An IOT Based Private Blockchain Framework for Attendance Management Using QR Code

Priyanka B. Dongre[1], Pushpneel Verma[2]
Bhagwant University, Ajmer, Rajasthan
{ priyankadongre90@gmail.com[1],pushpneelverma@gmail.com[2] }

Ph.D Scholar, Bhagwant University, Ajmer, Rajasthan[1], Associate Professor, Bhagwant University, Ajmer, Rajasthan[2]

Abstract. Blockchain and Internet of Things are considered as most disruptive technologies of the decade. Internet of Things has established its existence in several areas including manufacturing, smart home system to IT enabled Services on the other several use cases are available for blockchain mentioning its successful application in finances to supply change management, electronic health care record etc. Researchers are also trying to integrate blockchain and Internet of Things. This paper introduces the primary work carried to integrate blockchain and internet of things. To integrate blockchain and internet of things it is essential that all the participating devices work in an environment that allows them to communicate and initiate transactions thereby allowing the successful creation of block and blockchain.The major contribution of this paper includes development of a private blockchain that allows various users of system to perform their activities as per the rules or smart contracts defined while they are the part of blockchain. We have developed a private blockchain framework that utilizes a novel method to create the blocks and blockchain using SHA-256 algorithm, QR Codes and stores the information in blockchain at a particular timeframe. The proposed private blockchain framework is explained in terms of use case taken for marking attendance of students using mobile phones and teacher's laptop which participate in the blockchain creation. The rest of the paper is organized in five sections. Initially a short introduction of the proposed system is given then in second section related work is presented. Third section describes the proposed system architecture, implementation details are highlighted then in last section conclusion and directions to future work are given.

Keywords: Internet of things, blockchain, QR Code, student attendance.

1 Introduction

ICASISET 2020, May 16-17, Chennai, India
Copyright © 2021 EAI
DOI 10.4108/eai.16-5-2020.2303960

With the advent of technologies several attendance markings systems came into existence. There are systems that are successfully used in several organization including industries and academics that marks the attendance using biometrics or RFID smart cards. The biometric attendance systems marks attendance based on fingerprint patterns that are stored in database and use needs to mark his/her attendance using fingerprint on the biometric device. The RFID smart cards have unique identity which is recorded when user holds it in front of the reader and the attendance get marked. Several web-based framework and android based frameworks are used to for attendance marking. All of these systems have their own advantages and disadvantages.

Here in the proposed system we are trying to build our own private blockchain and integrate it with IOT network. The proposed private blockchain is built using python programming language and we do not use any proprietary or public blockchain frameworks like Ethereum, Hyperledger etc. The basic objective here is to implement a simple private blockchain and IOT framework that will allow creation of blockchain and will provide the easy to use features for the users. The attendance marking in this system will be done by scanning QR codes using students mobile. The section 3 describes the system architecture and section 4 describes the implementation details.

2 Literature Survey

The literature survey is organized into four sections where we discuss few introductory concepts and understanding of blockchain, its types and frameworks, Cryptographic functions, QR code and some of the similar works available in literature.

2.1 Blockchain, Types and Frameworks

At higher level Blockchain is considered as a mechanism to store the digital data in a certain way. The data may be in the form of text, images, files or transaction information containing transfer of Bitcoins between two accounts. This information is stored as a block in a linearly structured way as block after another block. Thus it becomes a chain of block and hence known as “blockchain” where block is a data storage unit and each block not only contains the transaction information / digital data but also contains the information about previous block and next block along with the timestamp when that block was created. The applications of blockchain are found in several areas including Finance, Logistic, Assets & Supply Chain Management, Health Care, Education, Government, Data Management etc.

There are three categories of blockchain. viz, permissioned blockchain, permission less blockchain, and consortium blockchain. The permissioned blockchain is also known as private decentralized blockchain on which an organization or an individual has the control and decides who can join that blockchain network and what kind of rights the user can have. This type of blockchain stores the data in encrypted form and works as per the concepts of blockchain. Permissioned blockchains are useful for the individual organizations to maintain the transparency in their business processes. There are several examples of permissioned blockchain including “Bankchain” etc.

