ISSN 2278-3091
Volume 10, No.3, May - June 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse101032021.pdf
https://doi.org/10.30534/ijatcse/2021/101032021

Securing Academic Record using Blockchain with Hyper ledger Fabric

G. Dhanalakshmi[1].B. Bhavethra[2]. Muppa Keerthi Chowdary[3]. S. Keerthana[4].
Associate Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai$_1$.
Student, Department of Information Technology, Panimalar Institute of Technology, Chennai
bhavethra2001baabu@gmail.com[2],keerthimuppa123@gmail.com[3],keerthanas1408@gmail.com[4]

ABSTRACT
Student records (SR) have to be stable and safe from the third parties. The blockchain could guarantee safety, privilege, transparency and also provides access control. Despite of having a scalable architecture in Hyperledger fabric Block chain there are various factors which affects the performance of the system and causes latency. Added to that it could also not provide better indexing capability.In this proposed system, a storage structure is created which could provide better access time. Initially, a block of desired size is created, based on the configuring parameter this reduces the latency. Next, the metadata of the SR block is duplicated on an off-chain database to overcome the disadvantage of indexing capacity and latency .SR data will be transparent and could be accessed at less time using less manpower and time.

1.INTRODUCTION:

Student records (SR) are confidential information of University. It should be distributed among the stakeholders like students, Student affairs and faculties.SR needs to be protected securely with access control system. Blockchain tracks down the flow of information and stores the transaction. Hence blockchain could be used for keeping the SR data confidential.

Blockchain is a trending technology, which is approved in the present day. It is widely used in the field of IoT, education, Insurance and financial market. It is of three types i.e., public, consortium and private. A public Blockchain could be accessed by anyone in various organizations. Consortium Blockchain allows everyone or only the desired members to obtain hybrid access method. Private Blockchain supports only predefined users or organization to make changes in the data.

The suggested system is looking forward to meet the needs of the university with good performance and cheap cost.

2. HARDWARE AND SOFTWARE COMPONENTS

2.1SOFTWARE REQUIREMENTS

- Python
- Pyside2(Qt5bindingf or Python3)
- Hyperledger fabric
- State database

2.2HARDWARE REQUIREMENTS:

- P2P network with distributed ledgers

3.RELATED WORKS

In this system Students, Student affairs, Faculties, and Companies are currently considered as stake-holder. The stakeholders can have different cont-act opportunity to read, write and update for SR data. A student can also read access to his/her in-formation. Student affair can read, written and updated all student information. Although faculty can read all student information, but they can only write and update some information. Companies can only read some information for internship students. This system is configured in 2 organiza -tions which contains two peer nodes respectively. The Hyperledger Fabric blockchain is distributed in each peer.

In this system 10 different chain codes will be specified on different types of 10 channels for all stakeholders. If two stakeholders exchange data between them they need to satisfy two types of Chain code. The first type is defined to confirm Data agreement between two stakeholders for exchangeable data. The second type is needed to run and exchange data among stakeholders.

In this system, solo is currently used as an order-ing service to create a block of transaction. Block size controls maximum number of transactions batched into a block. The absolute maximum no. of bytes and the preferred maximum no.of bytes for each transaction in a block affects the block size. size. Block size should be scalable depending on the transaction arrival rate to increase throughput and decrease latency. If the transaction arrival rate is larger than or equal to situation point, the block size should be higher. Otherwise block size needed to be lower.

In this proposed system, the creative-time of the transaction will be stored as additional metadata for each transaction in the blockchain. An off chain database (MongoDB) is used to duplicate the metadata such as key, version, block-id, transaction-id and the timestamp of the Transaction. MongoDB is a type of open-source document database. A document is also stored as a set of key-value pairs. It supports a highly scalable and performance- oriented database.

4.HYPERLEDGER FABRIC ARCHITECTURE

Hyperledger fabric is a collection of key value pairs and private blockchain with infrastructure and safe CPU and network utilization. I will only support predefined organizations of the users. It complies with the data protection regulations when the permissions are considered.

