully implemented by blockchain.

- Votebook
- FollowMyVote
- VoteWatcher

II. RELATED WORK

The work done in literature in the areas of e-voting with blockchain has been reviewed in this section.

H.V.Patil et.al.[7] investigates the various problems in a traditional e-voting system and initiates a model to resolve these issues. The authors have evaluated the significance of blockchain to implement distributed e-voting system. They have also stated some existing framework of blockchain and their limitations. In another existing system based on blockchain, F.P. Hjalmarsson et.al [8] proposed a methodology named proof-of-authority (POA) permissioned by Go-Ethereum. The proposed framework consists of two types of nodes: district node and boot-node. Along with nodes, authors considered election as a smart contract. which consists of three parts: 1) Identification of election roles 2) agreement or election process 3) voting transactions. To implement and deploy the proposed method, three frameworks were used: Exonum, Quarum and Geth. The major shortcomings of the approach are that it is based on private blockchain implementation and uses district-based voting.

Revised Manuscript Received on February 05, 2020.
* Correspondence Author

Shalini Jindal, Research Scholar, Department of Mathematics, J,C.Bose University of Science and Technology, YMCA, Faridabad, India Email: Shalinijindal91@gmail.com

Tarun Kumar Garg*, Associate Professor, Department of mathematics, Satyawati college, University of Delhi, India. Email: tkgarg@satyawati.du.ac.in

Ajeet Singh, Assistant Professor, Department of mathematics, satyawati college, university of Delhi, India. Email: singhajeet966@gmail.com

The proposed approach overcome the limitations of existing e-voting systems and ensures integrity and security. A.B. Ayed [1] address the limitation and security threats in existing e-voting system such as Estonian I-voting system, Norwegian I-voting system, New South wales ivote system and D.C. Digital vote-by-mail service. To address the security breaches in these existing electronic voting systems, authors proposed a model of blockchain e-voting system. In the proposed system, the first transaction will not be counted as a vote (as in other systems), it will contain only candidate's name and will be served as foundation block. In this, user can either cast a vote or protest a vote and all the transactions are encrypted using one-way hash function.

P. Tarasov et.al [4] proposed a technology 'zcash', a payment scheme used in voting system. The authors have overcome a gap of tackling anonymity issues that exists in existing e-voting systems. Zcash is a decentralized payment scheme which relies on zero-knowledge proofs. It is an implementation of zero cash concept but with different architecture. It differs with bitcoins in terms of addresses, as zcash uses two addresses, z-address and t-address to preserve anonymity and privacy. R.Osgood [6] analysed the problems and vulnerabilities of existing voting machines. The authors investigated electronic voting machines (EVMs) in united states and found that EVMs are vulnerable to WINvote security vulnerabilities. The author explained the technology used in blockchain system and discuses different implementation that have been implemented for blockchain voting systems. There are three types of implementation are used in literature as stated 1. Votebook 2. FollowMyVote and 3. VoteWatcher. By studying these implementations, authors have proposed a secure, realistic and effective approach by combining implementation of VoteWacher and VoteBook. S.Shah et.al.[9] proposed a new system with client server architecture integated with a blockchain system. The system consists of four parts: users, authentication Server (AS), Arbitration server (AR) and Blockchain system. The proposed system includes various steps of traditional voting system along with ability to verify users' own vote. The proposed system has been evaluated in terms of economic and social benefits. It offers privacy along with transparent verification of casted vote for elections.

R. Hanifatunnise et.al [10] proposed a system for recording database of e-voting using blockchain technology. The system records the results of e-voting system that is conducted after the completion of election process. The results of each node is stored and recorder using blockchain permission protocol. The proposed system has following processes: Verification, get a turn, updation of database, creation of a new block and broadcast. The system is built using Pycharms community software and tested for nodes ranging from 1 to 500,000. A.K. Koc et.al. [11] proposed and implemented an application of e-voting as a smart contract for the Ethereum network. It uses Ethereum wallets, soliditing language and android platform. In this, Ethereum network is preferred as it provides wide range of use cases along with smart contracts. The smart contracts are written in C++ and javascript which are executed by the peers in every 15 seconds of Ethereum networks. These are validated by two other users and after execution contracts can be shared with other candidates. 'Voter' is defined as a struct in solidity programming language with various functions such as give RightToVote() and winningProposal(). Y.Wu [12] proposed a novel protocol named BlockVotes for e-voting using blockchain and ring signatures. The proposed protocol consists of several entities, namely, voters, registrations authority, election authority and bitcoin address pool with several phases. The protocol has been developed by PhP programming language. In this, MVC framework named SLIM has been developed using MYSQL database. Table 1 shows a comparative study of various methods used in literature.

