Securing IoT with Blockchain-Based System for Attendance Management

Priyanka Dongre[1], Dr. Pushpneel Verma[2]

[1]*Department of Computer Science and Engineering, Bhagwant University, Ajmer, Rajasthan, India*
[2]*Department of Computer Science and Engineering, Bhagwant University, Ajmer, Rajasthan, India*

Abstract: In every organization, managing the attendance of personal is an important task. Student attendance management is a critical study aspect in academic institutes. In the initial era of education, student attendance was maintained using paper records. It has slowly advanced over a few decades. Many educational organizations use smart-card or RFID-based cards, biometric devices such as fingerprint scanners, face recognition, etc., for recording student attendance. The use of such technologies has its advantages and disadvantages. Recently Internet of Things and Blockchain has gained the attention of many researchers. Researchers are trying to use these technologies to build several applications, including Smart Home Systems, Supply Chain Management, Electronic Healthcare record management, etc. However, an IoT network has constraints on power consumption, processing power, and security of end devices in the network. On the other hand, a few issues associated with blockchain are storage limitation, data privacy, consent revocation, energy consumption, scalability, and performance. In this paper, an Blockchain-Based integrated with Internet of Things (IoT) Data Sharing System for student attendance management is proposed. The paper also addresses the issues of authentication and access control. We introduce a multifaceted authentication system for user device substantiation, PKI-RSA-based blockchain implementation for data sharing, and a rule-based access control scheme to access the blockchain data. The predominant implementation details of the proposed system are explained in this paper.

Keywords: **Blockchain, Internet of Things, Attendance Management, User Authentication, Data Sharing**

1. Introduction

Over the years, Information Technology has changed several areas in educational systems. Monitoring students and managing student data are some of the domains. Attendance of students for classes and labs is a critical aspect of their learning activities. Marking student attendance by calling their names or asking students to sign on a paper was more common in the early days of education. However, these methods were more time-consuming and can be easily tampered. With the introduction of computers, the Internet, wireless sensor networks, the traditional attendance management systems have changed a lot. The use of RFID-based smart cards and biometric technologies such as fingerprint scanning, iris, barcode, face recognition, etc., has been employed in such systems.

An IoT network is made up of a combination of associated objects or (intelligent) 'things' that are usually connected via the Information highway. IoT devices are often assigned unique IP addresses to help identify the devices on the network. These devices have the potential to interact with one another and can often be remotely managed. They can also gather or sense data from their nearby surroundings and then process them into meaningful information used by the system or its users. The homogenization of the IoT into every day activities has been expanding fast and is becoming more popular in various fields and sectors, including healthcare, industrial automation, and manufacturing. Smart

IoT devices can unite smoothly with their surrounding environment to provide access to different types of information and services in well timed.

Extensive work has been introduced in blockchains for the management of digital cryptocurrencies such as Bitcoin. Blockchains technology playes a major role behind these currencies. The distributed and decentralized nature of blockchains improves the integrity and security of financial transfers. Regardless of the type, permissionless or permissioned, basic concepts in blockchains remain unchanged. The latter requires authentication, network device identification, enrollment by the central authority thus preventing them to join the blockchain network directly, unlike a permissionless blockchain. Blockchain work by storing all transactions that occur on a network in a hash-based structure referred to as a *block*. A transaction can refer to a financial transfer, change of ownership of an asset, such as cars or bonds, or information exchange between two individual participants over the network. Each block of the blockchain transactions contains the hash value of the prior block. The ledger then obtained can be stored in a database or flat-file accordingly. Blockchain is an emerging and promising technology that offers peer-to-peer communication, data security, integrity and authentication.

2. Literature Survey

There have been several proposed approaches for automated attendance systems for recording the appearance of the working persons. Attendance system like Biometric-based face recognition, fingerprint, and even iris-based attendance systems are available in the market. Similarly, device-based attendance systems like Smart Cards and RFID-based attendance systems are available in the market as products. These various attendance recording techniques are acceptable to various different scenarios and are practically deployed in offices, institutions, laboratories, factories, etc.

Unfortunately, all of such techniques are applied only within defined places and should been owned [1].

Rjeib, H. D., et al., (2018) has presented an information system for recording attendance that uses RFID and web-based application for the academic society. The system not only manages the attendance of the student but also provides various information systems for the staff and students. The method is time-competent and minimise the manual attempts required to record attendance data, and is less power-consuming [2].