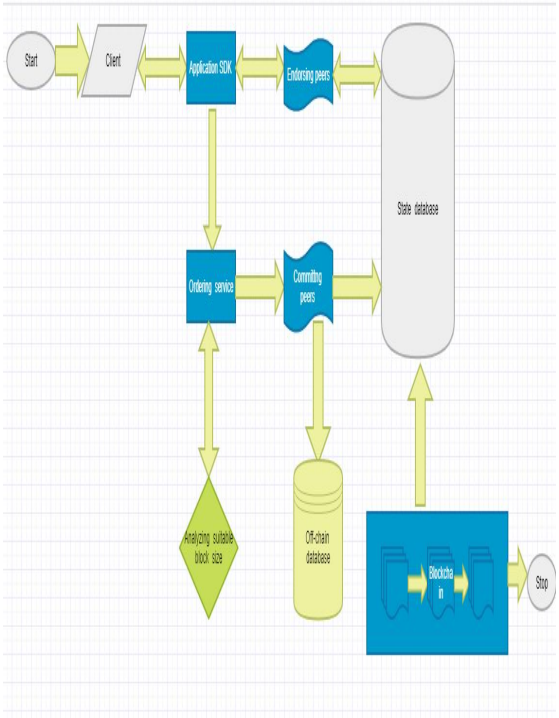


Figure1: Transaction life cycle of Hyperledger fabric

4.1PROPOSED ARCHITECTURE

In this system Students, Student affairs, Faculties, and Companies are currently considered as stake-holder. The stakeholders can have different contact opportunity to read, write and update for SR Data. A student can also read access to his/her information Student affair can read, written and Updated all the student information. Although faculty can read all student information, but they can only write and update some information. Companies can only read some information for internship students.

This system is configured in 2 organizations which
Contains two peer nodes respectively. The Hyperledger Fabric blockchain is distributed in each peer. In this system 10 different chain codes will be specified on different types of 10 channels for all stakeholders. If two stakeholders exchange data between them they need to satisfy two types of chain code. The first type is defined to confirm data agreement between two stakeholder's exchangeable data. The second type is needed to run and exchange data among stakeholders.

In this system, solo is currently used as an ordering service to create a block of transaction. Blocksize controls maximum number of transactions batched into a block. The absolute maximum number of bytes and the preferred maximum number of bytes for each transaction in a block affect the block size. Block size should be scalable depending on the transaction arrival rate to increase throughput and decrease latency. If the transaction arrival rate is larger than or equal to situation point, the block size should be higher. Otherwise block size needed to be lower.

In this proposed system, the creative-time of the transaction will be stored as additional metadata for each transaction in the blockchain. An off chain database (MongoDB) is used to duplicate the meta data such as key, version, block-id, transaction-id and the timestamp of the Transaction. MongoDB is a type of open-source document database. A document is also stored as a set of key-value pairs. It supports a highly scalable and performance- oriented database.