Table 1: Various Methods in literature

Author Name and Year	Proposed Methodology	Framework Used	Advantages	Limitations
R. Osgood, 2016	VoteWatcher + VoteBook	-	Promotes economic development	-
A.B. Ayed, 2017	Yes	-	Authentication, Anonymity, accuracy and Verifiability	Inability to change vote in case of user mistake
R. Hanifatunnise et.al., 2017	Recording results of e-vote		Stores e-voting results effectively with average capacity of 216.04 bytes for each block	-
Y.Wu, 2017	BlockVotes	Ring signature algorithm	Ballot privacy, verifiability, eligibility	-
H.V.Patil et.al., 2018	Blochchain in e-voting (BEV)	-	Blockchain is publically verifiable an no corruption will occur as it is distributed	Complexity, technology's immaturity, scalability of platform
F.P.Hjalmarsson et.al., 2018	Go-Ethereum Permissioned Proof of Authority (POA)	Exonum, Quorum, Geth	Utilized smart contracts for secure and cost efficient election	Private block chain, district-based evoting
P. Tarasov et.al., 2018	Zcash (Payment Scheme)	-	Cheap voting system	Integration with Ethereum protocol is prnding
A.K.Koc et.al., 2018	Smart contract for Ethereum network	Ethereum wallets, android platform	Ethereum with smart contract provides a broader solution base for internet related issues	Small scale polls and elections
S.Shah et.al, 2019	Client server architecture with blockchain	-	Ability to verify user's own vote, cost-efficient	-

III. ELECTRONIC VOTING AND BLOCKCHAIN

In this section authors briefly explain the E-voting system and its shortcoming and the blockchain technology.

A. Electronic Voting

E-voting is a process of casting and tabulating votes casted by users through electronic means. In recent years. Several applications were used for e-voting. Among them, Direct Recording Electronic (DRE) system and Internet voting are most commonly used. For DRE's three types of machines are used, namely, Touch screen machine, punch key machines and wheel machines. To cast a vote electronically, machines consists of a memory chip and a removable memory card. After casting all the votes, the memory card is removed and loaded to a computer to tabulate the casted votes. The process of e-voting is very easy and convenient to all, but there exist some security issues due to which it is criticized [13]–[15].

B. Drawbacks Of E-Voting

There exists some drawback due to which e-voting is not considered as a permanent means [1] Some issues are like:

- The machines are poorly designed and programmed which are more prone to hacking.
- The software used for e-voting are proprietary software, so no one can verify and validate such software. It can lead to anonymous casting of votes.
- E-voting machine usually fail to boot, record votes inaccurately and inappropriately.
- There is no way to evaluate the efficacy and integrity of e-voting machines.

C. Security Breaches In E-Voting

Apart from drawbacks, e-voting systems are prone to many security attacks. Some of threats discovered in recent years are :

- The main threat to public polls is cyber -attacks. E-voting is most vulnerable to Distributed Denial of Service (DDOS) attack, that makes casting of votes inaccessible to voters.
- State level attacks occurs due to access to wide range of network traffic.

To mitigate these security breaches, e-voting systems should deploy:

- Prevention of anonymous casts of votes
- Verifiability of the vote
- Transparency to every user with privacy
- Prevention from deletion of evidences

To address all these issues, Block chain technology has emerged to cast secure votes in a decentralized environment.

D. Blockchain

Blockchain is a time-stamped series of immutable records of data called as block, based on a distributed ledger. Distributed ledger is a distributed database that maintains records that is shared across cluster of computers in a synchronized way that is not centralized. Cluster of computers are referred as nodes that agree to process the efficacy of transactions based on set of network rules. Each node maintains their own copy of blockchain. Each block of data is linked to each other and is secured using cryptographic hash function (SHA-256). If a node substantiates a transaction, it is considered as a block and is secured with a hash function and is added to the blockchain. The second block is formed, it will contain a hash function of the previous block and its own data, and a chain (series) of block is formed termed as blockchain. The first block is called as genesis block [1], [7], [8]. All the data in block are connected through a linked list structure. Block chain is transparent in nature i.e. anyone and everyone can see the information and everyone involved in a blockchain is responsible for all the actions that take place. It has no transaction cost and is skillful and intelligent way to process information from one user to another. The complete process of blockchain is explained in fig 2.

