Blockchain based Decentralized Electronic Voting System:A Step towards Transparent Elections

Shehzad Latif [1] Tayyaba Anees[2]

School of Systems & Technology(University of Management & Technology)
School of Systems & Technology(University of Management & Technology)

Abstract
Public Elections are the best way to elect the government in democracy. Thus, it is the utmost responsibility of the state to organize non-fraudulent elections. With the advancement in technology we have an opportunity to switch our voting system from ballot paper to an electronic voting system. The Estonian voting system is one of the leading electronic voting systems which is still not perfect & need to improve its security & privacy features. Keeping in focus the privacy & transparency concerns this paper introduces a blockchain based decentralized electronic voting system for elections on large scale. The significant features of the proposed system are data integrity & transparency. Blockchain uses encryption & hashing to ensure the security of each vote. The scalability & verifiability in proposed system make the voting process more secured and reliable.

Key words:
Blockchain, e-voting, Bio metrics, Distributed Ledger, Authentication, Immutable Ledger

1. Introduction

Elections play a significant role to elect suitable person for the specific task. An election on Blockchain is a concept to make elections electronic and to maintain its database to immutable ledger, so no one can claim fraud in processes. Every center has its own recognized certificate from which it can make transactions to the network; there will be no chance of hacking. Every single activity can be logged on immutable ledger. By adding multiple nodes or peers on a system load sharing can be possible. Elections on Blockchain is based on decentralized immutable ledger so the data loss, and network downtime issues can overcome, and better performance can be provided by the system to end users and system administrators.

Blockchain is the first radical technology innovation of the 21st century. Blockchain uses very advance techniques for data security. Every block is signed from the previous block hash and by changing any data from any node by hacker block chain to network will automatically discard that node from the network. As, blockchain is a decentralized immutable ledger, data lost can be overcome and integrity will be guaranteed.

In Pakistan after every five years state is responsible to arrange national elections. Every citizen has a right to cast the vote to their desired candidates in elections through paper balloting. In the modern world with such advancement in technology we propose an electronic voting system for elections in Pakistan. But there isn't any system which claims fairness in election. Transparency, security, integrity & lack of confidence of people on the system are the major issues in the current voting systems. Our proposed system is based on blockchain and claim to be one of the transparent & secured systems for voting.

Our proposed system allows political parties to register on a single platform where the candidates can register to any party they want to join. Candidates can switch parties as per their desires. Also centers can be registered to assure that votes can be casted through a valid system. All registrations are performed by the administrator of the system. No one can be registered twice using same identity number. The voting application allows voters to cast votes using their fingerprints which fetch their identity related information from directory. A person can cast vote only once. Only verified votes will be considered for counting to issue the valid and transparent results.

The rest of paper is organized as follows: Section II discusses the motivation & literature review; Section-III is material and methods; Section IV is proposed solution; Section V Covers the implementation details & lastly Section-VI is Conclusion & Future Work.

2. Motivation And Literature Review

The prior motivation of this research paper is to provide secure electronic voting system for elections in Pakistan by proposing a reliable electronic voting mechanism based on blockchain. When electronic voting mechanism is available to every individual on its smart devices, every administrative decision can be made by people; or at least people's opinion will be accessible by the authorities. This will lead democracy in right direction. It is of great importance for us, as elections can easily be manipulated or tempered. Also, large scale elections are very

Manuscript received December 5, 2019
Manuscript revised December 20, 2019

expensive especially, if there are hundreds of distributed voting centers for millions of voters [1]. Electronic voting is the solution to the problem if implemented perfectly. This approach is older than blockchain. Hence, all examples so far used means of centralized computation and storage mechanisms.

Estonia is one of the best examples, as government of Estonia implemented one of the first complete e-voting solutions [2]. This concept was debated in 2001 & officially adopted in 2003 [3]. This system is still in use as many modification & improvements were made on the original scheme; which made it very robust & reliable. For authentication of voters they used smart cards & personal card readers as distributed by their government [4]. Every citizen with computer & internet along with the smart can caste his/her vote remotely. Citizens can also create digital petitions & proposal for laws & acts at the website of parliament which can be digitally signed by other citizens who want to support them by using these smart cards. Proposal of citizens will be discussed in parliament; if it achieves a prescribed limit of signatures. It is the excellent example to strengthen the democratic process in our beloved country by using computing & information technology.