In case of public blockchain, anyone can join the blockchain and has the rights to participate in the data generation and access the blockchain information in secure way. This is a completely decentralized blockchain which utilizes consensus mechanisms, proof of work, proof of stake, miners, mining etc. Bitcoin and Litecoin are quite popular examples of blockchains. Another type of blockchain is one which is created and controlled by a group of organizations or people. It does not have a central authority but the members in the group has certain roles and responsibilities according to which it is controlled and executed.

There are number of blockchain frameworks, that are coming up in the market. Mostly used blockchain frameworks include Bitcoin, Litecoin, Ethereum, Zcash, Dash, Ripple, Monero, Peercoin, MultiChain, Hyperledger etc. Ethereum and Hyperledger are most commonly used blockchain frameworks by researchers.

2.2 Crypto-graphic Functions:

To organize the data in blockchain it uses number of cryptographic techniques or functions called hash values. The data integrity and authenticity are maintained using these cryptographic hash values at various levels. Hash functions, Asymmetric key, hash pointer, merkle tree, digital signatures etc. are commonly used to organize the data block and information contained within the blocks. A hash function is typically a mathematical equation having properties that makes it useful for encryption. A hash function performs the task of mapping a unique fixed length key value of binary nature to an arbitrary length binary input. SHA-256 is one of the examples of such hash function. Asymmetric keys are the private and public keys which are generated for each block in the blockchain. The verification function and digital signature function utilizes these keys. More details on data organization in blockchain using cryptography can be found in [3].

2.3 QR code:

Quick response code abbreviated as QR code is an image organized in pixel matrix. It is attached to a device or equipment. It can be read by machine or device. The QR code contains the relevant information about that particular equipment or device to which it is attached. It contains several parameters like locator, identifier and tracker.

The Quick Response system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include product tracking, item identification, time tracking, document management, and general marketing.[2]

A QR code consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera, and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data is then extracted from patterns that are present in both horizontal and vertical components of the image.[2]

Fig. 1. QR code

2.4 Similar Woks:

Navin, K., Shanthini, A., & Krishnan, M. M. (2017, August) has proposed a framework to track field personal using QR based technique on mobile phones. In this framework two different mobile applications were used field personal and recipient clients. The QR code-based mechanism helps to identify the person and eliminate the false reporting. The authors also discussed the use case scenarios where the proposed framework can be applied [12].

Hermanto, N., & Baihaqi, W. M. (2018, November) implemented an online student attendance / presence marking system using QR code and IMEI numbers of mobile based on android platform. In this system the students can mark their attendance using mobile phones and reading the QR Code from lecturer's mobile phone at every meeting. Alternatively, the lecturer can display it through projector and students can read the QR code using mobile phones. In this system the IMEI number associated with each student mobile is used to validate the mobile phone owners [13].

Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2018, April) has addressed the problem of counterfeiting certificates using blockchain. The system helps to improve the credibility of paper-based certificates. The system stores the relevant data in by generating electronic files in the blockchain and generated a QR code that is associated with certificate to verify the authenticity of certificate. The QR code can be scanned using mobile phones to verify the authenticity [14].

Meng, Z., Morizumi, T., Miyata, S., & Kinoshita, H. (2018, July) has designed a scheme of copyright management system that combines blockchain, digital watermarking, QR code, Inter Planetary File System (IPFS) and perceptual hash functions. In this work authors used blockchain to securely store the watermark information. The order of creation of watermarks is authenticated using timestamp in blockchain. The perceptual hash functions generate a hash value based on the information of watermark [15].

Baralla, G., Pinna, A., & Corrias, G. (2019) proposed a system that allows the consumer to reconstruct the product history up to the origin in order to verify product health and quality by simple QR code scan. The blockchain chosen for this purpose is Hyperledger Sawtooth, issued with writing permissions and rules to guarantee access only to members recognized as legitimate participants in the process [16].