IV. METHODOLOGY

In this section authors explained the complete methodology of E-Voting using blockchain. To meet and satisfy the security and privacy issues of e-voting, blockchain process is presented.

- The first transaction for casting vote will represent a candidate and will be a special transaction.
- The special transaction will include the name of the candidate and will be served as foundation block (Genesis block) followed by other blocks.
- Each vote will be recorded and updated in a blockchain. To ensure the security of the system, information of previous voter will be contained in next block in a decentralized environment, so no corruption can take place.
- To implement blockchain, following structure of blocks is necessary and shown in Table 2.

Table 2 Block structure

Attribute	Description	Size
Size of a block	Represents size of the whole block	4 Bytes
Header of block	Represents Encryption through Hash function	80 Bytes
Record	It contains data served in a block	Vary with carrying data
Counter	Represents Total number of records	1-9 Bytes

With the process of blockchain, process of e-voting is merged. The main activities in working of e-voting system using blockchain are as follows:

Registration of voter: The main phase is the registration of voters by election administrator. An election administrator prepares a list of eligible voters and maintains a database with all their credentials. Credentials may include Social Security number (SSN), address and voting confirmation provided by local authorities to the users. This is an essential step to prevent Sybil attack [1], where attackers attack a system with large number of fake identities and cast illegitimate votes. The registration of vote is depicted in fig. 3

