Proceedings of the Second International Conference on Inventive Research in Computing Applications (ICIRCA-2020)
IEEE Xplore Part Number: CFP20N67-ART; ISBN: 978-1-7281-5374-2

E-Voting Systems using Blockchain: An Exploratory Literature Survey

Vivek S K*
Undergraduate Student
B.M.S. College of Engineering
Bengaluru, India
viveksk69@gmail.com

Yashank R S*
Undergraduate Student
B.M.S. College of Engineering
Bengaluru, India
rsyashu@gmail.com

Yashas Prashanth*
Undergraduate Student
B.M.S. College of Engineering
Bengaluru, India
yashprash@gmail.com

Yashas N*
Undergraduate Student
B.M.S. College of Engineering
Bengaluru, India
yashasn14598@gmail.com

Namratha M*
Assistant Professor
B.M.S. College of Engineering
Bengaluru, India
namratham.cse@bmsce.ac.in

***Abstract*—E-Voting or electronic voting is a means for the election process to be conducted without the use of traditional paper ballots. The e-voting process, to be implemented in a large-scale scenario, requires the addressing of concerns concerning the security and reliability of such a system. The Blockchain technology, introduced by Satoshi Nakamoto using the cryptographic currency Bitcoin in 2008, opens up possibilities of designing and developing a secure, transparent and decentralized system with the absence of a third party for access and control, in the election procedure of casting and counting of votes.**

***Index Terms*—decentralized nature, distributed ledger, Trusted Third Party, RSA encryption, Hyperledger Sawtooth,**

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 security, 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 elections [1]. 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 [2].

The ideology of designing and implementing an e-voting system using blockchain overcomes the majority of drawbacks of standard e-voting systems and offers encouraging research initiatives [3]. 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 [4].

*Equal contribution from all authors

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 (permissioned), 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 [5]. 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 improve 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 [6]. 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 constitute of the following requirements and features [7] [8]:

- Public Verifiability: All stakeholders of the election process (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 cryptography 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 cryptography 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.

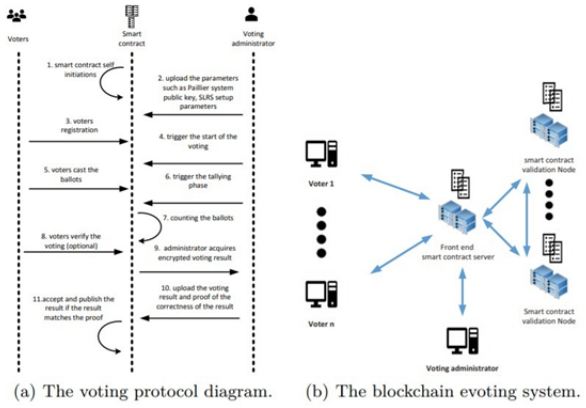
- Eligibility: Making sure that only eligible candidates have access to the system.
- Authentication: Authenticating users wishing to access the e-voting system, using a unique voter ID issued to them, along with other credentials.
- Fairness: The election results are not live. Due to the absence of 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 [9]:

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

The architecture can be summarized as follows:



(a) The voting protocol diagram. (b) The blockchain evoting system.

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 [7] [10]. 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 implementation using the sidechain technology, in which two sidechains are linked to a parent blockchain [11]. 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 [12]. 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 [13]. 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 required 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.

Various authentication and security methods which can be applied are:

- Elliptical Curve Cryptography [14]: This consists of two steps:
  - Initialization:
    - Each voter generates private key
    - Each voter generates public key from the private key (Identity element O, elliptical curve base point G, integer n such that $nXG = O$, then create private key D_a)- public key $Q_a = D_aXG$
    - The private key is not shared by voters
    - Public keys are sent securely by voters to the centralized database called the Public Key Infrastructure (PKI)
    - Miners are randomly elected
    - First block (genesis block) is generated
  - Voting:

- SHA 256 to generate the hash value of the vote. H= Hash (ID + vote + timestamp)
- Voter's private key to generate signature S of hash value H
- Voter sends ID, vote, timestamp, S to the miner
- The miner obtains voter's public key from a centralized database called the Public Key Infrastructure (PKI) using voter's unique voter ID
- Miner uses SHA 256 to generate hash value using H=Hash (ID + vote + timestamp)
- Miner uses the public key to verify S and get H'
- If H and H' are the same, signature S is accepted
- Miner queries and verifies that voter has right to vote
- Miner generates a new block by including the previous block's hash value and information of the current vote.