Benčić, F. M., Skočir, P., & Žarko, I. P. (2019) presented a system that describes the DL-Tags solution and includes a cost analysis of all implemented transactions on the Ethereum blockchain. The proposed solution provides evidence of the product's origin and its journey across the supply chain while preventing tag duplication and manipulation. It is among the first documented practical solutions using DLT and IoT for supply chain management, which is designed to be distributed ledger agnostic [17].

Tantidham, T., & Aung, Y. N. (2019, March) introduced an emergency service system for Home Service Providers that utilizes smart contracts on Ethereum blockchain to handle the access control of untrusted public services for IOT enable smart homes.

The testbed designed for Smart Home System includes, Raspberry Pi as an IoT Gateway to manage the sensor data of sensors equipped devices in Smart Home and data gathered from environmental sensors[19][20]. The second component of this system is a Miner deployed on Ethereum platform and third component is a Web Application for the users of smart home. In this system QR code is used as a passcode to control the access of staff and users or peers in the network [18].

3 System Architecture of Proposed System:

In today's attendance system we can observe the lacunas such in the part of authentication of the attendance which involves the trust factor and the digitalization is not their which means that the data can be tampered and the main focus of this project is to address these two major issues. Figure 1 shows the proposed smart attendance system using IoT and blockchain.

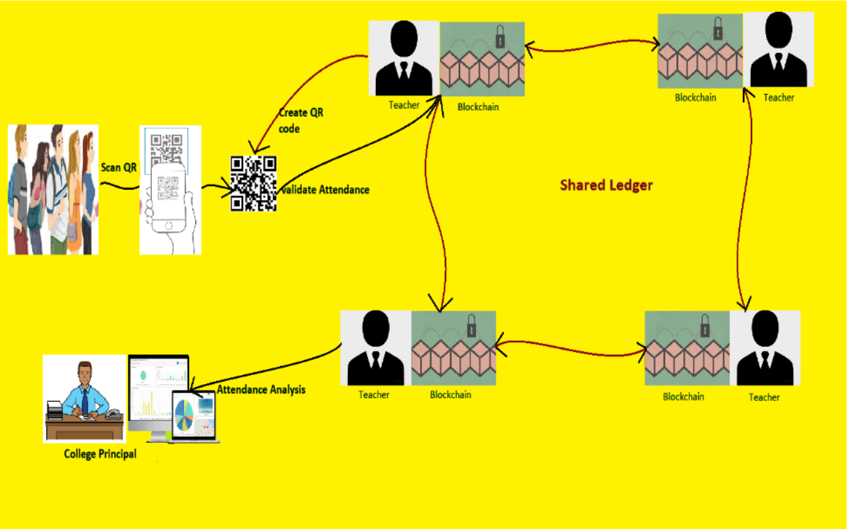


Fig. 2. Smart Attendance System Using IOT and Blockchain.

This Decentralized platform is mainly intended to be used by the various organization such as an engineering college or a university where we want to replace the obsolete attendance system with the novel one. Website will be main user interface where users can operate all the provided functionality. However, this web site will be only a part of a larger system. This project mainly focuses on the attendance management part in any organization and can be integrated with the other management parts of the system which handles all the data for any organization. Website will only be the interface for the user data and the execution of provided functionalities.