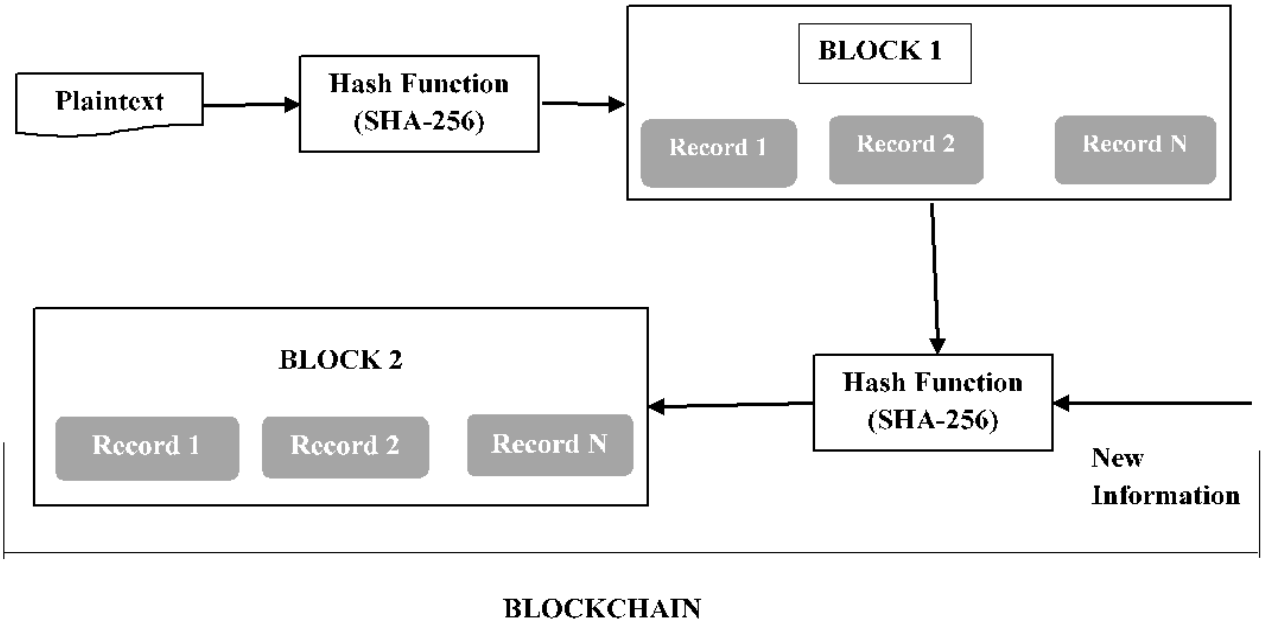

Fig 2 Information flow in blockchain

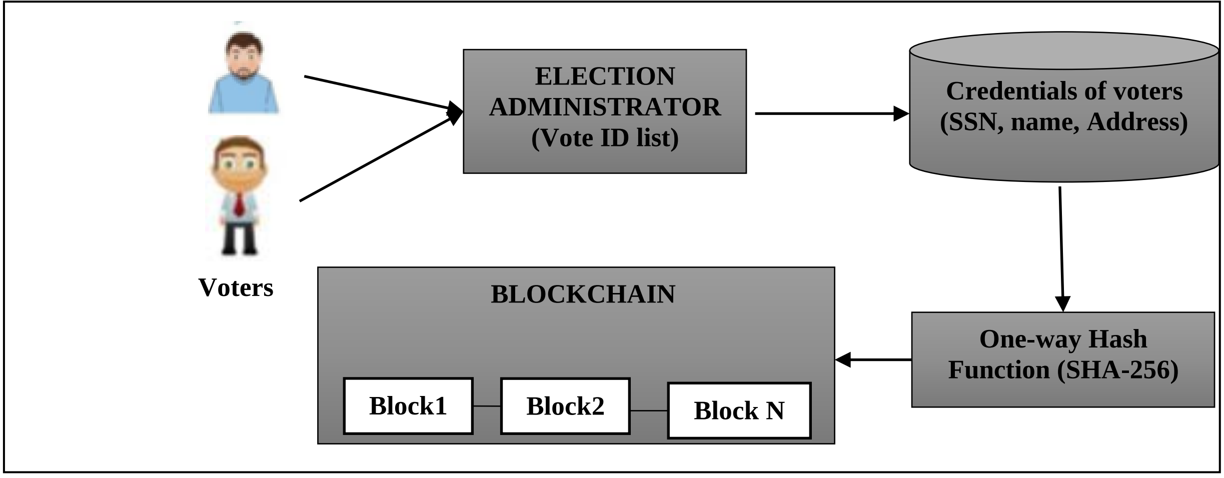
Voters
ELECTION ADMINISTRATOR (Vote ID list)
Credentials of voters (SSN, name, Address)
One-way Hash Function (SHA-256)
BLOCKCHAIN
Block1
Block2
Block N

Fig 3 Registration for voters

- **Request to cast a vote:** To cast a vote, the user must log in to a voting system with their credentials. If entered credentials by the users match with a database, then the voters will be authenticated to cast a vote. This step is illustrated with the help of fig. 4
- **Cast a vote**: Voters will choose an option, either to cast a vote or protest a vote.
- **Vote Encryption**: Once the user casts a vote, an input will be generated by a system consisting of identification of the voter along with complete name and hash function of the previous vote. The information will be encrypted using SHA-256 hash function which cannot be reversed and recorded in the block header of each vote.
- **Vote added to Blockchain**: Once a block is created with vote, the information is recorded in the respected blockchain. A series of casted votes is created and linked to each other.

The complete process of e-voting with blockchain is illustrated in fig. 5

V. RESULTS

E voting is the emerging field in the voting system, but due to data integrity and privacy it cannot be applicable in real world application. Block chaining provides a way to secure data in a distributed system. Both block changing and e-voting are best match to secure data with privacy commitment. In this research paper a detail study is shown where e-voting is implemented by the block chaining. The three main techniques implemented by the block chaining and e-voting and their attributes are shown in table 3.

