Plasma Voting: A Secure e-Voting Platform

Alisha Punwani, Prathamesh Pendal, Pallavi Saindane, Aditya Sajeev

Department of Computer Engineering, Vivekanand Education Society's Institute of Technology, Mumbai 400074, India

Publication Info

Article history:
Received : 12 February 2020
Accepted : 26 May 2020

Keywords:
Blockchain, e-Voting, smart contracts, smart contracts, metamask

Corresponding author:
Pallavi Saindane
e-mail: *pallavi.saindane@ves.ac.in*

Abstract

Voting is a process where people vote to raise opinions about the contestants and make important decisions collectively. Having a transparent, secure and reliable voting system is the need of the hour. Firmly registering and splitting transactional data, constructing computerized and organized delivery chain processes, improving transparency around the entire value chain are a few examples of these difficulties. Blockchain provides a potent method to engage these problems. This paper provides a basic execution of a blockchain built e-Voting system using Ethereum blockchain provided by Ganache locally, while it also discusses the feasibility, future scope and liabilities understanding the needs of a voting system. The review explores that various possibilities are free for making use of blockchain in diverse business sectors; yet, there are still some challenges to be addressed to achieve higher usage of this technology, with some advancements, this technology can prove to be a boon in near future.

1. INTRODUCTION

Voting has now become a way to make a collaborative and collective choice, or explicitly raise an opinion among a meeting or collection of electorates. During balloting, the person to be selected is the contestant of an election, and the individual that draws a poll for his or her chosen candidate is the voter. Since the beginning of the 17th century, voting has been the habitual apparatus by which present day democracy is operating. In this paper we propose a basic implementation of an e-Voting system using Ethereum blockchain. It is implemented using the Ethereum blockchain along with truffle and ganache at the backend. Users can connect to the system using metamask which is a Google chrome extension. Here, we have performed smoke tests for test cases for various scenarios such as the information verification of the contesting candidates, eligibility of the user to vote, maintaining the vote counts of the candidates and a check to avoid double voting.

Blockchain: Blockchain uses an associate network of computers to perform and validate transactions. Blockchain can be defined as an increasing list of blocks or records. They are connected using cryptography. The cryptographic hash of the last block is linked with the current block. In the Proposed System, we will use DApp (Decentralized application) made using a private blockchain.

Ethereum Platform and Ether: Ethereum is an operating system featuring smart contracts. It is a public, open-source, blockchain-based distributed computing platform Ether can be considered as cash. It is used to make transactions on an Ethereum Blockchain. There is no requirement of a third person to approve the transaction.

Node Package Manager: NPM is provided by Node.js. It consists of a command line client, NPM and an online database of public. NPM is used for installing the required node packages.

Truffle Framework: Truffle is the framework used for testing, building and deploying applications on the Ethereum network. It has some primary development frameworks for Ethereum smart contracts and decentralized applications (DApp) like Truffle and Ganache. Here we can Compile, Migrate and Run in order to compile the contracts, deploy them and run their unit tests. Thus it is an environment for development and a framework for testing and helps by providing project structure, files and directories.

Ganache: Ganache (Truffle Suite) is used to provide a modifiable local Ethereum Blockchain. Ganache provides a personal blockchain for Ethereum development which develops contracts and applications and also runs tests. It helps to perform all actions on the main chain without any cost. Ganache provides us with the external accounts, each account has a private key, which is used to log into metamask.

Metamask: Metamask is a chrome extension, it is used to access DApps that are ethereum enabled in your browsers. It allows users to manage and import accounts using private keys on their Ethereum wallets. It allows a user to interact with their DApps. Voters can connect to the application through metamask extension. Ethers or gas required to

cast a vote (or write to a blockchain) are available with the accounts provided by Ganache. These accounts are needed to be imported in Metamask using their private keys.