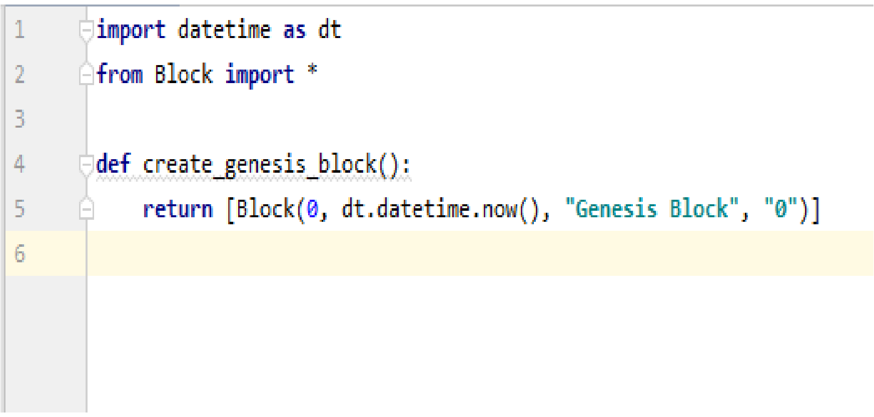
To use product, users are required to register through the web interface. All the user only related to that particular organization and have the unique identity in the organization can be the part of the system. The user will be provided with the account which he/she will use to mark the attendance as the student or if he/she is a teacher then he will generate daily QR code for the students to mark the attendance for a subject at particular time. Other user such as the dean of the department or the director of the college will have the view access to all these occurring scenarios and they will be able to analyze the data accordingly.

4 Implementation Details

In this section the implementation details are explained at high level. The programming languages used to implement the framework includes Python 3.7, HTML5, CSS, Java Script, jQuery. Flask and Bootstrap 4 is used as web application framework and mongodb is used to store the database.

4.1 Genesis Block:

The following code snippet shows the genesis block.



```
import datetime as dt
from Block import *

def create_genesis_block():
    return [Block(0, dt.datetime.now(), "Genesis Block", "0")]

```

Fig. 3. Genesis Block Code Snippet

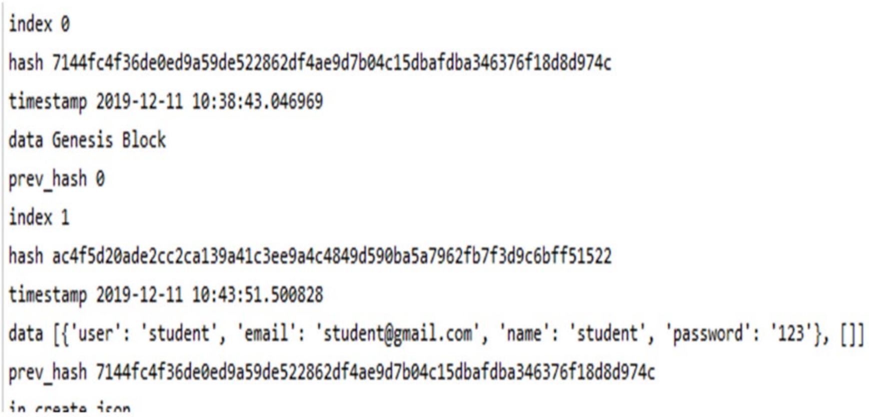
This block gets created when the code is executed for first time. As shown in figure 1.5 the genesis blocks get created and stored at index 0 in the blockchain. Later on, the other blocks are created as a full block or full node.

4.2 New User registration Block:

This block contains the information like type of user that means the user is student or professor or dean of the department, Email ID, name and password.

4.2.1 Data structure to store the registration data:

Registration {user: String,
Email: String,
Name: String,
Password: String
}



```
index 0
hash 7144fc4f36de0ed9a59de522862df4ae9d7b04c15dbafdba346376f18d8d974c
timestamp 2019-12-11 10:38:43.046969
data Genesis Block
prev_hash 0
index 1
hash ac4f5d20ade2cc2ca139a41c3ee9a4c4849d590ba5a7962fb7f3d9c6bff51522
timestamp 2019-12-11 10:43:51.500828
data [{'user': 'student', 'email': 'student@gmail.com', 'name': 'student', 'password': '123'}, []]
prev_hash 7144fc4f36de0ed9a59de522862df4ae9d7b04c15dbafdba346376f18d8d974c
in create json
```

Fig. 4. Registration block added in the blockchain after Genesis block

4.3 User Log in to the system

Upon successful registration the user is able to login into the system. As there are different roles for the users in the system the login in and logout actions are not captured as a block instead each user participates in the creation of several blocks according the roles.

