E-VOTING SYSTEMS USING BLOCKCHAIN: A SYSTEMATIC REVIEW AND FUTURE RESEARCH DIRECTION

Dhiraj Amrutkar*,Gaurav Dongare*,Sayog Sonune*,
Archana Y. Chaudhari**

**UG Students, Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Savitribai Phule Pune University, Pune, India.*
***Assistant Professor, Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Savitribai Phule Pune University, Pune, India.*

Article DOI: https://doi.org/10.36713/epra7157
DOI No: 10.36713/epra7157

ABSTRACT

One of the most important discoveries and creative developments that is playing a vital role in the professional world today is blockchain technology. A blockchain is a distributed, digitized and consensus-based secure information storage mechanism. Blockchain technology moves in the direction of persistent revolution and change. In the last couple of years, the upsurge in blockchain technology has obliged scholars and specialists to scrutinize new ways to apply blockchain technology with a wide range of domains. The dramatic increase in blockchain technology has provided many new application opportunities, including e-voting application. The present article provides a systematic review of emerging blockchain-based e-voting systems. In this paper, we call attention to the open research matters in this fast-growing field, explaining them in some details. It was concluded that frameworks needed enhancements in order to be used in voting systems due to these reservations.

KEYWORDS: *blockchain, e-voting, cloud computing, ethereum; ballot*

I. INTRODUCTION

Today’s democracies are built on consensus among the population through voting. Currently, a lot of countries use the traditional ballot system, which requires centralized control with a trusted party for conduction of the voting process, and recording and counting of the vote ballots by the trusted third party. However, this introduces the possibility of corruption and manipulation of votes. As an improved alternative to the ballot system, an electronic voting, or e-voting, system has been proposed and implemented in limited scenarios, due to its promising capabilities of reducing costs and decreasing manual intervention. However, e-voting systems have not been implemented on a large-scale due to concerns regarding secu- rity, transparency, distributed authority, data integrity, privacy and compliance requirements.

An election, which takes place in the form of voting, is a process that involves members in mutual competition. This forces us to develop a system which is very secure and is not vulnerable to attacks by the people participating in the elections, the voters or the third party which conducts the elec- tions. Such a process cannot be secured by cryptographic process alone. If the secret key used in the cryptographic process is found out or manipulated by the party conducting the elections, the entire system fails and is not secure. In such an environment, it is necessary to adhere to policies like the distributed ledger. Blockchain being a technology which uses distributed ledgers, can be ideally used for this process. The blockchain network can be either a permission-less network like Bitcoin or Ethereum where anyone is allowed to interact with the network, or a permissioned network like Hyperledger Fabric, Hyperledger Sawtooth or Exonum where only known members are allowed to interact with the network. Another important issue to be addressed is the anonymity of the voter. Due to the increase in research and progress in the field of big data analytics, this data is susceptible to discovery and manipulation. This can be resolved by using techniques like one-time ring signatures and homomorphic encryption.

The ideology of designing and implementing an e-voting system using blockchain overcomes the majority of draw- backs of standard e-voting systems and offers encouraging research initiatives . The fundamental decentralized nature of blockchain conceptualizes the technology as a secure third party. Consequently, an e-voting system implemented using the blockchain technology can be trusted to add only valid and verified voting blocks to the blockchain network. In addition, any attempt to tamper with the blocks in the blockchain is viewed as a violation of the blockchain network's consensus principles and is prohibited by the blockchain network [4]. Therefore, an e-voting system based on blockchain is convenient, automated, transparent, secure and free from corruption.

II. LITERATURE SURVEY

A. *The Blockchain Technology*

Blockchain is so-called, as it consists of a chain of blocks,that is, interconnected nodes that have their copy of the distributed ledger that contains the history of all transactions. Data is processed and put in a block through a process called mining. Every block contains a hash of the previous block and hence it forms a chain of blocks, with the first block known as the genesis block. Hence, it forms a linked list kind of Structure.Blockchain has a number of ledgers where data can only be appended but not deleted or tampered. Consequently, it is immutable. Blockchain can either be public, where anyone can read or write data onto the blockchain, or private (permis- sioned), in which case only a few restricted individuals can read or write data.

B. *Existing E-Voting Systems and Betterment using Blockchain*

Estonia has been using electronic voting (I-voting system) since 2005. The basis of this system is a national ID card given to all its citizens. These cards are encrypted files, which uniquely identify the owner and can be used for signing documents, banking services, and so on. For the voter to cast his/ her vote, the voter must insert their card into a card reader, after which the voter will be granted access to the voting website. Moreover, the eligibility of the voter is verified after the voter enters their when prompted on the website interface. Once authenticated, the voter has time until four days before election day, within which the voter can cast his/her vote, and also modify the casted vote. Once the vote has been submitted, the vote is passed through the publicly accessible vote forwarding server to the vote storage server, where it is encrypted and stored until the online voting period is over. From the vote storage server, the vote information is transferred to an isolated vote counting server through DVDs. This server decrypts and counts the votes, and produces the election results. However, there is a possibility of malicious attacks that compromise the client-side machine by changing the voter's votes, without the voters' knowledge. Moreover, another possible risk is that of an attacker directly infecting the servers through malware being placed on the DVDs used for the transfer of votes. Consequently, such an electronic-voting system introduces concerns of security due to the presence of a vulnerable centralized authority and database server to store and manage the votes.