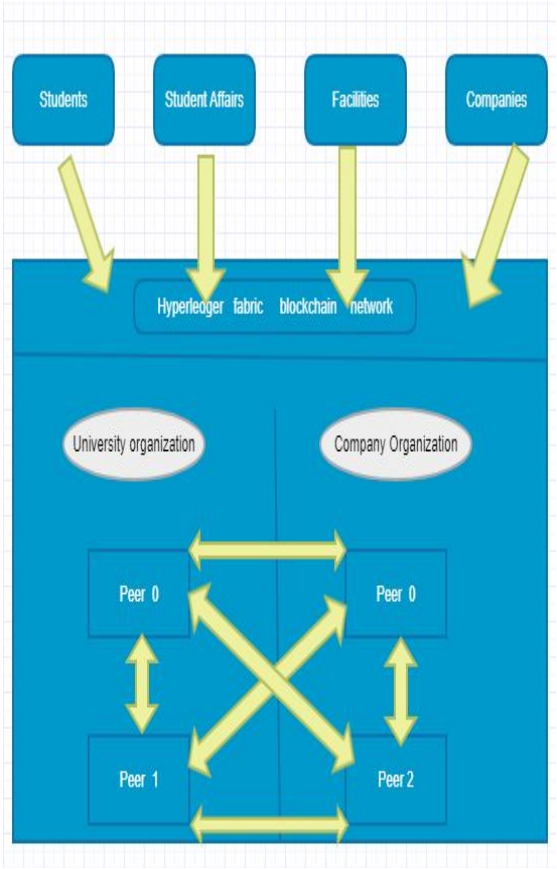


Figure 2: Proposed network architecture

5.DESIGN OF THE STUDY

Designing of this implementation projects requires the study of various frameworks and pre-designed models, which include learning the new frameworks, development plan, and writing user test cases to deal with an issue that come up during the implementation.

The design flow chart developed shown in the figure below:

1. An instructor and student will be peers in the HLF network.
2. The instructor will then send in a request to insert in a student marks/grade request.
3. Endorsing peers will then write a Chain code on this record and moves this transaction to ordering peer.

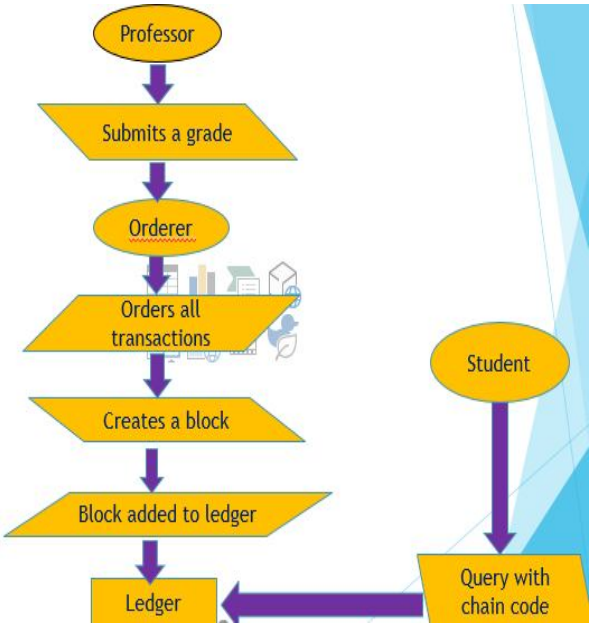


Figure 3: Flow chart for implementing the student records

4. The ordering peer than validates all the proposals and sorts them out alphabetically, and then the block gets generated and forwarded to the committing peer.
5. Committing peer than validates the received block from Ordered, commits the block onto ledger, which is immutable and tamper-free.

6.ANALYSIS AND RESULTS:

The results of the application used to connect educational organizations to share sensitive information related to students. This project mainly focused on the developing a network for safe and secure communication without any middleware organizations to take care of data integrity and confidentially. Hyperledger fabric is very scalable, it supports multiple programming languages and the ability to integrate components such as consensus algorithms and membership services, which issues and validates certificates. Regarding the security provided by this architecture, Hyperledger Fabric bundles in TLS encryption and Membership Service providers for proper certificate handling. This paper also discusses a structure of block with multiple transactions and how the structure helps in making the entire blockchain immutable. The metadata of the SR block is duplicated on an off-chain database and it overcome the indexing capacity and latency.