All the users of the organization need to login to the system. To login into the system user device needs to be connected to the internet. After that user go to the web browser and insert the URL for the attendance system in the browser and choose the option for log in to the system. The user will then be redirected to the login page and they will insert the details such as the user-type, email id and password and click on login button to enter into the system.

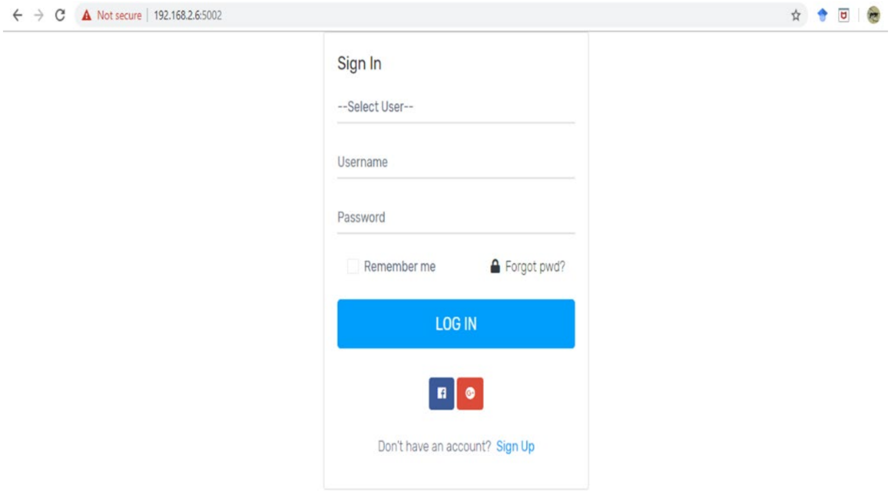


Fig. 5. Login page for user

4.4 New subject creation block:

The next step is to create subject and add it to the blockchain. The supervisory node i.e. professor has the rights to create the subject. This block contains the information like name of the subject, subject ID, class ID, department and number of students registered for that particular subject.

4.4.1 Data structure to store the new created subject data:

```
New Subject {subject Name: String,
                    Subject Code: String,
                    Department Name: String,
                    Class ID: String,
                    Number of students: int
                    }
```

4.5 QR code generation block:

To mark the attendance for the particular subject in particular time period each supervisor has to create the QR code each time when he/she is conducting the class. The QR generation block generates different QR code for each subject for a particular time period. For example, as per the class timetable for every subject mentioned in the timetable at particular time the supervisor needs to generate the QR code and display it for ordinary nodes to mark the attendance.

4.5.1 Data structure to store the QR code generation data:

This block contains the information like name of the department, class name, class ID, number of students, subject name, subject ID, lecture starting time and lecture end time.

QR Code {Department Name: String,
Class ID: String,
Number of students: int
Subject Name: String,
Subject ID: String,
Lecture Start Time: time,
Lecture End Time: time
}

4.6 Mark attendance block:

Once the supervisory node generates the QR code it is displayed for ordinary node to scan and mark the attendance for that particular subject in a particular time slot. Upon successful marking of attendance of all ordinary node a new block is created and added to the blockchain.

4.6.1 Data structure to store marked attendance data:

This block contains the information like name of the department, class ID, subject ID, lecture starting time, lecture end time, username and device ID. The data structure used to mark student attendance is as follows.

Attendance {Department Name: String,
Class ID: String,
Number of students: int
Subject Name: String,
Subject ID: String,
Lecture Start Time: time,
Lecture End Time: time,