Translating this process to the blockchain network to im- prove reliability and resolve concerns of manipulation from the client system, a system can be proposed consisting of two blockchains- the vote blockchain and voter blockchain. This involves a registration process of voters followed by the voting process. In the registration process, the voter fills a form with all his/her personal details. This is a transaction and is added to the voter blockchain. In this process, the miner analyses the transaction and awards the user with a vote token, obtained from a pool of infinite vote tokens. Following this, a ballot paper and a password are sent to the voter, using which the voter can cast his/her vote. The user is now authenticated with the following three pieces of evidence: identification number, the password generated during registration and the ballot paper. As a result, following the authorization step of verifying the user's right to vote, another transaction is created in the same voter blockchain, which is the transaction containing the user's vote token, indicating the availability of the user's vote. Once the user votes, this transaction containing the user's vote is removed from the voter blockchain.

In order to simplify and scale the design, the system can be designed to have a 3-tier architecture: National, Constituency and Local. The local tier consists of all polling stations and is associated with a constituency node. The constituency tier contains all nodes in the constituency level. The national nodes are responsible for mining transactions and adding blocks to the vote blockchain. As part of the design, there exists an encryption method based on public and private keys and a structure where the data is segregated and isolated logically. This segregation has been achieved by getting the different constituency level nodes to generate distinct key pairs. The public key of a constituency node will then be distributed to the polling station nodes connected to that particular constituency node, which use the public key to encrypt any vote made at those polling stations. The vote and voter data from all constituency nodes are then stored in an encrypted format within the blockchain and are propagated out to the entire network. Therefore, even if a hacker manages to get hold of a constituency private key, he/she would only be able to decrypt a part of the blockchain, that is, the votes originating from that particular constituency node. Consequently, this design makes the system more independent and secure. However, this system is not effectively manageable for large-scale implementation due to large overhead in encrypting all the votes.

C. *Requirements*

The existing e-voting systems proposed for implementation using the blockchain technology can be summarized to con- stitute of the following requirements and features

- Public Verifiability: All stakeholders of the election pro- cess (including people spectating voting process) can verify the election's whole procedure and result.
- Individual Verifiability: Each voter can verify that his/her vote has been accurately recorded and considered.
- Dependability and Reliability: Asymmetric-key cryptog- raphy and various blockchain mechanisms to protect against attacks. Digital signatures (blind signature or short-linkable ring signature) are used to validate votes to allow adding of only valid and verified votes to the blockchain network.
- Consistency: Through consensus mechanisms of blockchain, all nodes have the same copy of records (same copy of blockchain) at a particular point of time, and all of them will contain the same final result after the election process is complete.
- Auditability: The whole procedure is auditable after the election, if necessary.
- Anonymity: No connection between voters and votes. Complete privacy of voters is ensured through cryptogra- phy and the use of zero-knowledge proofing to validate votes.
- Transparency: The whole process is open to the public. It is secure while being transparent.
- Scalability: Short-linkable ring signature is used for the digital signature mechanism, which has the ability to support a large number of voters.Eligibility: Making sure that only eligible candidates have access to the system.
- Authentication: Authenticating users wishing to access the e-voting system, using a unique voter ID issued to them, along with other credentials.
- Fairness: The election results are not live. Due to the absence of a centralized authority, counting of votes can only be performed after the entire election process is complete, by decrypting the encrypted blocks in the blockchain network.

D. *Blockchain Methodology for E-Voting System*

Any blockchain-based e-voting system will consist of the following entities :

- Smart Contract Admin
- Voting Process Admin/ Authorization Organization
- Smart Contract
- Voters

The architecture can be summarized as follows:

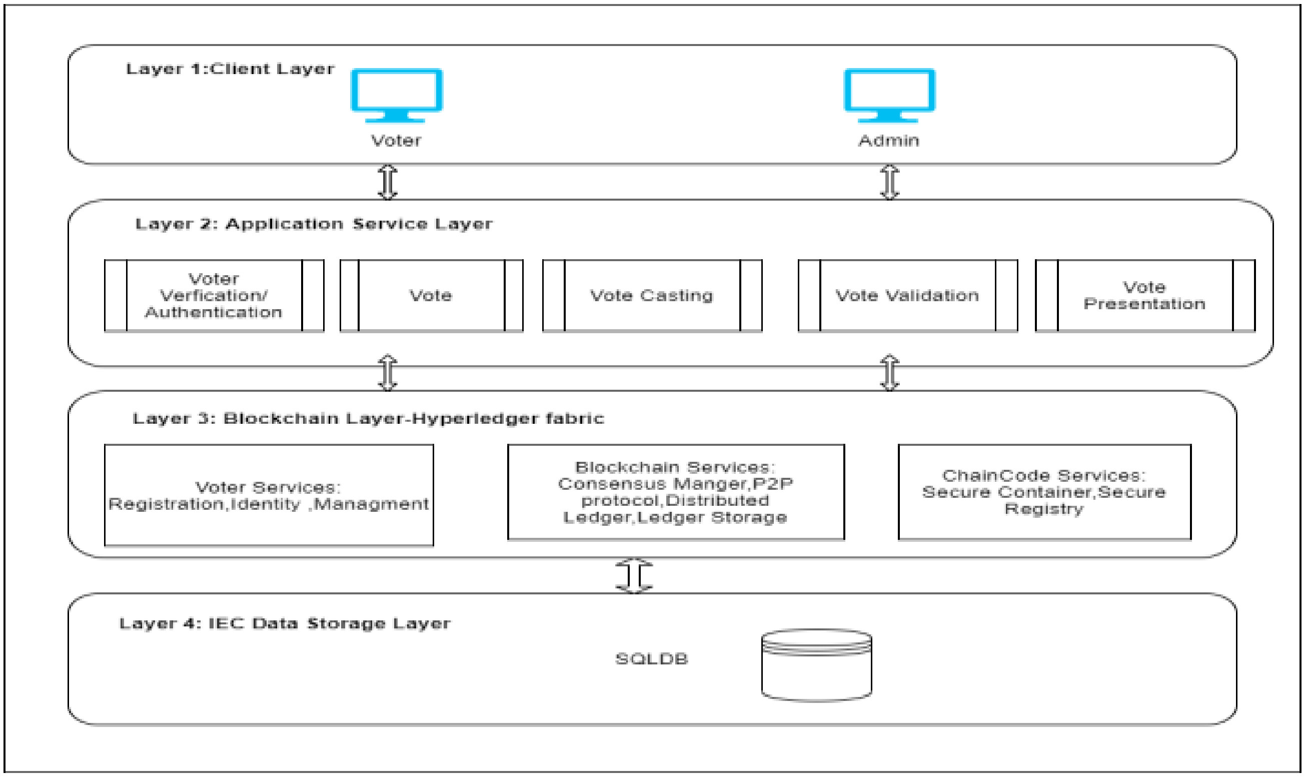
Layer 1:Client Layer
Voter
Admin
Layer 2: Application Service Layer
Voter Verfication/ Authentication
Vote
Vote Casting
Vote Validation
Vote Presentation
Layer 3: Blockchain Layer-Hyperledger fabric
Voter Services: Registration,Identity ,Managment
Blockchain Services: Consensus Manger,P2P protocol,Distributed Ledger,Ledger Storage
ChainCode Services: Secure Container,Secure Registry
Layer 4: IEC Data Storage Layer
SQLDB

Fig. 1. Simple Architecture of a Blockchain e-voting system [9]

The working of a simple blockchain-based e-voting system can be explained as follows: The very first transaction added to the block is a special transaction which represents the candidate. It has the details of the candidate and acts as a foundation on which the votes can be added to that candidate. However, creating one chain for each candidate introduces a larger overhead for storage and processing, making it more complex.

Alternatively, crypto-voting has been explored for imple- mentation using the sidechain technology, in which two sidechains are linked to a parent blockchain . Moreover, one sidechain stores the voter and vote information, while the other sidechain stores the count of votes, or the results. However, this makes the election results live during the election process, and impedes the principle of fairness of a democratic election.

An alternate design for the e-voting system can consist of a district node and a boot node where the district node manages the smart contract of the boot node . The district nodes collectively agree upon whether a vote is valid or not, which makes the system decentralized.

The following frameworks can be used for smart contracts: Exonium which uses Rust language, Quorum which is based on Ethereum framework and Geth which is a short form for Go-Ethereum.

Ethereum is a platform where decentralized applications can be built either on a public or private network. Ethers are needed to use the public Ethereum platform. It uses a smart contract to validate and store votes. However, the Ethereum framework is a heavy-weight framework.