2. MOTIVATION

In various countries like Ghana and some parts of sub-Saharan Africa there are cases of inaccurate recording of votes during elections. There are instances when the recorded votes are changed either accidentally or intentionally. Using such malpractices the elections are also won sometimes, if the system allows the figures to be manipulated, this puts the integrity of elections at stake and also is a source of various crimes in Africa. A fair election should consist of transparency, integrity and bring trust among the people by ensuring proper transfer of votes from point to point. These requirements can be satisfied by using Blockchain. Blockchain can built Decentralized system, and the database cannot be owned by a single person or entity, rather it belongs to various stakeholders.

3. RELATED WORK

According to Nir Kshetri et.al [1], E-Voting is one of the important sectors that can get impacted by blockchain Technology. Using digital-currency analogy, BEV gives each voter a "wallet" with user credentials Users are also given a coin. The user can use his/her coin to vote only once. After that the coin is deposited into the wallet.

According to Fridrik P Hjalmarsson et.al [2], this paper starts evaluating some blockchain frameworks and evaluates blockchain applications as a service to implement public, distributed and decentralized e-Voting systems. Moreover through case studies, this paper evaluates distributed ledger technologies like election and says implementation of a blockchain application for the same improves the security, also reducing the nationwide cost for elections.

According to Ahmed Ben Ayed [3], Blockchain can be used to develop new digital services. In this paper, they have designed an electronic voting system which is secure, reliable and anonymous and can be used in local or national elections which help increase the vote count and public trust.

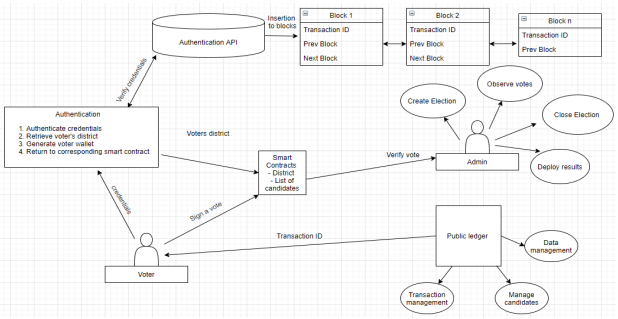

Figure 1: System Architecture

In the paper [12] the author discusses growth in industries. Cyber-crime, Partnerships which are based on trust and fraud are the main parameters on which growth in industries depends increasingly. The author suggests that Blockchain will enable faster product innovations, more agile value chains, closer customer relationships, and quicker integration with IoT and cloud technology addressing the challenges mentioned above. When we work with trusted contract trading costs are lowered in Blockchain. This can happen without intervention of third parties.

According to Angraal S. et al. [13], Blockchain technology has penetrated several fields. One of the important fields is the healthcare unit. In the healthcare industry electronic health records of patients must be kept private. Blockchain improves transparency in health records and improves authenticity. It performs this task using many use cases like electronic health records, streamline claims processing. The transparency of components used to build medications for patients, track distribution of medicine, and ensure the authenticity of prescriptions can be gained using Blockchain.

The author of paper [14] proposes a new technology. Transfer of assets between multiple Blockchains can be achieved using pegged side chains. Users can access the assets of people who own them. Authors can interact with each other using cryptocurrency.

4. EXISTING SYSTEM

Elections use electronic voting machines (EVMs) for polling the votes. The voter can vote according to the lists of candidates or vote for other people he/she prefers. Voting ballots have to be anonymous and noted by the voters in personal cubicles so that no person other than the voter can find out for whom a citizen has balloted. EVMs consist of two units, the control and balloting units. An EVM can cater to a maximum of 64 candidates and can record a maximum of 3840 votes. It is not possible to vote again once the vote is casted by pressing the button on the EVM.

Shortcomings: Errors during data entry, security issues, time and cost inefficient, too much paperwork and

Figure 2: User interface after voting showing the vote count

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

many other issues

5. E-VOTING SYSTEM

The online vote casting is referred to as electronic voting (e-vote casting). It is an approach for casting and counting votes. Users of e-vote casting are voters and authorities that handle the elections. Here the voter can post his/her votes electronically to any nearby election authorities via e-vote casting. The election governments are accountable for accumulating votes from citizens. E-voting with high efficiency and flexibility can save time and effort, that's getting more attention in place of conventional balloting. With the advancements of the Internet, e-balloting became the crucial method of corporations.