Mac ID: String
}

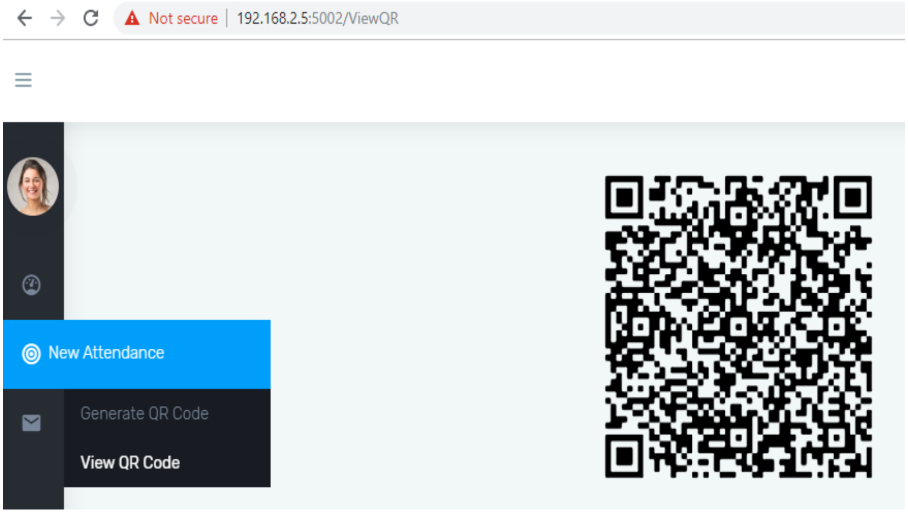
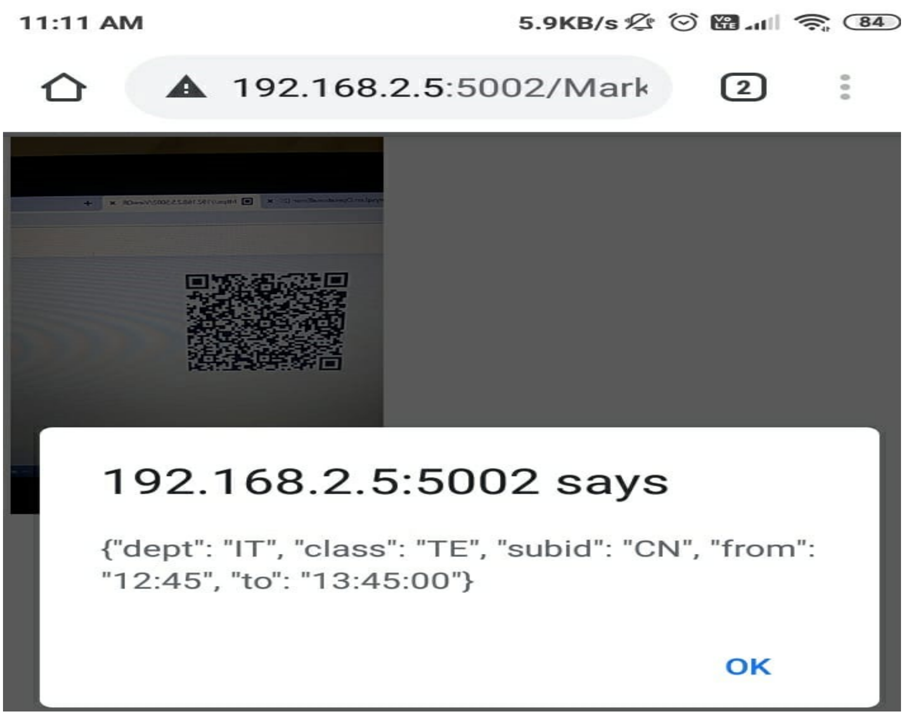


Fig. 6. QR code displayed by supervisory node for marking the attendance

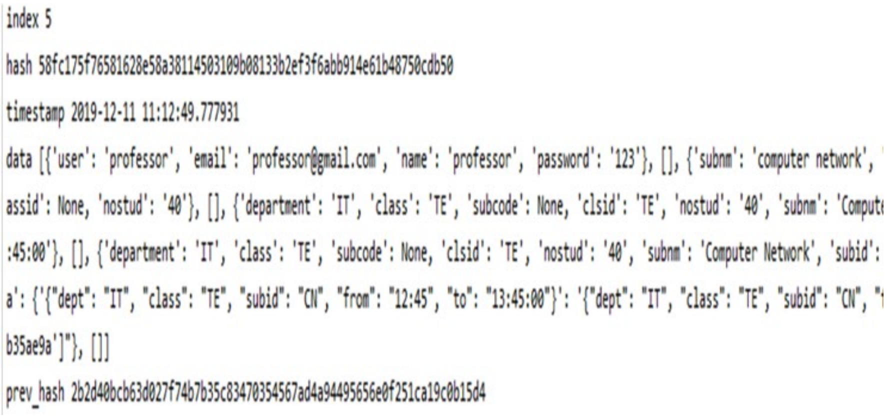
Once the supervisory node displays the QR code all the ordinary nodes has to scan the QR code using their mobile device. The figure 1.15 shows the ordinary node marking attendance by scanning the QR code. The figure 1.16 shows the code snippet written to scan the QR code whereas in figure 1.17 we can observe that the block created after scanning the QR code and it is added to the blockchain at index 5.