In [8] and [9], By using RFID cards/technology the attendance systems are developed. The recording of employee attendance is done by RFID with a card attached to it in order to save the attendance data of the employee to the database. Meanwhile, in [10], face detection and recognition algorithms are bult by the system. Attendance is recorded by capturing a person's image with a camera, and with several processing methods, in order to store the attendance in the database. In [11], the authors use the methods of face recognition but by using different algorithms to store the attendance. In [12], marking of attendance is done by the system by using a smartphone thereby making possible for the employee employee to access the online system from everywhere, and the data is recorded in the MySQL database. Various attendance system have been developed like thumb impression [13], where the recording of attendance is done by using fingerprint and the recorded data are later saved into the database.[3].

Ardina, H., & Nugraha, I. G. B. B. (2019) developed A Blockchain-based employee attendance system to manage attendance transactions so that the stored data can be maintained for its integrity and reliability. Blockchain network with consensus mechanism , only permitted parties enter the blockchain network and they can delete, change or even renew data. All the participants in the network will be known if any changes in the data on the blockchain is been done. If a piece of information has ever experienced any unauthorized changes, the conventional databases do not have special features to check it. The blockchain based system does not allow any administrator

permission to edit or delete data. Someone who inserts an information record on the blockchain will not be able to deny that he is doing the activity. The entire database and history is accessible to each party on the blockchain. The employee attendance system based on blockchain always require to provide a database that keeps its integrity and reliability and tamper-proof [3].

Tu, J., Duan, et al. (2018) presented a blockchain architecture and implementation of the attendance management system. The system makes use of a MAC address to locate the attendance. This can be risky since one could report in instead of other individuals. So, the better option is to take more rigorous ways such as face identification or fingerprint recognition or to reduce this risk. Further, algorithms like Proof of Work used in the attendance management is slow and energy-consuming[4].

A. Challenges associated with IoT networks [7]:

IoT networks typically utilize constrained devices that use low-bandwidth standards and must maintain an open, secured communication channel with more powerful devices, such as Smartphones or gateways. Guaranteeing this channel's security requires optimal cryptography algorithms and proper key-management systems, and security protocols that connect all these devices through the Internet [11].

Authentication: Authentication can be challenging to achieve in IoT due to the nature of its' constrained devices and their heterogeneity. Authentication is identity establishment between communicating parties [6]. IoT devices should be able to verify each others' identities to guarantee that an object is, in fact, who it is claiming to be. In IoT networks, authentication usually occurs between an IoT device and a central authority.

Authorization: Authorization is ensuring that a particular device has appropriate privileges to access a resource or perform a specific task.

Identity Management: Different devices are connected to IoT, and the number of these devices is increasing. IoT devices can be impersonated maliciously by adversaries to perform malicious tasks. Hence, the identities of IoT devices on the network require validation.

Privacy: With the increasing acceptance of IoT around us, the amount of data that is generated by IoT devices is enormous. IoT devices can transmit information that categorizes their users' behaviors, preferences, and patterns. In most cases, collected information can be analyzed and used for profiling or even marketing. Therefore, privacy concerns in IoT have been raised.

Confidentiality: All kinds of data travel through the IoT network. Some of that data is confidential. In the context of health care, for example, almost every packet traveling through an IoT network contains patients' personal information that allows physicians to check their patients' medical status remotely. Such data should be protected from interception. It is of equal importance as well to protect the data stored on these devices.

Integrity: Integrity refers to the assurance that information has not been modified by unintended parties. Preserving messages integrity' is crucial in many IoT applications, such as patients' medical information. Therefore, confidential data should be immune to change throughout the transmission process.

Availability: Data in IoT should be available for access by authorized users at all times, whenever they require it. Intrusion detection and protection against DoS and DDoS attacks are crucial to guarantee a smooth flow of data.

Availability: Data in IoT should be available for access by authorized users at all times, whenever they require it. Intrusion detection and protection against DoS and DDoS attacks are crucial to guarantee a smooth flow of data.

B. Challenges associated with Blockchain [6]:

Although blockchain was gaining more attention and used to provide more data security in several attacks, it has a few challenges in practical implementation in a small setup.

Performance –The blockchain performs several task such as consensus mechanism, traditional database prosessing and redundancy checking due to which the processing speed of blockchain can lead to slow performance.