The Multichain framework can be used to create private blockchain networks. It requires less computation power and is free for usage, unlike the Ethereum network. The primary feature of an e-voting system is anonymity- no one should know whom the voter voted for. For this purpose, TTP (Trusted Third Party) can be used. The other component re- quired is an authentication organization, similar to the election commission. Due to the support of both of these features in multichain, it can be used as the blockchain network. Each vote is treated as an asset in the multichain. Before voting, the voter should have an intention to vote. The voters register following which the authorization organization assigns an identification number to each voter, to be used in the voting process, creates a public address in the multi-chain network and stores it against the voter. During the voting process, the voter has to submit the identification number and his/her secret message (vote). The Trusted Third Party (TTP) is used to verify the vote. The TTP generates a public key for the voter using the network and uses this to store the information against the hash of the secret message and the identification number of the voter. Multichain also restricts the voter to vote only once. During the e-voting process, voters access the system through an interface using their voter ID and credentials, and view the list of candidates. When the logged-in voter votes for a candidate, the voter's information and the vote cast is verified by TTP and securely added to the blockchain network.

III. BIBLIOMETRIC ANALYSIS

It is mandatory for the researchers to have in-depth knowledge about the ongoing researches in their respective field and the authors who contribute to such research. This information keeps on changing with time. Due to the evolution of new technologies, several other pieces of information about researches come into existence. There are multiple methods used for analyzing the trends in various fields, which includes webometrics, bibliometric, scientometric, and H-index [18]. Among this, bibliometric analysis is common in most research works as it is a combination of qualitative and quantitative research works. This study uses publication types, subject areas, secondary data research, yearly publication trends, geographical publications, and citations method for analyzing the researches. For the bibliometric analysis, the author used the Web of Science(WoS) [19] database to construct the literature. Several networks have been built regarding keywords and title of the researches on e-voting system and blockchain, citations, and authors.

i) Keywords

The query for the Web of Science was classified into two blocks as primary keywords, secondary keywords, secondary keywords. The proposed keyword strategy applied for this research is mentioned in Table 1.

Table 1: The proposed keyword strategy

Primary Keywords (AND)	**"e-voting using Blockchain"**
Secondary Keywords	"iVote" or "I-voting" or "blockchain ballot" or "distributed online voting" or "electronic voting" or "blockchain enabled e-voting" or "blockchain based e-voting"

ii) Languages

The WoS database is the base of this research paper. Preliminary investigation through planned keyword search tactic generated in all 38 publications. This is then restricted to publications in English only (Table 2).

Table 2: publishing languages trends.

(Source: https://www. webofknowledge.com accessed on 19th March 2021)

Type	Count	Percentage (%)
English	33	86.842 %
Korean	3	7.895 %
Italian	1	2.632 %
Polish	1	2.632 %

iii) Document Types

All types of publications retrieve from the result of the queries for the considered span are taken into account. Majority of the extracted publications are published in article. There are 93% of journal article are published in WoS (refer Table 3).

Table 3: shows documents types published in WoS

(Source: visited webofknowledge.com accessed on 19th March 2021)

Type	No. of publication	Percentage(%)
Article	35	92.105
Review	2	5.263
Early Access	2	5.264

iv) Research Publication Trend

The related documents were retrieved as journal papers, conference papers, articles, reports, etc., for the span of five years from 2017 to 2021. The graphical representation of the yearly publication trends in e-voting system using blockchain is shown in Fig. 2. The trend increased in 2020.

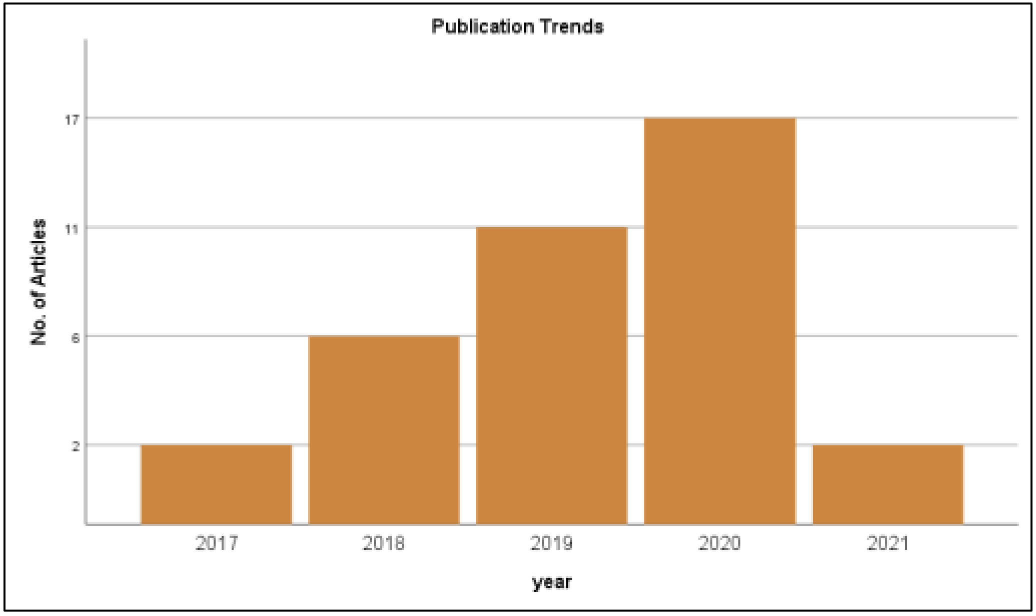

Fig 2: Research Publication trends
(Source: visited webofknowledge.com accessed on 19th March 2021)

v) Author Statistics

Fig. 5 depicts top 15 authors contributing and their affiliations to blockchain based e-voting from WoS. It is clear from figure 4 that key contributing authors are Arshad J, Khan NM.