The Estonian model is best in its nature but it also has some drawbacks too. Its centralization creates a single point of failure which may be attempted for hijacking & hacking. One of the most common examples is DDoS Attacks which can harm servers, databases and software's used. Administrators may also steal or manipulate valuable information during elections. Hence, scalability is an important issue of the above system. As, Estonia is less populated country; in comparison with it Pakistan is relatively very populated country with population estimated more than 20 billion.

Among countries using electronic voting trends, Switzerland is one of the top most countries. In Switzerland, every citizen with age above 18 can take an active part in elections held on various topics & discussions. They also started working on remote voting officially [5]. Few similar works are available on the internet which addresses the similar issues such as Follow my Vote [6]. Voters cast their votes independently & anonymously which are then get counted by applying the mathematical formula, because there can be a chances of fake votes. That's why this system put a margin to the ratio of results. Hence, it doesn't show the actual results.

Straw Poll [7] is another website which allows its users to create questionaries' and get answers through polling. People share the links of questionnaires and users having the link can cast their votes. It shows how the powerful electronic voting system is. Voter authentication, duplication of votes & non-repudiation are the major drawbacks of Straw Poll.

Y. Takabatake [8] in his research paper proposed a strong methodology for electronic voting based on Blockchain. Counter measures for anonymity & privacy of vote are considered by the using an intermediate unit b/w the voter & the candidate (wallets) along with two different coins for these intermediate coins (vote) transfers. Intermediate unit collect the coins (votes) sent by the voters & convert them into another currency using currency's wallet. As, a result new coins are send to candidates by the intermediate units. It is good in all aspects & very informative. But, it does not discuss the implementation aspects & nor provide a detailed discussion about it.

Our focus is on implementation work. We would like to build a solution to elections in our beloved country. We will assure its working in a way that election commission can easily create elections when needed and all participants can cast & keep track of their votes.

3. Material and Methods

The Blockchain technology provides transparency, trust & information security. Today the architecture of blockchain is being used widely in record keeping & maintaining sensitive databases. The blockchain network consists of many computers in a way that alteration of information is not possible without the consensus of whole network. The structure of blockchain is represented by a list of blocks with transactions in a particular order. Pointers & Linked List data structures are used in blockchain. Pointers represent the variables which keep the information about the location of other variable & Linked list represents the sequence of blocks where each block has data which is linked to the other block via pointers.

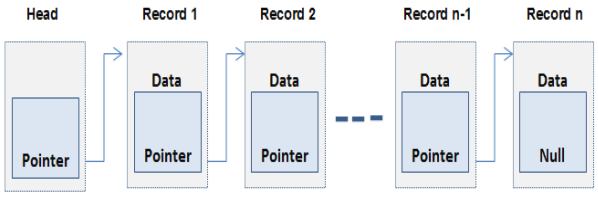

Fig. 1 Record Keeping in Block Chain

In Figure 1, logically the first block does not contain any pointer as it is first in the linked list. Similarly the last block contains pointer which has null value; which means that chain stops here. Figure 2 shows the blockchain sequence diagram for the connected list of records.

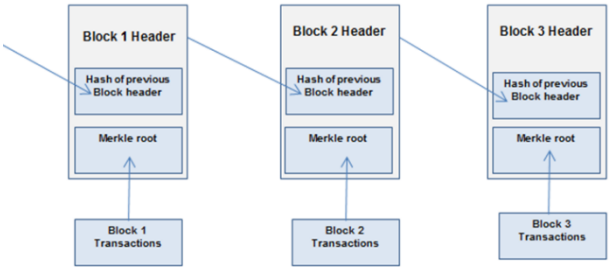

Fig. 2 Sequence Diagram for Connected List of Records

Structure of Blockchain can be categorized as:

1. Public blockchain
   In Public Blockchain anyone can access system & data. Examples are Bitcoin & Etherum.
2. Private blockchain
   It is totally opposite to public blockchain in which system is controlled by authorized users which invites participants.
3. Consortium blockchain
   In consortium blockchain structure few organizations are involved & procedures are setup & controlled by authorized users

As previously discussed, blockchain is distributed technology in which all participants hold a local copy. System can be centralized or decentralized based on the types of blockchain and its contexts. A public blockchain is considered to be open-ended and decentralized. All records are visible to the public and anyone can participate in the consensus process.