Scalability – As the blockchain network grows larger, requirements of large storage space, computational power and bandwidth arises. Hence the scalability of blockchain is a significant issue for a public blockchain.
Privacy – All transactions in the blockchain are trasparent for each public key. However, it can preserve a certain amount of privacy via the public key [24]. The publically accessible nature of blockchain makes that data accessible to every node on the network.
Energy Consumption – The process of creating blocks of a public blockchain consumes large amount of electricity and computational power. Therefore, the computational power is used for this process only.

3. Proposed System

The below figure illustrates the proposed system architecture. The system's major components include Blockchain, IoT network, Webserver, and End-users known as Nodes that transfer data to the Blockchain.

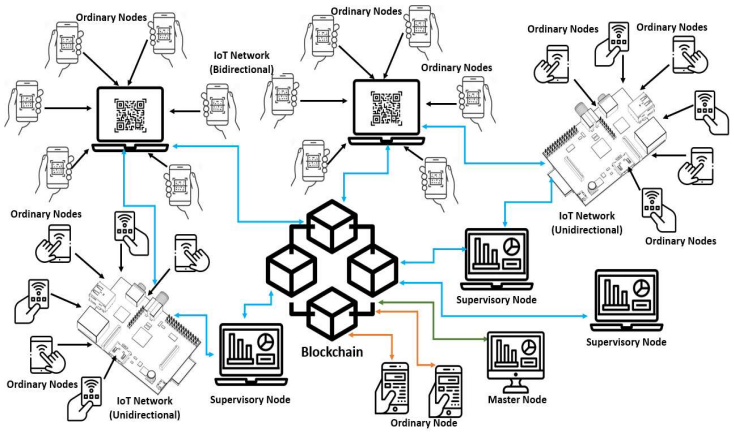

Figure 1. System Architecture

IoT networks can contain several devices such as mobile phones, RFID card readers, RFID Tag, etc. Blockchain stores all the data transactions through a webserver. The nodes are the users who use the Blockchain and IoT network for data sharing and communication through a web server. The nodes are classified as ordinary nodes, supervisory nodes, and master nodes. The master node is responsible for managing the entire blockchain network. The master node can add or remove the supervisory nodes and decides how many IoT networks one supervisory node can manage. In addition, the master node can add or remove the supervisory nodes. Also, the master node can remove or assign IoT networks to a supervisory node.

3.1 Implementation

This section describes the high-level implementation of the proposed system.

3.1.1 Use Case:

In this section, the use case of the proposed lightweight blockchain framework of IoT networks is explained. For example, Students, Teachers, and the Dean are involved in using the system in a university. These users can be treated as nodes that use end devices in the IoT network to request the required service to a web server. Here the roles of these nodes are defined to request to execute a transaction in the Blockchain.

3.1.2 IoT Network:

The IoT networks are of two types viz Unidirectional IoT network and Bidirectional IoT network. The unidirectional IoT network generates one-way traffic, whereas the Bidirectional IoT network generates two-way traffic. Each device connected to an IoT network can initiate data write operation only when the supervisory node enables the data

write operation for ordinary nodes. The ordinary node connected to a unidirectional IoT network can initiate the data write transaction through the supervisory node. In a unidirectional IoT network, the ordinary nodes are connected to Raspberry Pi, which collects the data from the devices connected to the network. The supervisory node acts as an interface between the private Blockchain and IoT network devices. The supervisory node allows only authenticated ordinary nodes to connect to the Blockchain to initiate data write transactions. Ordinary nodes such as smartphones can only initiate the data read transaction from the Blockchain through a webserver or supervisory node.

3.1.3 Unidirectional IoT network:

The unidirectional IoT network is built around a Raspberry Pi Gateway and contains an RFID Reader, an RFID tag, Finger Print Scanner, etc. These devices have the low computing power and hence cannot use the blockchain directly. The Raspberry Pi Gateway acts as the interface between the supervisory node and these IoT devices. When the supervisory node initiates the data record session for the unidirectional IoT network, only the data transactions are allowed from the devices connected in the unidirectional network. Therefore, each transaction initiated by such devices is stored on Raspberry Pi Gateway and stored on the Blockchain through the supervisory node.

3.1.4 Bidirectional IoT network:

The bidirectional network contains devices that can send and receive data, such as smartphones, laptops, and computers. The ordinary nodes in this network can initiate the data write transaction when the supervisory node initiates the session to ordinary nodes. The supervisory node creates and displays the QR code, which is then scanned by the ordinary node to initiate the transaction that is added to the Blockchain. The ordinary nodes in this IoT network can read the blockchain data through the Webserver by initiating the HTTP request.