6. SYSTEM DESIGN AND IMPLEMENTATION

6.1. Comparison of different Blockchain Platforms

The paper [16] discusses BLOCK BENCH which is the "first evaluation framework for analyzing private blockchains." BLOCKBENCH measures performance in terms of scalability, throughput, latency and fault-tolerance and also gives an overall view. Using BLOCKBENCH for three major private blockchains: Ethereum Hyperledger Fabric and Parity, a comprehensive assessment was conducted. After comparison through various major and minor benchmarks, it suggested that Ethereum has the highest latency when compared to Parity and Hyperledger Fabric. Ethereum uses the PoW consensus protocol. After measuring the CPU and network utilization it was concluded that Hyperledger is communication bound while Ethereum is CPU bound. It is noted that while Ethereum's latency and throughput degradation is almost linear beyond 8 servers, Hyperledger nearly stopped working after 16 servers when it comes to the scalability factor. It was seen that Ethereum is nearly unaffected by the change, when they ran the systems with 8 clients for over 5 minutes, during which they killed off 4 servers at 250th second, while this was not in the case of Parity and Hyperledger. Keeping all the above discussed properties, we have selected Ethereum blockchain for our implementation

Blockchain uses a peer-to-peer network of computers to perform and validate transactions. In the Proposed System, we will use DApp which is built using a private blockchain. Voting has always been a source to make collective decisions or express one's opinions. Keeping in mind the integrity and the security of a voting system. We kept the following test cases in my mind while designing the system shown in Figure 1:

- Test case for Candidate Count
- Test case for Candidate Information Verification
- Test case for Voting of a Candidate
- Test case for Validation of a Candidate
- Test case to check double voting

The building blocks of the project are as follows: The frontend of an application is what's visible to you, it's an uncomplicated interface like a website or app. HTML, CSS and JavaScript were used in its development. Backend of the application is one or more smart contracts which use logic and are written using the solidity language. They are the integral building blocks of a dApp.

The system was built keeping two types of users in mind, the Admin will be responsible for creating elections, verifying the candidates, observing and deploying the election results while the voter can view elections, vote for the candidate of their choice and observe election results. The current implementation only consists of the voter's side of the application .Frontend gives an user interface to the system users to provide some inputs in this case their votes and access the blockchain. It was developed using HTML, CSS and JavaScript pages. Pages in the frontend consist of the HTML/CSS page that is index.html whose interface is provided by Metamask (Chrome extension) and whose actions are scripted by a JavaScript page called app.js.

The following parameters were also considered by the system:

- Eligibility: According to rules only eligible voters can vote to the candidates.
- Uniqueness: Once a user has submitted his vote to the candidate of his choice he won't be able to vote again.
- Privacy: Anyone other than the admin of election cannot see information about voters.
- Accuracy: System takes user's vote to his intended candidate accurately.
- Efficiency: The vote counts are calculated within a minimum amount of time.

Smart contracts written were judged for the following evaluation measures, considering 2 candidates contesting the election. The following smart contracts were written in solidity to establish connection to the local ethereum blockchain provided by Ganache. They perform the following functions.

- Election. Sol - The entire voting process code is written in this smart contract. This contract also verifies whether the voter is a valid voter or not and keeps the count of votes. This smart contract acts as a virtual ballot.
- Migration. Sol - This is a subordinate Smart Contract file. It keeps a track of all the migrations that occur each time the blockchain is restarted and reset. After using commands like truffle migrate --reset, it also initializes the count to zero.

After connecting to their accounts with metamask, the voters can see the following interface. The voter can now select the candidate he/she wishes to vote.

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

Once the voting is performed the voter cannot vote again. After voting he/she can see the current vote count of the election, hence he/she can keep a track of the votes their selected candidate gets as shown in Figure 2.

7. IMPLEMENTATION RESULTS

Table 1 shows all the tests being executed and time taken to execute each test and run the contracts mentioned above individually.