However, this design of implementation contains a vulnerable database of the public to private key mappings of voters, which if compromised, can lead to misuse and invalidity of the entire process. Moreover, due to the absence of an encryption mechanism of the voting block consisting of the voter ID, vote, timestamp and signature, there is a constant threat of sniffing (interception) during the transfer from nodes to the miner.

- Blind Signature [8] [15]: Blind signature procedure can be performed on the hash value by the election organizer and/or inspector. The vote string V, consisting of the choice code, zero string and random string, is hashed and passed through a computing function C_{Voter} to produce $C_{Voter}(hash(V))$. The voter then creates two messages containing $C_{Voter}(hash(V))$. One of the messages is sent to the election organizer and the other message is sent to the election inspector. The organizer and inspector receive their respective messages and sign the message using their private signature $S'_{Organizer}$ and $S'_{Inspector}$ respectively. Upon receiving the messages from the election organizer and inspector, the voter passes each message through the inverse computing function C'_{Voter}, in order to obtain the messages signed by the organizer and inspector ($S'_{Organizer}(Hash(V))$ and $S'_{Inspector}(Hash(V))$). Lastly, the voter sends the 'ballot' consisting of the vote string, and signatures from the election inspector and organizer to the organizer, using a pair of private asymmetric keys pk' and sk'.
- Short-Linkable Ring Signature [9]: Linkable ring signature (LRS) can be applied in our system to protect the privacy of the voters. In practice, the short linkable ring signature (SLRS) is applied to make the size of the signature constant, with the growth of voter numbers. SLRS has the following features:
  - Every ballot that is accepted by the system is from one of the valid users
  - The voter can check whether his/ her ballot was counted by the blockchain.
  - The size of the signature is constant to support scalability.
  - Double-voting is prevented

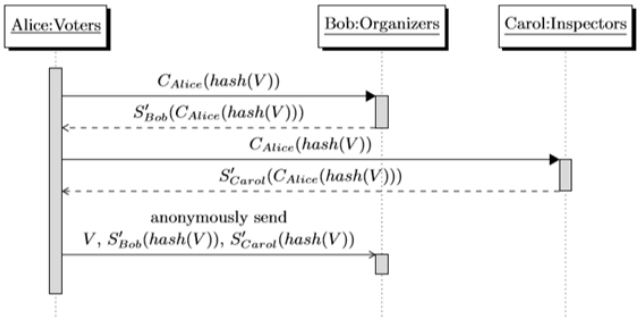


Fig. 2. Sequence Diagram of the Blind Signature Process [8]

E. The Hyperledger Sawtooth Framework

The Hyperledger Sawtooth framework is a flexible framework- it can be designed to act as a public blockchain network, or a permissioned one [16]. This framework consists of an entity called the transaction processor, which provides a platform for the computational and business logic of blockchain, the smart contract, to execute. The validator in this blockchain network is responsible for validating the signature of the received block, directing it to the transaction processor, and adding the block to the blockchain once it is sent back by the transaction processor.

One of the most powerful and beneficial features of the Hyperledger Sawtooth framework pertinent to an e-voting system, is the ability of the framework to group transactions to be performed in batches, and execute the transactions in parallel [17]. This increases the scalability of the system, for large-scale voting implementation scenarios. In addition, the framework can be developed as a permissioned network, thus allowing only the registered polling stating nodes to transfer voting blocks to the blockchain network.

III. Discussion

The blockchain based e-voting systems discussed and explained 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.

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

Article	Key Design 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 transaction. 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]	Distributed Node 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. Different 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 Hyperledger Sawtooth, which supports parallel execution of transactions.
Ganji et al. (Dell EMC, 2018) [13]	Multi-chain framework 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 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.	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.
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 implementation, 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.

IV. PROPOSED METHODOLOGY

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 implementation. 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.

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, decentralized storage and anonymity. As a result, designing and implementing 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 mechanisms. 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 usage of frameworks like Hyperledger Sawtooth in designing and implementing realistic, robust and practical e-voting systems 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 International 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 Applications 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 Security, 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 SYSTEM 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." Hyperledger Sawtooth. Accessed September 11, 2019. https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html