3.2 Blockchain:

Blockchain is an integral part of the system, and it is an immutable database that stores all the transactions in blocks. For every session initiated by the supervisory nodes, all the data transactions done by ordinary nodes are stored on the Blockchain. Each transaction in the block contains the timestamp, mac_id, user data, previous block hash code, and next block hash code. All the data stored in the blockchain is referenced as a linked list where you can identify the previous and next blocks easily using the previous hash and next hash code. The Web server communicates with the Blockchain using the HTTP protocol. The supervisory nodes and the master node can access the blockchain through a web server. The ordinary nodes on a bidirectional IoT network can access the Blockchain through the Webserver. The ordinary nodes in a unidirectional can not access the Blockchain.

3.4 End Devices:

The system contains several end devices, including smartphones, laptops, RFI cards, Fingerprint scanners, computers, etc. Each of these devices is part of a unidirectional and bidirectional IoT network.

3.5 End Users:

The users of the system are classified as Ordinary Node, Supervisory Node, and Master Node. Each of these users has specific access rights defined according to a policy.

4. Results and Discussion

This section discusses the results of user authentication, data storage, and data access schemes implemented.

This section discusses the results of user authentication, data storage, and data access schemes implemented.

4.1 User Authentication

A multi-factor authentication scheme is implemented in this system. The Webserver executes the user registration smart contract when the user registers on the system. For each user, a unique Private Key is created at the time of user registration, and the mac address of the user, along with

the user data, is stored on the Blockchain. When the user wants to connect to the system, the webserver executes a user authentication smart contract to get the encrypted list of permitted devices' mac IDs. Thus, a two-stage user authentication protocol is designed to authenticate the users on the network. First, the user sends a request to the webserver to log in using the private key.

Second, the webserver executes the user authentication smart contract to verify the user authenticity and gets the list of permitted devices. Once the private key and device mac id of the user match, then the device is authenticated and connected to the blockchain. Upon successful authentication, the webserver writes user session block on the blockchain, and the user can perform the data transactions according to its role. First, the data block is generation is done and then appended to the Blockchain. The data block contains the unique hash code, timestamp, user data, encoded mac id, and previous hash code. The previous hash code is the unique value of the previous block in the Blockchain. This can be seen in the below figure.

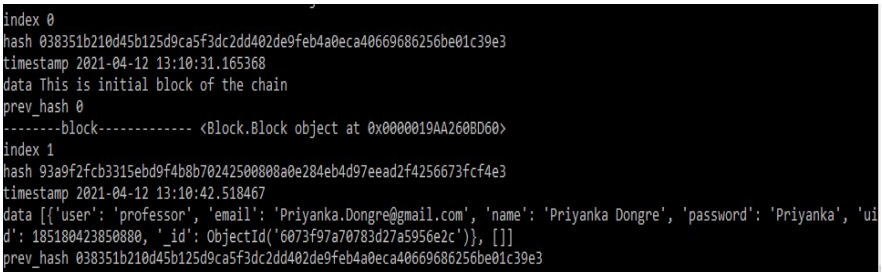

Figure 2: Data Block added to Blockchain upon Successful User Authentication

4.2 Data Storage

The data storage is done in several blocks on the blockchain. For each transaction, a data structure is defined, and the data transaction is stored on the blockchain when the webserver initiates the smart contract for each of the nodes in the system. The smart contract create_generate_genesisblock() creates the genesis block. Once the genesis block is created, each of the data transactions generated by users is added to the blockchain when the user performs the transaction. The figure below shows the creation of the Genesis block.

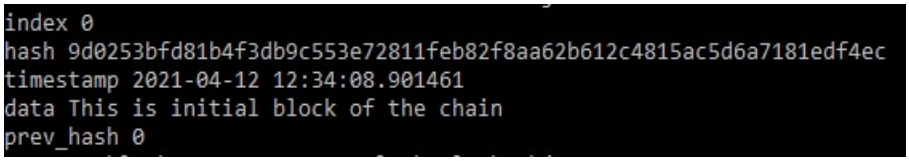

Figure 3: Genises Block

Table 1. shows the time taken to generate the block in seconds.