Table 2 evaluates the average cost used for deploying contracts. Seven observations are taken and the average is taken. The cost of deployment always remains the same.

This implementation is based on a local ethereum blockchain provided by Ganache. Gas is used in ethereum blockchain to make transactions and deploy contracts. Nodes in the blockchain attempt to maximise profits by determining the cost of a transaction compared to computational cost. This cost should be reduced to make a blockchain project viable.

8. COMPARISON WITH EXISTING SYSTEMS

Table 3 compares normal voting and decentralized e-voting. Depending on different performance measures an overview of both the processes are given:

Currently there are multiple E-voting system platforms available over the internet. One of such examples is the Helios voting system. It has multiple versions of its own. Helios 1.0 was found with some potential threats. Hence it is upgraded to Helios 2.0 by overcoming those threats. But Helios 2.0 has gone through cross-site-scripting (XSS). The attack was achieved using browser rootkit. It is a script which is capable of capturing passwords and monitoring traffic. There are some new applications over the internet which are based on Helios such as Zeus, Apollo. Apollo has tackled the problem of XSS. Current voting systems are vulnerable to most of OWASP top vulnerabilities. Voting system using blockchain can bring revolutionary change to the e-voting platform. Currency used by the blockchain based voting system is Ether and gas. We can initialize elections by writing smart contracts for them. Functionality of EVM is mainly controlled by smart contracts. As we have seen above we can write promise chains to avoid duplicity. Verification of candidates of election, for count of votes

Table 1: Contract Execution Time

Sr No.	*Test*	*Contract*	*Avg time(ms)*
1	Test for candidate count	Initialization with 2 candidates	102 ms
2	Test for candidate information verification	Initializes the candidates with the right values	195 ms
3	Test for voting a candidate	Allows a valid voter to make a vote	602 ms
4	Test for validation of candidates	An exception is thrown for invalid candidates	493 ms
5	Test to check double voting	An exception is thrown in the case of double voting	985 ms

Table 2: Contract Deployment

Contract	*Time(ms) for 7 observations*	*Cost(gas)*
1	715	277462
2	1367	277462
3	4217	277462
4	3455	277462
5	6895	277462
Average	3330	277462

Table 3: Comparative Analysis

Sr No.	*Features*	*Existing Voting*	*e-Voting with blockchain*
1	Updating votes	One cannot change the vote	One can change the vote
2	Authentication	Not possible	Every user has a unique id
3	Easy access	One needs to be present	One can vote from anywhere
4	Accuracy	Votes can be tampered	Votes cannot be tampered
5	Vote calculation	Slow, requires more time	Faster and easy
6	Live update	Not Possible	Possible
7	Cost required	Cost depends on various factors	One time set up cost
8	Technology used	Logical contracts	Smart contracts

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

etc. Ethereum virtual machine (EVM) performs voting by allowing peer-peer, transparent and decentralized way of voting. As blockchain is decentralized most of OWASP vulnerabilities don't work on it. Every vote is encrypted using complex hashing functions.

9. RESEARCH GAP AND CHALLENGES IDENTIFIED FOR LARGE SCALE IMPLEMENTATION

Blockchain is originally a managing method of Bitcoin which is decentralized, it was crafted to issue and transfer money for the users of the Bitcoin currency and is independent of the control of any third party organizations. The public transaction ledgers that are made, cannot be modified or deleted, even after the nodes approve all the data. This is also why it is recognized for its security, anonymity and data integrity features. Blockchain has also been applied to make an environment for node-to-node data sharing in a cloud and digital contracts. The pillar of this technology is data integrity.

Blockchain also has some limitations and challenges when it comes to technicality. Swan [18] presents technical research gaps for adaptation of Blockchain in the future.

Latency: To achieve better security, more time must be spent on a block in the chain, to surpass the cost of double spending attacks. Double spending is spending money more than once successfully, Bitcoin verifies every transaction added to the blockchain to lower the problem of double spending by taking care that inputs for each transaction are not been used previously. This should be done in seconds but it usually takes around 10 minutes.