192.168.2.5:5002 says

{"dept": "IT", "class": "TE", "subid": "CN", "from": "12:45", "to": "13:45:00"}

Fig. 7. Output of QR code read for mark attendance



```
index 5
hash 58fc175f76581628e58a38114503109b08133b2ef3f6abb914e61b48750cdb50
timestamp 2019-12-11 11:12:49.777931
data [{'user': 'professor', 'email': 'professor@gmail.com', 'name': 'professor', 'password': '123'}, [], {'subnm': 'computer network', '
assid': None, 'nostud': '40'}, [], {'department': 'IT', 'class': 'TE', 'subcode': None, 'clsid': 'TE', 'nostud': '40', 'subnm': 'Comput
:45:00'}, [], {'department': 'IT', 'class': 'TE', 'subcode': None, 'clsid': 'TE', 'nostud': '40', 'subnm': 'Computer Network', 'subid':
a': {'{"dept": "IT", "class": "TE", "subid": "CN", "from": "12:45", "to": "13:45:00"}': '{"dept": "IT", "class": "TE", "subid": "CN", "
b35ae9a']"}, []]
prev_hash 2b2d40bcb63d027f74b7b35c83470354567ad4a94495656e0f251ca19c0b15d4
```

Fig. 8. Output of marked attendance data stored in blockchain

5 Results and Discussion:

The proposed algorithm is successfully implemented in python. The algorithm is able to generate the five types of blocks for the proposed private blockchain network. The different blocks generated using the proposed algorithm are genesis block, registration block, new subject creation block, QR code generation block and mark attendance block. The system is in its initial stage, at this statge we have calucalated the time taken to generate each block. As shown in figure 4 the registration block is added after genesis block. The registerd students can mark their attendance as shown in figure 8, the data gets added to to the mark attendance data block after reading / scanning the QR code. 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

The Graph below shows the time taken to generate the block by proposed algorithm.