Components of Blockchain Architecture:

1. **Node** – Every computer within the blockchain architecture is known as node. Each node holds the copy of blockchain ledger
2. **Transaction** - It is the smallest building block of blockchain architecture which includes records & information etc.
3. **Block** – It is a data structure which keeps record of transactions distributed to all nodes.
4. **Chain** – Arrangement of blocks in sequential order is known as chain.
5. **Miners** – These are the specific nodes which verify the block before adding anything.
6. **Consensus-** Also known as Consensus protocols which are set to carry out the operations in blockchain.

Every transaction or new record within the block chain results in the creation of new block; which is then ensured to be get digitally signed to prove its genuineness. This block is added to the network after verification by the majority of nodes in the system.

A

Table 1: Comparison b/w Public, Private and Consortium Block Chain

Features	Public blockchain	Private blockchain	Consortium blockchain
Consensus process	Permission less	Needs permission	Needs permission
Consensus determination	All miners	Within one organization	Selected set of nodes
Centralization	No	Yes	Partial
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Read permission	Public	Public or restricted	Public or Restricted
Efficiency (use of resources)	Low	High	High

Decentralization

The industry has declared decentralization as the core component of blockchain. The decentralization of the computational system can be categorized into three main aspects:

1. Structural decentralization: Number of nodes does a system consist of. Number of nodes at any time can the system tolerates breaking down.

2. Political decentralization: Number of those nodes at any time can system tolerates breaking down.

3. Logical decentralization: The system's interface and data structure look more like a single monolithic object or not.

From a structural perspective, the block chain [9] is based on the peer-to-peer network, and there is no central controller, so it is decentralized. The blockchain makes it difficult for a few people to control the whole system through a consensus algorithm from a political point of view so it is political decentralization. Structural and political decentralization brings three advantages to block chain: fault tolerance, anti-attack and anti-collusion. In the blockchain, however, there is no node that can control and coordinate the book data generation. Each node coordinates to create a consistent account book through the consensus algorithm. It is the whole network's unified account book, so it is logically decentralized.

Advantages & disadvantages of decentralization

The five major advantages of block chain's decentralization are given below:

1. Fault tolerance: No single node depends on decentralized systems. Multiple nodes are mutually dependent which decreases the possibility of failures.
2. Protection against attacks:
3. Monopoly avoidance.
4. Collision avoidance.
5. Decentralization enables each node to function e fficiently on its own, and thus considerably Impr oving the node's functions and roles.

Decentralization has four major flaws too which are given below:

1. Decision making process is slow.
2. Wastage of resources.
3. Slow processing speed.
4. High Network Pressure

It is assumed that decentralization is not the best way to address all the problems [10, 11].

The mechanism of consensus determines decentralization. The main focus
of the consensus algorithm is to address the problem of B yzantine Generals
[12] and to achieve eternal quality in the assertive networ k environment; therefore, there might be one and perhaps more dishonest nodes in either the network that may inten tionally supersede the protocol or decode inaccurate infor mation, there seems to be a problem of decentralized network quality, and the expense is comparatively low eff ectiveness.
The level of "decentralisation" of a distributed ledger syst em is determined by the consensus mechanism. In general , the greater the level of centralisation, the lower the effec tiveness of the network. In order to raise the block chain speed as well as reducing energy consumption, the best approach is just to strengthen its consensus algorithm, that must address the problem of Byzantine Generals ; else it will no longer be a decentralized system.

Incentives

All network assets, device assets and hardware assets are offered by clients themselves in the decentralized block ch ain system, so each node is itself a service user and a su pplier. Clients will not participate if incentives are not offered to them. Hence, for each task like elections & generation of new block it offers tokens as incentives. Fairness is required a compensation & reward for the stakeholders to motivate them to participate & maintain the safe operations of the block chain.
This is just to avoid changing the details of a ledger by me ans of economic equilibrium,
Token is an eventual motivation method.Moreover, this method of motivation also encourages nodes to stay honest.If a covetous attacker had the capacity to control the immense power of all honest nodes than the full netwo rk CPU power, he is using this ability to acquire advantag es.
He will find that observing the game's rules is even more profitable. Accept the rules, as violating the rules can affe ct the system itself as well as endanger it's economic pow er's reliability.

Consensus Mechanism

Cryptography algorithm, decentralization and consensus process are the basis of blockchain architecture. The consensus process is considered to be the most important component of blockchain, which is also considered as the soul of blockchain innovation. The process of consensus substantially impacts the trust level among the nodes of the entire system and also measures the confidence level of users on the system [13]. The consensus process is actually a collection of methods which help stakeholders to come up with a mutual understanding. These methods

are collectively known as 'consensus mechanism" Few are given below:

i) Proof of Work

PoW is a mechanism used by the "Consensus Layer" of bit coin, which claims workload. Its immediate task is to evaluate a unique hash value known as "mining", which is a hash of block to meet required criteria. Its starting "n" bits have always been '0s'. The number of 0's tends to increase computation complexity. The co mputation

depends greatly on the hash speed of the device t o take a correct Hash of Block which needs a lot of computations.