Throughput: The Bitcoin network's throughput at its full strength is computed as 7 tps (transactions per second). While other processing transaction networks are Twitter (5,000tps) and VISA (2,000tps). The throughput of the network needs to be enhanced.

Security: The Blockchain used now has a 51% chance of attack. In a 51% attack a single entity would have all the power of the network's mining hash-rate, sufficient to make changes to the blockchain. More research is needed to overcome this problem

Size and bandwidth: The size of a Blockchain in the Bitcoin network is over 50,000MB (February 2016). Blockchain could grow 214PB in every year if the throughput is on the levels with VISA. The number of transactions that can be performed are limited (on average 500 transactions in one block). Bandwidth and Size issues need to be resolved

9.1. Challenges in adopting blockchain

Promise system in blockchain is trustworthy. However we have to face many challenges in adaptation and deployment in industrial applications. Challenges can be categorized into two categories 1. Technical 2. Non-Technical. Technical challenges include security, scalability, Integration on various platforms.

Integration: It is very challenging to integrate blockchain based systems with the existing systems. Blockchain provides solutions for multi distributed applications that are used in companies and organizations and not independent applications. The challenge is due to security and interoperability issues. Blockchain in future will enable many doors to add new functions and features that support futuristic business models. In addition with this issue, many applications, old and new, are built by different vendors using various different platforms and programming languages, with different operating environments and different methodologies. The integration process becomes more complex. Any good integration model must maintain the integrity, the correctness and the trustworthiness of the existing systems in a way that it stores accurate business data and information among all integrated systems along with maintaining the system's functionalities. Moreover, any integration should also maintain the security and safety of applications involved not risking the data in hand. The integration in any form must not lead to any availability or reliability issues or any kind of privacy concerns.

Secure Systems: When we talk about the voting system, security is the most important parameter. Main challenge of the EVM voting system is electronic fraud prevention. It can be avoided using Blockchain as Blockchain uses cryptography for transactions. If someone is making people vote by capturing them and forcing them by using incorrect means, then it will become a big issue similar to the present voting systems. We can find various applications of blockchain over the internet. Many attacks like Denial of service can be performed on the available applications, Blockchain services can become unavailable due to these attacks. Double spend is also a great threat to the blockchain in which an entity has to pay double cost for a single transaction. Double spend can occur to the communities which have less number of entities. This type of attack happens for applications based on cryptocurrency. If we don't have sufficient security for our application, then it can be very harmful for our application. Blockchain can operate across various platforms which makes it more vulnerable to the corresponding threats. Currently Blockchain provides some security measures which can give solutions to some problems. There is a need for more research in the security area, So we can trust blockchain without any hesitation.

Privacy: There are several types of Blockchains depending on the situation and requirements.

- Public Blockchain – It is a blockchain where anyone can access the blockchain publicly in the terms of

 2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

reading/writing to a blockchain. The user can access the blockchain without any permission.

- Consortium Blockchain – Only allowed users can see the transactions. Anyone allowed can do transactions here. It is usually operated by an admin or stake holder.
- Private Blockchain – It is a type of blockchain controlled by one stakeholder. This type can be used for transactions within an organization

Different blockchain types are used in applications that differ. Hyperledger is a consortium blockchain that gives an open source blockchain to various industry types while cryptocurrencies like Ethereum or Bitcoin make use of the public blockchain. All blockchain types have different issues or concerns regarding privacy or security. A private blockchain is relatively better when it comes to privacy but it is considered as an insecure environment as it is governed by a single entity. While, a public blockchain can be accessed by various entities so it has some privacy related concerns. With a consortium blockchain the privacy is at stake as some selected participants can still keep a track of all the transactions.

Scalability: Scalability nowadays is done by reducing complexity in hashing algorithms. Distributed ledger takes a major role in scalability. It consists of multiple entities and their transactions. It consists of a record of every transaction that has happened between the nodes. Hence the process is relatively complex. It is only efficient for blockchain of limited size. If nodes in blockchain generate large amounts of transactions it can affect the overall performance. Current applications over the internet generate large amounts of transactions. Achieving the highest Transaction per second is the ultimate goal in scalability of blockchain. However scalable blockchain provides higher efficiency in cost of each transaction, Latency in throughput.