Table 1: Time taken for block generation

Block Name	Time Taken
Genesis	0.000999212
Registration	0.016958952
New Subject Creation	0.016954184
QR Code Generation	0.016955614
Mark Attendance	0.007982254

Below graph shows several blocks generation time in the proposed system.

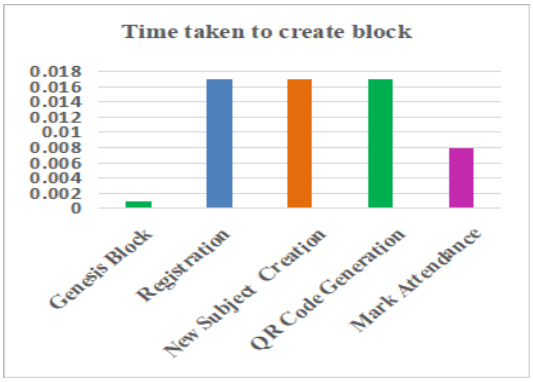

Figure 4: Time taken to generate the blocks

4.3 Data Access Control:

Role-based data access control is implemented in this system. As discussed in previous sections, each system user is assigned a specific role. The system users in this work are also known as nodes. Whenever the user wants to write data or read data transactions first, the user has to connect to the webserver. The web server authenticates and verifies the user's role by executing the smart contract and allows the nodes to write or read data transactions to the Blockchain. As the nodes in unidirectional nodes have less computing power hence the ordinary nodes on the unidirectional networks are not directly allowed to access the blockchain, whereas the ordinary node on a bidirectional network is allowed to initiate the read operation. When the ordinary node on a bidirectional IoT network sends a request to the webserver, the webserver executes the smart contract to read the blockchain data. Supervisory nodes can write and read the blockchain. Supervisory nodes are also responsible for writing the data on blockchain on behalf of ordinary nodes. Master nodes are allowed to read and write the data in the blockchain. For each read and write request from the supervisory node master node, the webserver executes the smart contract based on the roles, and the user can perform the operations as per the policy.

5. Comparative Analysis

This comparative analysis describes the comparison of the proposed system with existing systems. Here first, we compare the proposed approach with traditional semi-automated systems on a few generic parameters, then we give the comparison of methods that employ blockchain and IoT for the attendance management, and finally, we compare the blockchain transaction or block generation time taken by the purely blockchain-based systems and proposed system. As shown in Table 2, the traditional methods are not user-friendly, the data accuracy is low, they are more vulnerable, having slow speed, and are time-consuming as compared to the proposed system.

Table 2: Comparison between the traditional Blockchain system and proposed Blockchain system

Domain	Time Consumtion	Speed	System Security	Resources (Documents)	Data Accuracy	Adaptability
Traditional Blockchain System	> 5 min	Slow	More Vulnerable	More paperwork	Low	No
Proposed Blockchain System	< 1 min	High	Validated individuals only	Only electronic records	High	Yes

Table 3. describes the comparison of the available systems implemented using blockchain for attendance management. There are very few systems available in the literature that use blockchain for attendance management, and among all the available methods, none of the designs have implemented them for IoT networks.

Table 3: Comparison between existing blockchain implementations of AMS

Author	Blockchain	IoT
Hasna Ardina [3]	Yes	No
Jingyao Tu [4]	Yes	No
Ajayvikram Chauhan [5]	Yes	No
Proposed	Yes	No

As shown in Table 4, there are a few popular systems build around the blockchain even takes more time to generate the data block as compared to the proposed approach.

Table 4: Block-Time generation comparison between existing blockchain implementations [6]

Blockchain Name	**Block-Time**
blockchain AMS [4]	600 Secs
Bitcoin[15]	10 mins
AltCoins [31]	2.5 mins
Dogecoin [32]	60 secs
Ethereum [14]	12 secs
MultiChain [33]	Configurable
Hyperledger (Fabric) [34]	Unknown
Steem [35]	3 secs
Lisk [36]	10 secs
Proposed	<1 Secs

6. Conclusion

In this paper, we have discussed some of the challenges of IoT and Blockchain implementations and tried to address a few of them, such as user authentication, data storage, data sharing, and access control. We have successfully implemented an Attendance Management System using Blockchain and IoT. The system can work with unidirectional and bidirectional IoT networks, and the data is stored on Blockchain, providing more security to the data generated on the IoT network. Furthermore, we have introduced a multi-factor authentication scheme and a rule-based access control scheme to access the data. The results show that the proposed system takes less than 1 second time to generate the data block. Compared to the traditional semi-automated attendance management system, the proposed approach is more accurate, secure, and user-friendly. Although there is less work available on the use of IoT and Blockchain for attendance management, we believe that this work will motivate researchers to experiment around the use case.