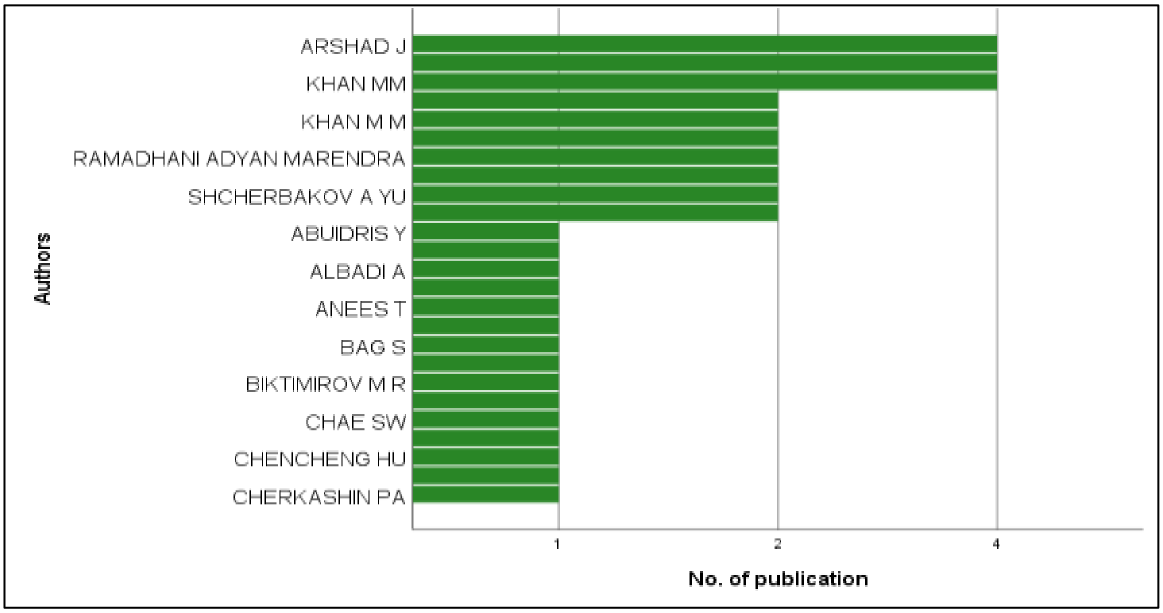

Fig 3: top 15 authors who have published papers in WoS on blockchain domain.
(Source: visited webofknowledge.com accessed on 19th March 2021)

vi) Geographical regional analysis

Fig. 4 gives countries having publications in the area of blockchain from WoS. England is the prominent publishing countries for undertaken blockchain study.

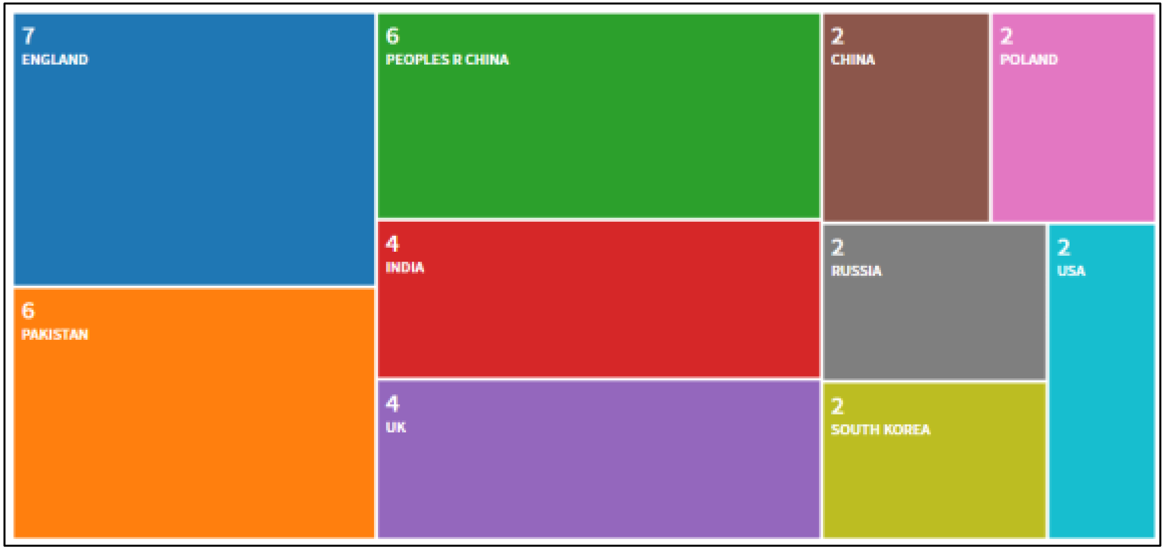

Fig 4: shows tree map indicating countries who are involved in publications related to blockchain