6.1SCREENSHOTS:

The data submission page

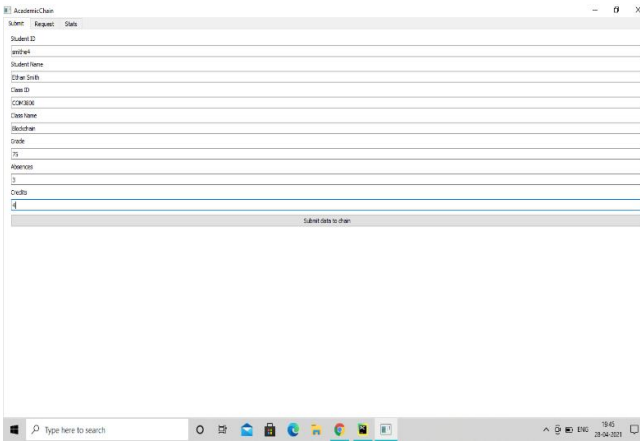


Figure 4: Student record of data submission page

The data request page

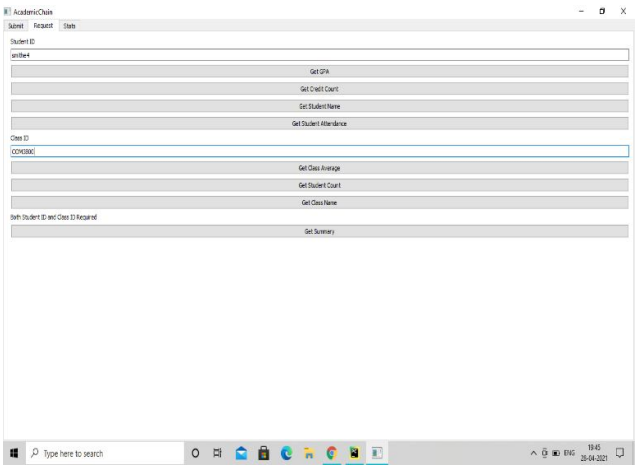


Figure 5: Student record of data request page

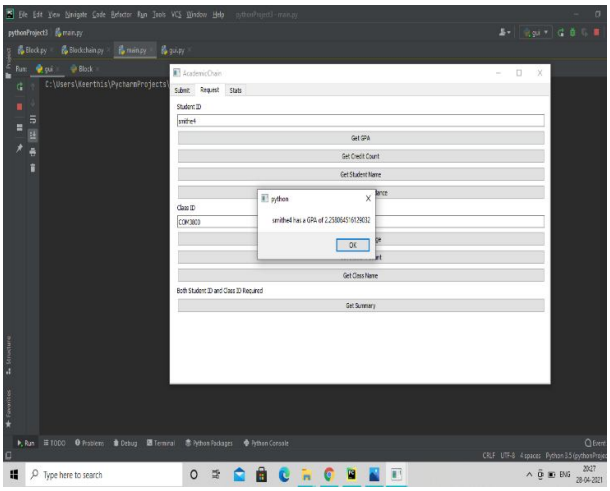
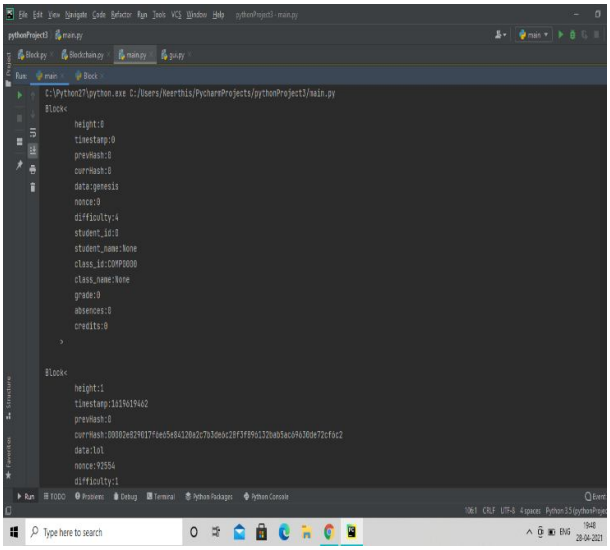


Figure 6: Student record of getting each data

The status page:



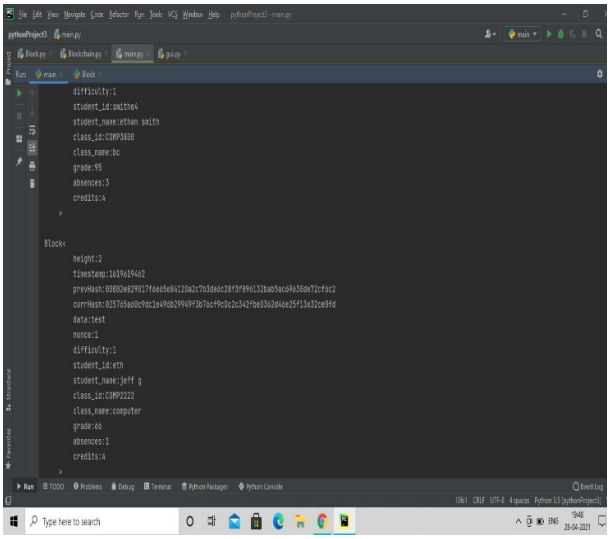


Figure 7: Student record of status page

7.CONCLUSION

This implementation study of Hyperledger fabric is to develop a network between the participating educational organizations; This is an open-source architecture that aims to develop distributed ledger applications. The student record will be transparently accessed with the high performance. The configuration parameter of block size is analysed to reduce the waiting time of transaction before creating a block. The MONGDB database will be used as an off-chain to duplicate the metadata of the block. The access time of the proposed system can be better than the original query of the Hyperledger fabric. The configuration of different elements in Hyperledger Fabric will be analysed and set up to support higher throughput and lower latency for Student record data. Since the application manages the ledger without any administering it, it needs to have a consensus algorithm, and to look at the blocks, the tool generated and crypto algorithms it uses in the process makes the ledger immutable, and every transaction needs to be signed, verified and valid.

REFERENCES

[1]. H-N. Dai, Z. Zheng, and Y. Zhang, “Blockchain for Internet of Things: A survey,” IEEE Internet Things J., vol.6, pp. 8073_8094, Oct. 2019.

[2]. X. LI, A.K. Sangaiah, S. Kumari, F. Wu, J. Shen, and M. K. Khan, and A. K. Das, “A novel chaotic maps-based user authentication and key agreement protocol for multi-server environments with provable security,” Wireless Pers. Commun., vol.89, pp.567-597, Jul. 2016

[3]. P. K. Sharma, M. Y. Chen, and J. H. Park, “A software defined fog node based distributed blockchain cloud architecture for IOT,” IEEE Access, vol.6, pp.115-124, 2018.

[4]. W. Liang, Y. Fan, K-C, Li, D. Zhang, and J-L. Gaudiot, “Secure data storage and recovery in industrial blockchain network environments,” IEEE Trans. Ind Informat., early access, Jan 13, 2020.

[5]. X. Li, A. K. Sangaiah, S. Kumari, F. Wu, J. Shen, and M. K. Khan, “An efficient authentication and key agreement scheme with user anonymity for roaming service in smart city,” Pers. Ubiquitous Comput., Vol. 21, pp.791-805, Oct. 2017.

[6]. Patrick Ocheja Brendan Flanagan, Hiroshi Ueda and Hiroaki Ogata, Managing lifelong learning records through blockchain.

[7].ABahga and V. K. Madissetti, “Blockchain platform for industrial Internet of Things,” vol.09, pp. 533-546, 2016.

[8]. JerinasGresch, Bruni Rodrigues, Eder Scheid, Salil S. Kanhere, and Burkhard Stiller.The Proposal of a

Blockchain-Based Architecture for Transparent Certificate Handling.

[9]. X. Li, J. Niu, M. Karuppiah, S. Kumari, and F. Wu, "Secure and efficient two factor user authentication scheme with user anonymity for network-based E-health care applications, vol. 40, Dec. 2016.

[10]. L. Aniello, R. Baldoni, E. Gaetani, F. Lombardi, A. Margheri, and V. Sassone, "A prototype evaluation of a tamper-resistant high performance blockchain transaction log for a distributed database." In Proc. Pp. 151-154, Sep.2017.