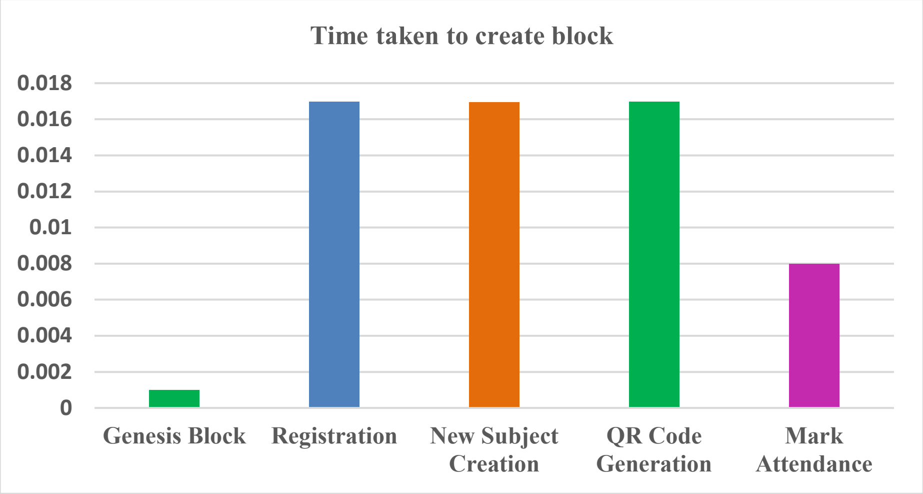


Fig. 9. Time taken to generate the blocks

6 Conclusion and Future Scope:

The proposed private blockchain framework is implemented in python using Flask as web application framework. As per the concepts of blockchain the framework is implemented SHA-256 algorithm is used as a cryptographic hash function. We were successfully able to generate the genesis block and as per the flow decided the various blocks gets generated and added to the blockchain. The data of students after scanning the QR code is added to the mark attendance block. The registration, subject creation and QR code generation blocks are generated with 0.017 seconds approximately.

In future more functionalities will be implemented to view the blocks and one more IOT component in the form of RFID smart cards can be included to make the system more complex and test it under the real time settings.

References

1. Kuo, T. T., Zavaleta Rojas, H., & Ohno-Machado, L. (2019). Comparison of blockchain platforms: a systematic review and healthcare examples. Journal of the American Medical Informatics Association, 26(5), 462-478.
2. Yang, W., Aghasian, E., Garg, S., Herbert, D., Disiuta, L., & Kang, B. (2019). A Survey on Blockchain-based Internet Service Architecture: Requirements, Challenges, Trends and Future. IEEE Access.
3. Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access, 7, 22328-22370.
4. Liu, Z., Luong, N. C., Wang, W., Niyato, D., Wang, P., Liang, Y. C., & Kim, D. I. (2019). A survey on blockchain: a game theoretical perspective. IEEE Access, 7, 47615-47643.
5. Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2018). Security services using blockchains: A state of the art survey. IEEE Communications Surveys & Tutorials, 21(1), 858-880.
6. Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in Industries: A Survey. IEEE Access, 7, 36500-36515.
7. Liu, J., & Liu, Z. (2019). A Survey on Security Verification of Blockchain Smart Contracts. IEEE Access.
8. Monrat, A. A., Schelén, O., & Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. IEEE Access, 7, 117134-117151.
9. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, 82721-82743.
10. Lo, S. K., Liu, Y., Chia, S. Y., Xu, X., Lu, Q., Zhu, L., & Ning, H. (2019). Analysis of Blockchain Solutions for IoT: A Systematic Literature Review. IEEE Access, 7, 58822-58835.
11. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the

internet of things. Ieee Access, 4, 2292-2303.

12. 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.
13. Hermanto, N., & Baihaqi, W. M. (2018, November). Implementation of QR Code and Imei on Android and Web-Based Student Presence Systems. In 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE) (pp. 276-280). IEEE.
14. Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2018, April). Blockchain and smart contract for digital certificate. In 2018 IEEE international conference on applied system invention (ICASI) (pp. 1046-1051). IEEE.
15. Meng, Z., Morizumi, T., Miyata, S., & Kinoshita, H. (2018, July). Design scheme of copyright management system based on digital watermarking and blockchain. In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC) (Vol. 2, pp. 359-364). IEEE.
16. Baralla, G., Pinna, A., & Corrias, G. (2019). Ensure Traceability in European Food Supply Chain by using a blockchain System.
17. Benčić, F. M., Skočir, P., & Žarko, I. P. (2019). DL-Tags: DLT and Smart Tags for Decentralized, Privacy-Preserving, and Verifiable Supply Chain Management. IEEE access, 7, 46198-46209.
18. Tantidham, T., & Aung, Y. N. (2019, March). Emergency Service for Smart Home System Using Ethereum Blockchain: System and Architecture. In 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 888-893). IEEE.
19. Vijayakumar. K, Nawaz Sherif. T, Gokulnath.S, “Automated Risk Identification using Glove algorithm in Cloud Based Development Environments”, International Journal of Pure and Applied Mathematics Volume 117 No. 16 2017.
20. J. Dafni Rose*, K. Vijayakumar and S. Sakthivel, “Students’ performance analysis system using cumulative predictor algorithm”, Int. J. Reasoning-based Intelligent Systems, Vol. 11, No. 2, 2019.