(Source: visited webofknowledge.com accessed on 19th March 2021)

vii) Source Statistics

Fig. 5 covers the publication journal in the area of blockchain. It is clear that maximum numbers of publications are from IEEE Access followed by International Journal of Information Security.

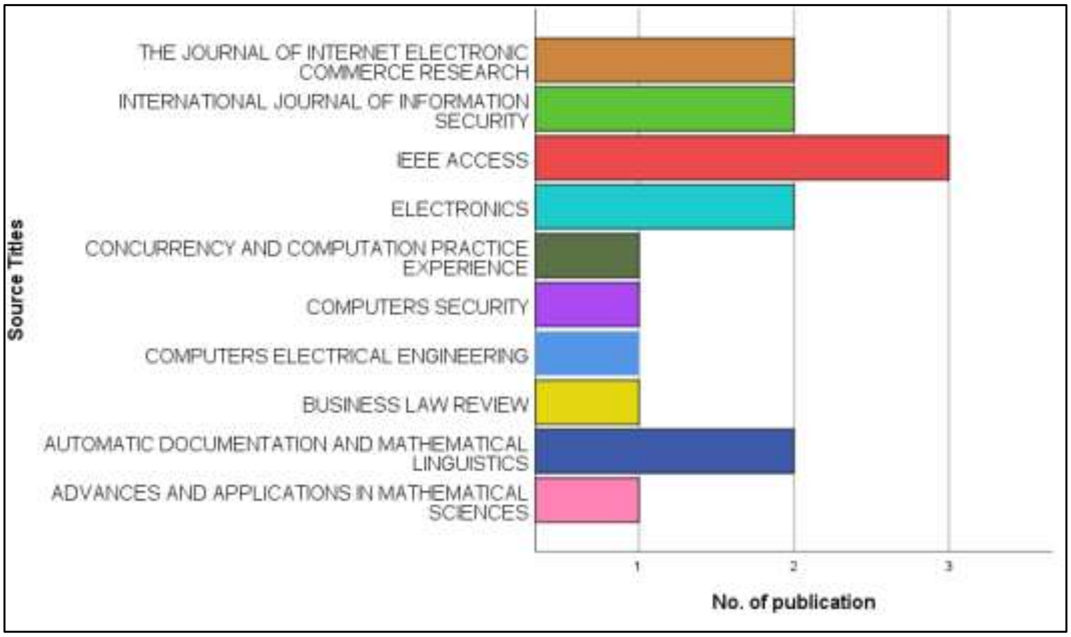

Fig 5: Journal statistics for Publications on topic blockchain in the ten most popular affiliations.

(Source: visited webofknowledge.com accessed on 19th March 2021)

IV. FUTURE RESEARCH DIRECTION

The blockchain based e-voting systems discussed and ex- plained consist of various notable features in terms of their architecture and design. However, further improvements in the systems are possible, particularly in terms of increasing the scalability of the systems, in order to support practical large-scale voting scenarios. The presented research on e- voting systems using blockchain not only demonstrates the advantages of such a system in terms of security, reliability, dependability and transparency of the entire election process, but also encourages further research on utilizing frameworks like Hyperledger Sawtooth in designing an e-voting system to support scalability and practical application in realistic election scenarios. Table I summarizes the presented research.

Ensuring complete anonymity of the election process, by eliminating all correlation between voters and votes without the additional storage and computational overhead of separate blockchains for voter information and the vote information, is required.

Various existing designs for blockchain based e-voting systems incorporate the ability of the election administration to query the blockchain during the election process in order to check if the voter ID of the current voting block already exists in the blockchain, which introduces the possibility of inequitable misuse by accessing count of votes information during the election. This undermines the democratic principles and ideologies of a fair election, and thus, needs to be addressed using a better design of the blockchain implementa- tion. Moreover, existing system designs utilize techniques like digital signatures and encryption to ensure the reliability of the system, but do not address scalability in the design decisions. The proposed solution aims at resolving these issues in a Hyperledger Sawtooth framework implementation, to ensure scalability using parallel transaction processing, and using two distinct divisions in a single blockchain, to ensure anonymity and fairness in the voting process.