Whenever a node gives the correct Block Hash v alue, it implies that the above node has experienc ed several trial computations since finding a correct hash is really an event of probability.

ii) Proof of Stake

It is similar to the equity voting system in which decision making powers increases with the increase in shares.

iii) Delegated Proof of Stake

Delegate proof of stake is an election qualification in addition to proof of stake. It is like the board of directors which are elected by the participants. The elected board of directors may exercise their privileges. Members having the right to vote are selected by the electoral process instead of just the quantity of coins.

Comparison b/w Proof of Stake & Proof of Work

Proof of Work is an election algorithm which is very efficient in preventing malicious attacks, but its major issue is consumption of resources whereas in case of Proof of Stake, there is no problem of resources [13].

Selection of Proof of Stake and Delegated Proof of Stake

In Proof of Stake, all nodes have to participate in elections [4]. Greater the number of nodes slower will be the efficiency and greater will be the pressure on network. Delegated Proof of Stake provides the concept that Proof of Stake nodes select some nodes among themselves through voting to give these nodes a decision power & then only these selected nodes participate for the decision instead of all nodes in the network. This process significantly improves the effectiveness of election. Thus, Delegated Proof of Stake minimizes the pressure on network & increases the efficiency by minimizing the number of nodes [15]. In simple words we can say it as a divide-and-conquer approach. Divide all nodes in two categories: the leaders and the followers. The leader nodes are decision makers; which are selected among all the nodes on the network. Whereas, rest of the nodes are followers; which are decision followers. By using this mechanism pressure on the network will get reduced without increase in computing resources [16].

4. Proposed Solution

To overcome this problem of transparency & security we propose the following ideas.

i) **Voting Distribution:** Vote is distributed to randomly selected peers.

ii) **Distributed Tally:** Vote Tallying is distributed to all peers which is then verified and corrected.

A. The Voting Process

Our proposed design has five stages which require off-chain and on-chain computations.

1) Voting Stage

Client application is used to create & submit the ballots of voters on blockchain during voting stage; which is then validated & recorded on ledger if valid.

2) **Ballot Verification Stage**

During ballot verification stage two way verification of ballots is performed and ballot will be decrypted and need to be verified by the peers whose HEPK. In valid ballot will be reported to blockchain and then verified by the smart contract. It helps to check the vote is result of dishonest voting or dishonest report. In case dishonest voting replacement of ballot is required.

If replacement of ballot is required proceed to revoting stage

Else move to 4th tally distribution stage

3) **Revoting Stage**

Peer has two choices for the ballot with status of replacement. Either to reject replacement & exclude it from voting process or to have it revote with a fresh ballot & encrypt it through the HEPK of an honest peer. In single transaction all substituted pairs are then broadcasted. Choices in the replaced ballot will be different one.

If there is not any new ballot... move to tally distribution stage.

Else repeat previous stage & verify new ballots.

4) Tally Distribution Stage

All ballots with status "honest" are tallied in a distributed manner. Result of every sing tally is published to blockchain. Using the homomorphic encryption property result of each tally is verified by smart contracts. In case of identification of dishonest tally, peer will be declared as dishonest.

As, a result revoting stage is repeated unless all tallies are identified as honest.
If peer fails to perform the assigned tally it can be declared as dishonest and the counting will repudiate its entire votes. It is expected from "honest tally" to issue its result in given time.
If there is not a single invalid tally, move to stage 5 in case all tallies have submitted their result.
Else keep repeating revoting stage

5) Aggregation Stage

Finally, smart contract will aggregate the results of all tallies to be published on chain; which results in ending of voting rules. Voting results will be available to all peers to view from the ledger; they can also look & verify the whole process.

5. Implementation

To implement the design, a system can be executed on Hyperledger Fabric.. It helps in creating a consortium blockchain network having permission controls and transaction consensus. Implementation of the design has two parts:

(i) Client
(ii) Smart Contract.