Table 3 Description of implemented technology

Technology	Attribute	Size
Votebook	Size of block Header of the block	4 bytes 80 bytes

FollowmyVote	Size of block Header of the block	8 bytes 120 bytes
VoteWatcher	Size of block Header of the block	6bytes 80 bytes

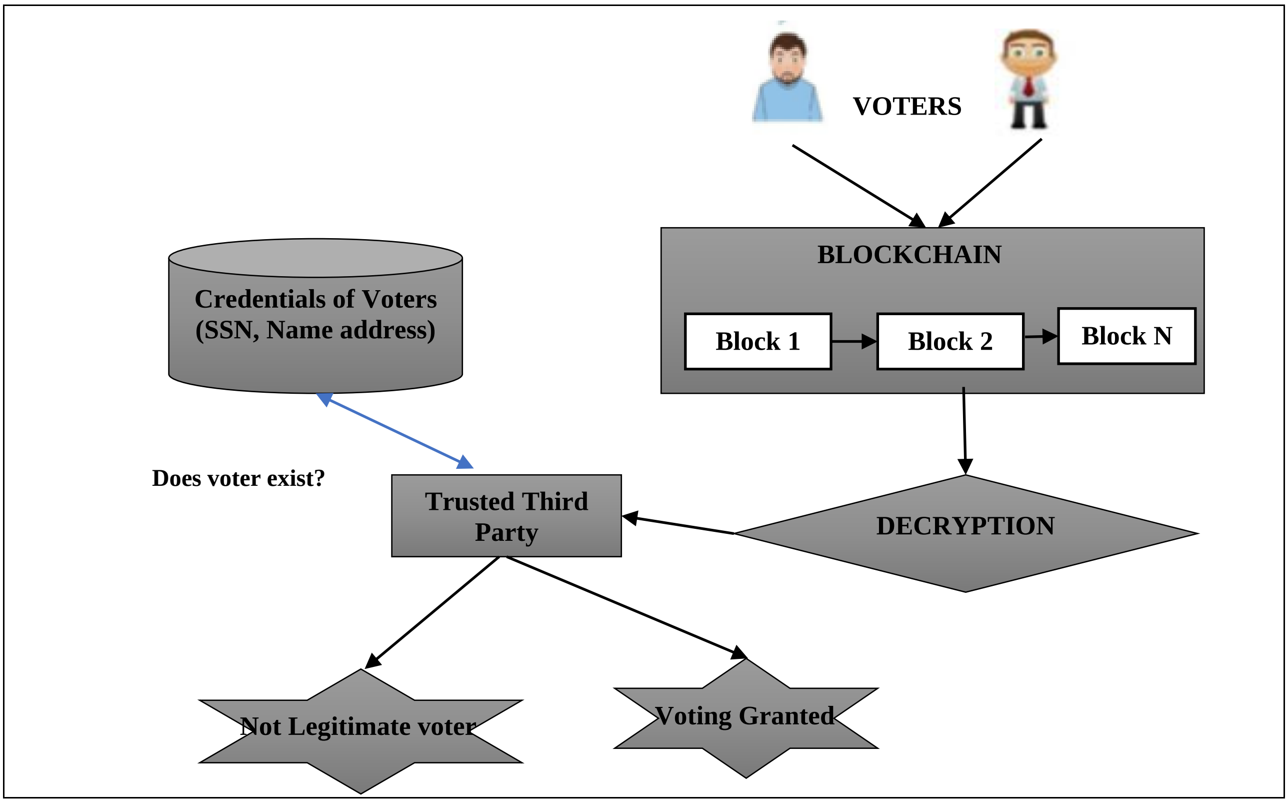

Fig 4 Request to Cast a Vote

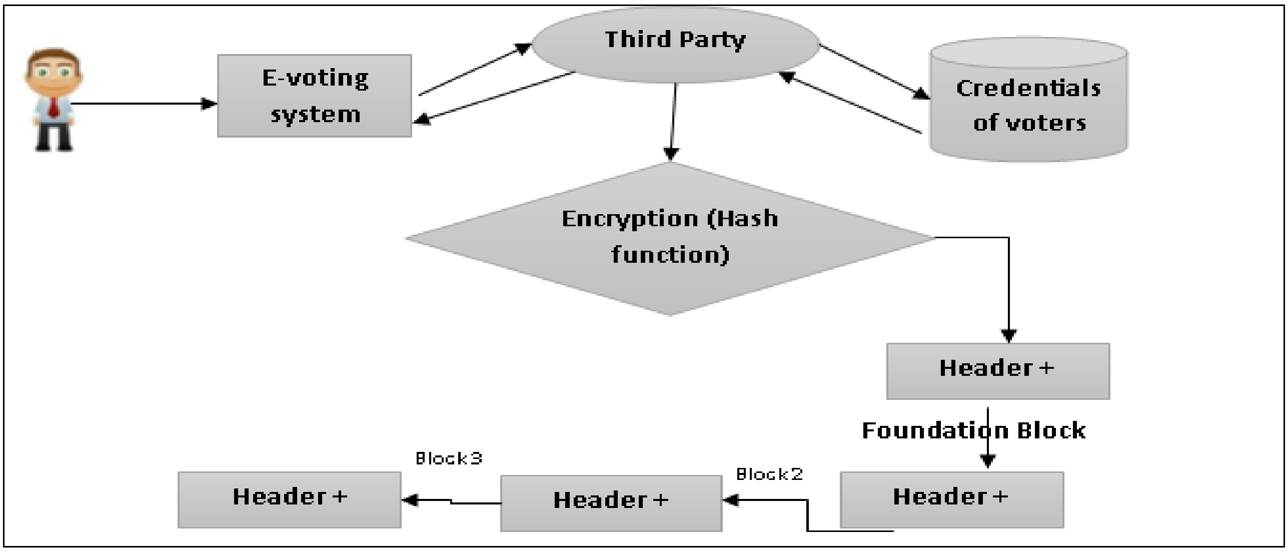

Fig 5. E-voting with Blockchain Process

VI. CONCLUSION

Electronic voting (E-voting) has been emerged as a solution to cast vote from anywhere in the world. With the availability of internet and voter id, it enables user to cast their vote without being available at a specific location. But to cast vote electronically, the system should be secure, cost-efficient and reliable. To provide such a secure system, blockchain technology has emerged. In this paper, various blockchain technologies implemented by several researchers has been reviewed and compared. Various drawbacks and security issues are identified and a method to implement blockchain has been elaborated. In future, a new method to improve an existing technology will be introduced.

REFERENCES

1. Ben Ayed, "A C ONCEPTUAL S ECURE BLOCKCHAIN - BASED E LECTRONIC VOTING S YSTEM," vol. 9, no. 3, pp. 1–9, 2017.
2. J. Gerlach and U. Gasser, "Three Case Studies from Switzerland :," 2009.
3. Sofie, G. Stenerud, and C. Bull, "When Reality Comes Knocking Norwegian Experiences with Verifiable Electronic Voting," pp. 21–34.
4. P. Tarasov and H. Tewari, "THE FUTURE OF E-VOTING," vol. 12, no. 2, pp. 148–165.
5. S. Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," pp. 1–9.
6. R. Osgood, "No Title," pp. 1–21, 2016.