TABLE I
COMPARISON OF VARIOUS EXISTING E-VOTING SYSTEMS USING BLOCKCHAIN

Article	KeyDesign Choice/ Algorithm	Highlights of Proposed System	Limitations/Possible Improvements
Ben Ayed. (IJNSA, May 2017) [7]	Candidate-specific blockchains	Describes Estonia's I-Voting system and proposed a blockchain based e-voting system with each block consisting of block size, block header, transaction counter and transac- tion. A separate blockchain is used for each candidate.	Greater storage and processing overhead due to different blockchain for each candidate. Usage of a single blockchain can improve performance
Barnes et al. (2017) [5]	DistributedNode Architecture	The proposed system consists a scalable architecture for large-scale voting scenarios with national nodes managing constituency nodes which in turn manage local nodes. Dif- ferent private/public key pairs within each constituency node and its corresponding local nodes improves security and decentralizes vulnerability. Two blockchains are used - one for voter information containing the voter's vote token prior to voting, and one for the voter's vote.	A robust, scalable and secure system proposed can be further improved by using Hyperledger Sawtooth to parallelize transactions.
Liu et al.(IACR, 2017) [8]	Blind Signature	Voting block consists of sender's public key, receiver's public key and vote message. Utilizes blind signature process to allow organizer and inspector to sign the vote hash without revealing the actual vote.	Though this verification process adds additional security to the system, it introduces greater latency and delay in large- scale e-voting scenarios.
Yu et al. (ISC, 2018) [9]	Hyperledger Fabric with Practical Byzantine Fault Tolerance	Utilizes Hyperledger Fabric as the blockchain framework, consensus using practical byzantine fault tolerance, and short linkable ring signature method for scalability	Proposed system can be further improved by utilizing Hy- perledger Sawtooth, which supports parallel execution of transactions.
Ganji et al. (Dell EMC, 2018) [13]	Multi-chain frame- work based system	Specifies storage of votes in the form of assets, in a secure, usable and scalable manner. Multi-chain blockchain network in used in this proposed system, which limits each voter to a single	Proposed system consists of greater delay as secret message provided by each voter has to be verified by the TTP with the election commission, which then generates a reference number that can be used to view candidates and cast a vote.

		transaction. Trusted Third Party (TTP) is used to verify the validity of the voter using a secret message provided to the TTP by the voter.	
Hjálmarsson et al. (July 2018) [12]	Election as a smart contract	Proposed system consists of a district node which manages the smart contract of the boot node. Frameworks recommended are Exonium, Quorum and Geth.	Exonium is a paid system that can be utilized using cryptocurrency, making it expensive for large-scale implementa- tion, when other free and equally-powerful frameworks are available. Quorum and Geth are Ethereum based frameworks which do not support parallel execution of transactions, which limits scalability and speed. Proposed system can be further improved by utilizing Hyperledger Sawtooth, which supports parallel execution of transactions.
Patil et al. (IRJET, Nov 2018) [10]	General explanation of blockchain based voting systems	Generalized e-voting system using blockchain is proposed with SHA encryption of voter information. The vote block is added to the selected candidate's blockchain.	A different chain for each candidate introduces greater overhead. The system does not discuss implementation using any specific framework. The advantages of blockchain based voting processes are highlighted.
Yi. (EURASIP, 2019) [14]	Elliptical Curve Cryptography	The proposed system utilizes elliptical curve cryptography in which voter generates signature of their vote block using a private key, with the signature verified using the voter's public key present in a Public Key Infrastructure database.	Even though the system proposes an elaborate procedure of verification of the vote blocks, the PKI database used is still a vulnerable, which if exposed, can invalidate the entire process.

V. CONCLUSION

To solve the problem of traditional voting systems, e-voting systems using blockchain is a promising research venture. Blockchain systems guarantee security, reliability, decentral- ized storage and anonymity. As a result, designing and imple- menting e-voting systems using blockchain ensures public and individual verifiability, dependability, reliability, consistency, auditability, anonymity, transparency, scalability, eligibility, authentication and fairness through principles of consensus, cryptography, digital signatures, and various blockchain mech- anisms. The ideal implementation in terms of making the e- voting system faster, lighter and scalable is the Hyperledger Sawtooth framework, due to support for parallel processing of transactions. Further research can be performed into us- age of frameworks like Hyperledger Sawtooth in designing and implementing realistic, robust and practical e-voting sys- tems which can be utilized in large-scale voting scenarios. The research presented not only encourages exploration of blockchain technology in practical voting processes, but also demonstrates the plausibility of utilizing blockchain to develop secure and reliable systems in a multitude of domains like finance, supply chain, trade and so on.

REFERENCES

1. *Kirillov, Denis, Vladimir Korkhov, Vadim Petrunin, Mikhail Makarov, Ildar M. Khamitov, and Victor Dostov. "Implementation of an E- Voting Scheme Using Hyperledger Fabric Permissioned Blockchain." In International Conference on Computational Science and Its Applications, pp. 509-521. Springer, Cham, 2019.*
2. *Wang, Baocheng, Jiawei Sun, Yunhua He, Dandan*

Pang, and Ningxiao Lu. ”Large-scale election based on blockchain.” Procedia Computer Science 129 (2018): 234-237.