The flow of working is elaborated in Figure 3. Voting operations are held by clients that are conducted by each voters & voting logic which requires collaboration and consensus between all participants are maintained by smart contracts. The software programs enforced by smart contracts [17] are written into the blockchain and are immutable. Implementation details are elaborated as given below:

a) Smart Contract Determinism:
Smart contract determinism is the first challenge that needs to be resolved. In order to guarantee c onsensus in every phase of voting, verification & tally, the entire voting flow is carried out by smart contracts. The behavior of smart contracts should be deterministic as it is executed in all peers within the network. All non-voting operations e.g generation of key are carried out in client side.

b) Beginning & Finishing of Voting
Beginning and finishing time of voting is an important issue which needs to be addressed. Synchronization of peers is complex problem because global time does not exist in blockchain.

We need to set the starting time for global voting correctly for each stage, as system will execute automatically when time started.The message "Voting Begin" is presented by the promote r of the vote and ensures that it is registered on the blockchain. P eers check on their ledger this "Voting Begin" message to begin the vote. To synchronize all voters, we used a timeout window. For the development of a distributed timer, the following method s are used:

Timer with a global timeout setting will be initialized by each client.

(i) Special transaction is invoked by the client when local time expires.
(ii) Transaction requests are received by the smart contracts.
(iii) "Time Out" event will be broadcasted to all clients when its threshold value is achieved.
(iv) "Time Out" event is received by all clients.

c) Voting Flow

Using the proposed design as discussed above the voting flow is based on five stage which are implemented as follows:

1. **Voting:** "Vote" transaction is invoked by the client and ballots are stored on the ledgers accordingly.
2. **Verification:** Ballots are verified by each client; who get a "report" transaction of invalid ballots if any. Signatures and the report is verified by the smart contract which then blacklists the voter or reporter.
3. **Revoting:** "Revote" transaction is invoked by each client with new ballots; which will alter the ballots encrypted by blacklisted hepkid. Validation is again checked by the smart contract & stores it on ledger.
4. **Tally:** "Tally" transaction is invoked by each client with the tally results. Signatures are verified by the smart contract to store the tally result on ledger.
5. **Aggregation:** All the tally results are aggregated by smart contracts which then store the finalized results on ledgers. In case of dishonest behavior "Revoting" stage could be executed.