7. H. V Patil, K. G. Rathi, M. V Tribhuwan, C. Science, and D. Y. P. A. C. S. College, "A Study on Decentralized E-Voting System Using Blockchain Technology," pp. 48–53, 2018.
8. F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-Based E-Voting System," no. May, 2019.
9. S. Shah, Q. Kanchwala, and H. Mi, "Block Chain Voting System."
10. R. H. Author, "Blockchain Based E-Voting Recording System Design."
11. K. Koç, "Towards Secure E-Voting Using Ethereum Blockchain," no. February, 2018.
12. R. Jindal, R. Malhotra, and A. Jain, "Prediction of defect severity by mining software project reports," Int. J. Syst. Assur. Eng. Manag., 2016.
13. K. K. Sharma and P. M. Patole, "Securing E-Voting System using Blockchain," pp. 8638–8641, 2018.
14. R. Ganji, "ELECTRONIC VOTING SYSTEM," 2018.
15. F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, "Crypto-voting , a Blockchain based e-Voting System Crypto-Voting , a blockchain based e-voting system," no. January, 2018.
16. https:// followmyvote.com

AUTHORS PROFILE

Shalini Jindal is a Research Scholar in Department of mathematics, currently pursuing PhD in mathematics in J. C. Bose University of Science and Technology, YMCA Faridabad.
E mail: shalinijindal91@gmail.com

Dr. Tarun Kumar Garg has been working as an associate professor since last 20 years in the department of Mathematics, Satyawati College, University of Delhi, Delhi. His field of research is Wavelet Analysis, Reliability and availability of Mechanical systems and Optimization. He has published many research papers in international journals.

Ajeet Singh is Working as Assistant Professor in department of Mathematics of Satyawati College University of Delhi. He has a teaching experience of 9 years. His Research area is Mathematical programming and optimization.