7. References

[1] Navin, K., Shanthini, A., & Krishnan, M. M. (2017, August). A mobile based smart attendance system framework for tracking field personals using a novel QR code based technique. In 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon) (pp. 1540-1543). IEEE.

[2] Rjeib, H. D., Ali, N. S., Al Farawn, A., Al-Sadawi, B., & Alsharqi, H. (2018). Attendance and information system using RFID and web-based application for academic sector. International Journal of Advanced Computer Science and Applications, 9(1).

[3] Ardina, H., & Nugraha, I. G. B. B. (2019, November). Design of A Blockchain-based Employee Attendance System. In 2019 International Conference on ICT for Smart Society (ICISS) (Vol. 7, pp. 1-4). IEEE.

[4] Tu, J., Duan, Z., Tian, C., Zhang, N., & Wu, Y. (2018, November). A Blockchain Implementation of an Attendance Management System. In International Workshop on Structured Object-Oriented Formal Language and Method (pp. 169-182). Springer, Cham.

[5] Chauhan, A., Savner, G., Venkatesh, P., Patil, V., & Wu, W. (2020, August). A Blockchain-Based Tracking System. In 2020 IEEE International Conference on Service Oriented Systems Engineering (SOSE) (pp. 111-115). IEEE.

[6] Thwin, T. T., & Vasupongayya, S. (2018, August). Blockchain based secret-data sharing model for personal health record system. In 2018 5th International Conference on Advanced Informatics: Concept Theory and Applications (ICAICTA) (pp. 196-201). IEEE.

[7] Asiri, S. (2018). A Blockchain-Based IoT Trsust Model (Doctoral dissertation, Master's Thesis, Ryerson University, Toronto, ON, Canada).

[8] T.S. Lim, S.C. Sim and M.M. Mansor, " RFID Based Attendance System", IEEE Symposium on Industrial Electronics and Applications (ISIEA), Kuala Lumpur, Malaysia, 2009.

[9] M. Kassim, H. Mazlan, N. Zaini and M.K. Salleh, "Web-based Student Attendance System using RFID Technology", IEEE Control Control and and System System Graduate Graduate Research Research Colloquium Colloquium (ICSGRC), 2012.

[10] S. Chintalapti and M.V. Raghunad, "Automated Attendance Management System Based On Face Recognition Algorithms', IEEE International Conference on Computational Intelligence and Computing Research, 2013.

[11] P. Wagh, J. Chaudhari, R. Thakare and S. Patil, "Attendance System based on Face Recognition using Eigen face and peA Algorithms," International Conference on Green Computing and Internet of Things (ICGCloT), 2015.

[12] M.M. Islam, M.K. Hasan, M.M. Billah, and M.M. Uddin, "Development of Smartphone-based Student Attendance System," IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, 2017.

[13] J.A. Badejo, C.C. Eke, S.I. Popoola, T.O. Odu, and A.A. Atareyo, "Integrating Automated Fingerprint-based Attendance into a University Portal System," International Conference on Computational Science and Computational Intelligence, 2017.

[14]ethereum, "Ethereum Blockchain APP Platform." [Online]. Available: https://www.ethereum.org/. [Accessed: 27-May-
2018].

[15] bitcoin, "Bitcoin - Open source P2P money." [Online]. Available: https://bitcoin.org/en/. [Accessed: 27-May-2018].

[16] Plasma, "Altcoin," Altcoin.io. [Online]. Available: https://altcoin.io/.[Accessed:31-May-2018].

[17] B. Markus and J. Palmer, "Dogecoin." [Online]. Available: http://dogecoin.com/. [Accessed: 31-May-2018].

[18] multichain, "MultiChain | Open source blockchain platform." [Online]. Available: https://www.multichain.com/. [Accessed:
31-May-2018].

[19] Hyperledger, "Hyperledger-fabricdocs Master documentation." [Online].Available:http://hyperledgerfabric.readthedocs.io/en/release/prereqs.html.[Accessed:12-Feb-2018].

[20] Valve, "Steem - blockchain-based social media platform." [Online]. Available: https://steem.io. [Accessed: 31-May- 2018].