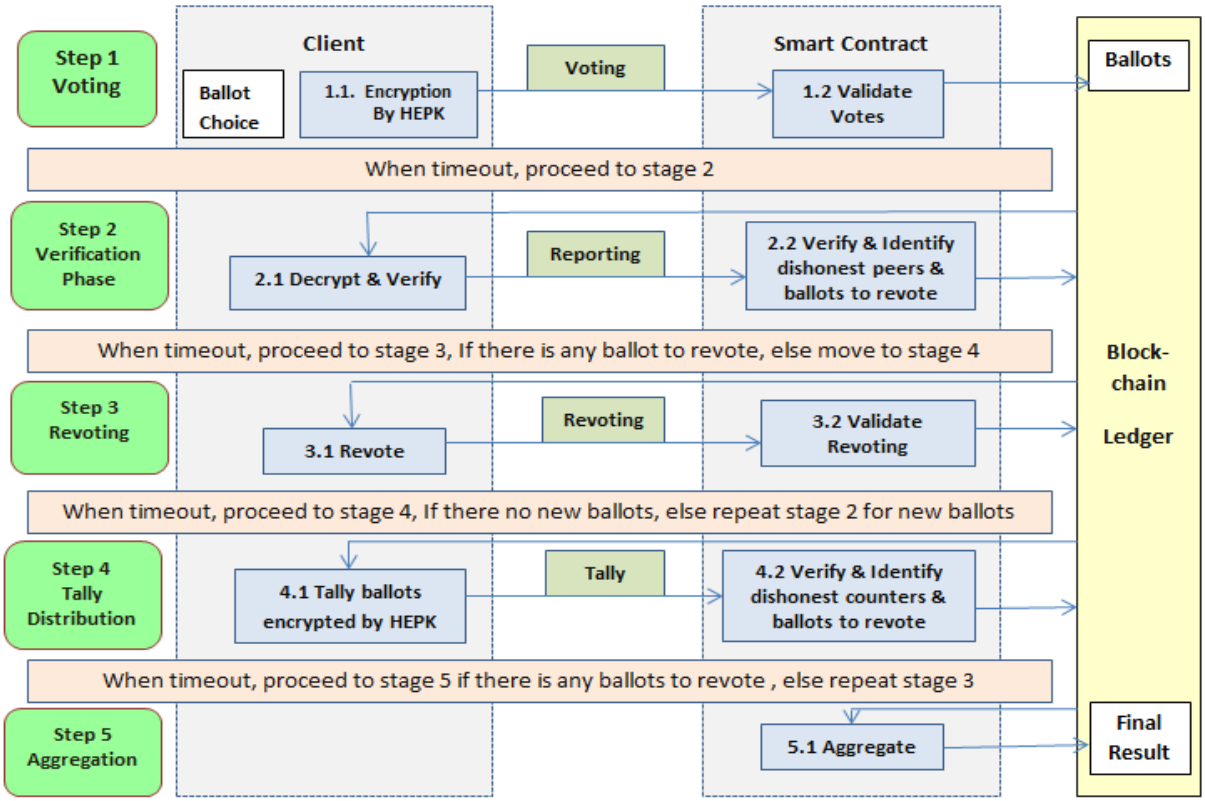

Fig. 3 Communicational Flow of the system

6. Conclusion

Public Elections are the best way to elect the government in democracy. Thus, it is the utmost responsibility of the state to organize non-fraudulent elections. The Estonian voting system is one of the leading electronic voting systems which is still not perfect & need to improve its security & privacy features. Keeping in focus the privacy & transparency concerns this paper
presented a blockchain based decentralized electronic voting system for elections on large scale. The significant features of the proposed system are data integrity & transparency. Blockchain uses encryption & hashing to ensure the security of each vote. The scalability & verifiability in proposed system make the voting process fully secured and reliable.

Refrences

[1] "Final report: study on eGovernment and the reduction of administrative burden (SMART 2012/0061)",2014,[Online]. Available:https://ec.europa.eu/digital-singlemarket/en/news/finalreport-study-egovernment-and-reduction-administrative-burdensmart- 20120061.

[2] F. Hao and P.Y.A. Ryan, Real-World Electronic Voting: Design, Analysis and Deployment, CRC Press, pp. 143-170, 2017.

[3] N. Braun, S. F. Chancellery, and B. West. "E-Voting: Switzerland's projects and their legal framework–In a European context", Electronic Voting in Europe: Technology, Law, Politics and Society. Gesellschaft für Informatik, Bonn, pp.43-52, 2004.

[4] Estonian National Electoral Committee “E-voting System”, 2010. [Online]. Available: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf.

[5] P. McCorry, S.F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy", International Conference on Financial Cryptography and Data Security. Springer, Cham, pp. 357-375, 2017.

[6] https://followmyvote.com

[7] https://www.strawpoll.me

[8] Y. Takabatake, D. Kotani, and Y. Okabe, “An anonymous distributed electronic voting system using Zerocoin“, IEICE Technical Report, pp. 127-131, 2016.

[9] Nakamoto, S, “Bitcoin: a peer-to-peer electronic cash system,” Consulted, vol.1, 2008, pp.2012, doi:10.1126/science.1079329.

[10] Shi, E., & Shi, E., “FruitChains: A Fair Blockchain. ACM Symposium on Principles of Distributed Computing,”

ACM, July2017, pp.315-324, doi:10.1145/3087801.3087809.
[11] Yonatan Sompolinsky and Aviv Zohar, "Secure high-rate transaction processing in bitcoin," In Financial Cryptography and Data Security, Springer, vol. 8975, July 2015, pp.507–527, doi:10.1007/978-3-662- 47854-7_32.
[12] Lamport L. Byzantizing Paxos by Refinement, "Distributed Computing," Springer Berlin Heidelberg, vol. 6950, 2011, pp.211- 22
[13] Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar, "Optimal selfish mining strategies in bitcoin," In Financial Crypto, vol.16, 2016, pp 515-532, doi:10.1007/978-3-662-54970-4_30.
[14] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P., "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," IEEE International Conference on Pervasive Computing and Communications Workshops. IEEE, May 2017, doi: 10.1109/PERCOMW.2017.7917634.
[15] Juan Garay, Aggelos Kiayias, and Nikos Leonardos, "The bitcoin backbone protocol: Analysis and applications," In Advances in Cryptology-EUROCRYPT 2015, Springer, vol.9057, 2015, pp.281–310, doi:10.1007/978-3-662-46803-6_10.
[16] Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar, "Inclusive block chain protocols," In Financial Crypto, vol.8975, 2015, pp 528- 547, doi:10.1007/978-3-662-47854-7_33.
[17] C.D. Clack, V.A. Bakshi, L. Braine, Smart contract templates: foundations design landscape and research directions, Mar 2017.