3. *Moura, Teogenes, and Alexandre Gomes. ”Blockchain voting and its effects on election transparency and voter confidence.” In Proceedings of the 18th Annual International Conference on Digital Government Research, pp. 574-575. ACM, 2017.*
4. *”Blockchain Tutorial.” Weka, Solidity, Org.Json, AWS QuickSight, JSON.Simple, Jackson Annotations, Passay, Boon, MuleSoft, Nagios, Matplotlib, Java NIO, PyTorch, SLF4J, Parallax Scrolling, Java Cryptography. Accessed September 11, 2019. https://www.tutorialspoint.com/blockchain/index.htm*
5. *Barnes, Andrew, Christopher Brake, and Thomas Perry. ”Digital Voting with the use of Blockchain Technology.” Plymouth University. Accessed Dezembro 15 (2016): 2017.*
6. *Hardwick, Freya Sheer, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis. ”E-Voting with blockchain: an E-Voting protocol with decentralisation and voter privacy.” In 2018 IEEE Inter- national Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1561-1567. IEEE, 2018.*
7. *Ayed, Ahmed Ben. ”A conceptual secure blockchain-based electronic voting system.” International Journal of Network Security & Its Appli- cations 9, no. 3 (2017): 01-09.*
8. *Liu, Yi, and Qi Wang. ”An E-voting Protocol Based on Blockchain.” IACR Cryptology ePrint Archive 2017 (2017): 1043.*
9. *Yu, Bin, Joseph K. Liu, Amin Sakzad, Surya Nepal, Ron Steinfeld, Paul Rimba, and Man Ho Au. ”Platform-independent secure blockchain- based voting system.” In International Conference on Information Secu- rity, pp. 369-386. Springer, Cham, 2018.*
10. *Harsha V. Patil, Kanchan G. Rathi and Malati V. Tribhuwan. “A Study on Decentralized E-Voting System Using Blockchain Technology”. International Research Journal of Engineering and Technology (IRJET). Volume: 05, Issue: 11, (Nov 2018).*
11. *Fusco, Francesco, Maria Ilaria Lunesu, FILIPPO EROS Pani, and Andrea Pinna. ”Crypto-voting, a Blockchain based e-Voting System.” In KMIS, pp. 221-225. 2018.*
12. *Hjálmarsson, Fririk., Gunnlaugur K. Hreiarsson, Mohammad Hamdaqa, and Gísli Hjálmtýsson. ”Blockchain-based e-voting system.” In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983-986. IEEE, 2018.*
13. *Ganji, Raghavendra, and B. N. Yatish. ”ELECTRONIC VOTING SYS- TEM USING BLOCKCHAIN.” (2018).*
14. *Yi, Haibo. ”Securing e-voting based on blockchain in P2P network.” EURASIP Journal on Wireless Communications and Networking 2019, no. 1 (2019): 137.*
15. *”What is a Digital Signature? - Definition from WhatIs.com.” SearchSecurity. Accessed September 11, 2019. https://searchsecurity.techtarget.com/definition/digital-signature*
16. *Sitoh, Paul. ”What Are the Differences Between Ethereum, Hyperledger Fabric and Hyperledger Sawtooth?” Medium. Last modified February 14, 2019. https://medium.com/coinmonks/what-are-the-differences- between-ethereum-hyperledger-fabric-and-hyperledger-sawtooth- 5d0fc279d862*
17. *”Introduction - Sawtooth V1.0.5 Documentation.” Hy- perledger Sawtooth. Accessed September 11, 2019. https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html*
18. *A. Chaudhari, and P. Mulay, “A bibliometric survey on incremental clustering algorithm for electricity smart meter data analysis,” Iran Journal of Computer Science, vol. 2, no. 4, pp. 197–206-197–206, 2019.*
19. *Archana Chaudhari, Rahul Raghvendra Joshi, Preeti Mulay, Ketan Kotecha, and P. Kulkarni, “Bibliometric Survey on Incremental Clustering Algorithms,” Library Philosophy and Practice (e-journal), vol. 2762, 2019.*
20. *A. Chaudhari, and P. Mulay, “Algorithmic analysis of intelligent electricity meter data for reduction of energy consumption and carbon emission,” The Electricity Journal, vol. 32, no. 10, pp. 106674, 2019/12/01/, 2019.*
21. *A. Y. Chaudhari, and P. Mulay, “Cloud4NFICA-Nearness Factor-Based Incremental Clustering Algorithm Using Microsoft Azure for the Analysis of Intelligent Meter Data,” International Journal of Information Retrieval Research (IJIRR), vol. 10, no. 2, pp. 21-39, 2020.*