There are several parts in blockchain which can effectively help in scalability.

- Proof of work (POW) algorithm - POW algorithm is scalable. In scalability of POW algorithms we can include proof of stake schemes. To increase scalability in application consensus period should be comparable with synchronization time.
- Scaling Bitcoin - It is observed that POW of bitcoin doesn't easily allow scalability. To increase scalability of blockchain with respect to bitcoin period of synchronization must be significantly smaller than runtime of consensus algorithm.

Another potential solution for scalability is VAPOR as discussed in the article [17].

Professional Preparation: Blockchain is a comparatively new technology in the mixture of technologies that exist today. Working with blockchain involves prepared professionals that know how to develop, deploy and utilize blockchain. As seen incorporating Information and Communication Technologies. (ICT) has seen affirmative outputs with respect to efficient and effective industrial and business applications and systems. ICT professionals are capable of managing and creating various types of applications. Blockchain related applications can possess some major integrity issues that as discussed in subsection 3.1. There's a domain of things that are to be considered by ICT professionals like the industrial sections they are working for, the technology that will be used to develop the application and so on. To design a fully integrated blockchain system the development team should have knowledge in varied fields of applications. With continuing shortage of professional and technically stable human resources, it is hard to find and train the required workforce for such projects.

10. FUTURE SCOPE AND CONCLUSION

If someone is making people vote by capturing them and forcing them by using incorrect means, then it will become a big issue similar to the present voting systems. Secrecy and End-to-End verifiability is very difficult to achieve. Whatever technical solutions selected, secrecy of the ballot will always be at risk as voting would take place without the supervision of authorities'. In some areas literacy rate is very low. Residents of that area cannot use Mobile phones, computers or any other electrical appliances. In those areas E Voting systems cannot be implemented. Current systems use very simple verification systems, In future these verification systems will be replaced by real time verification systems like Face recognition systems. Current E voting systems are only available on computers, but in future voting systems can be available on mobile phones which will increase ease of the voters. The biggest benefit of using a decentralized application is that there is no central authority involved on any data. Thus it is quite trustworthy. There is no danger of losing the data and also no one can interrupt with the election mechanism nor can anyone change or illegally access the data as blockchains are immutable. Once the person selects one candidate and votes for the same he cannot vote for any other candidate and also cannot change the vote, this is an asset in voting and helps legit voting avoiding any frauds and maintains the proper standards of voting. Thus blockchain is one of the best technology which can be used to conduct voting.

11. REFERENCES

[1] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In 2017 IEEE technology & engineering management conference (TEMSCON) (pp. 137-141). IEEE.

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

[2] [Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain Technology: Applications in Health Care. Circulation. Cardiovascular Quality and Outcomes, 10 (9).

[3] Antonopoulos, A. M., & Wood, G. (2018). Mastering ethereum: building smart contracts and dapps. O'reilly Media

[4] Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications, 9(3), 01-09.

[5] Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... & Wuille, P. (2014). Enabling blockchain innovations with pegged sidechains. URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, 72.

[6] Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K. L. (2017, May). Blockbench: A framework for analyzing private blockchains. In Proceedings of the 2017 ACM International Conference on Management of Data (pp. 1085-1100).

[7] Hanifatunnisa, R., & Rahardjo, B. (2017, October). Blockchain based e-voting recording system design. In 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA) (pp. 1-6). IEEE.

[8] Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain-based e-voting system. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 983-986). IEEE.

[9] Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. IEEE Software, 35(4), 95-99.

[10] Lee, K., James, J. I., Ejeta, T. G., & Kim, H. J. (2016). Electronic voting service using block-chain.Journal of Digital Forensics, Security and Law, 11(2), 8

[11] Singh, A., & Chatterjee, K. (2018, September). Secevs: Secure electronic voting system using blockchain technology. In 2018 International Conference on Computing, Power and Communication Technologies(GUCON)(pp. 863-867). IEEE.

[12] Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".