Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

Blockchain for Giving Individual Hub Control Over Their Databases

P. Naveen[1*], P. Sivakumar[2]
[1]Assistant Professor, Department of ECE, Kalasalingam Academy of Research and Education
[2] Professor, Department of ECE, Kalasalingam Academy of Research and Education
*naveenamp88@gmail.com, sivapothi@gmail.com

ABSTRACT

With the development of new digital products, software updates, integrating one platform through different devices, services, tools, we do face severe data breach in internet. Even the most secure firewall has been breached and data being modified. Today because of the development in artificial intelligence, few applications are partially controlled by system like suggestions for the page we view. If those data are breached and modified, then the entire system will suggest incorrect data. The entire global has faced some terrorists attack every now and then. Apart from this, illegal entry of criminals into unauthorized locations where people are using fake ID and getting into the current system. Now a days we are giving authorization for criminals to get into system by looking into the fake ID or verifying in a database. But criminals are fair enough to breach the database which is not that much secure. Because the existing system is centralized, not secure and reliable. Here we proposed a system based on hyperledger fabric approach to providing secure, immutable, reliable, decentralized, and palpable control over their database records. The proposed system employs decentralized storage of database system and trusted way of transaction to create, issue and revoke the data in the system. Here we evaluate the proposed smart contract metrics through latency, throughput and block time.

Keywords
Hyperledger Fabric, Blockchain, Average Latency, Throughput.

Introduction

Any organizations have long-lasting practices to maintain their employee records such as identifying, monitoring, and deploying their residents, and using a variety of methods to do so. Their manoeuvres include personal identification and validation procedures such as biometric-based technologies, encryption technologies, firewall-based methods etc. Today, many organizations maintain comprehensive identification systems for identifying and distinguishing between employees, other staffs, visitors, with widely accepted documents such as ID cards, facial features, etc. acting as long-term authentication tools. To clear these systems, many dominions have gone down in streamlining them by incorporating the practices of biometric authentication, which use the data collected to document an individual's unique physical characteristics — in general, fingerprints, facial features, iris, and retinal nerve verification.

One of the main criticisms of biometric database is that there are numerous major security vulnerabilities that pervade anywhere in biometric database operations and can result in data leakage. The corresponding organization should continue to increase their security for their database from being breached through cyber security team and must stop people hacking their personal information. The problem has gotten to such a level that one can simply access thousands of several organization databases with confidential information through some simple hacking methodologies that is openly available on Internet.
We are in a situation to track suspicious individuals' activities by their reference number, which will link them to other services they use. We need automated programs that scan every people activity and their forms to automatically label certain individuals as dangerous or suspicious.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

While it may help curb crime and terrorism, it has the potential to turn a sector into a repressive watchdog.
Many of the activities failed because of providing fake ID cards and misleading persons who needs to verify the database. 26/11 Mumbai attack reveals that 10 identity cards were fake, and they hoodwinked the entire system which results in loss of 165 lives. Also, people getting into other systems through fake IDs and using their data for illegal purposes. We were in a situation that we cannot check the originality of all organization identity. So, it is necessary to integrate every organization into a single system. Even though it is not an easy process because of the increased in digitalization and rapid increase in cybercrime we need to go for much secure, trustable and transparency technology to interact with an organization database.

Blockchain is one such technology that provide secure, trustable and transparency in the integrated system. Blockchain uses the distributed ledger for transactions so that all transactions are spread out and controlled globally. All the data is being synchronized and any organizations can take the copy of their transactions. To verify the ID, through this blockchain technology any organization can interact with any other organization in the system and confirm the details. Since we need to limit the use of interaction of low-level organizations (E.g., a computer centre, grocery shop) and high-level organizations (E.g., defence sector, Agent) we need to provide Admin control to one of the organizations.

To make a complete control in the proposed system here we used Hyperledger Fabric technology. Hyperledger Fabric is an open source blockchain that can integrate several components such as membership services and consensus algorithm. It has channel technology for secure transactions within the group of organizations. Here the proposed system is compared with the existing system in Table 1.

Table 1. Comparison with existing system

Parameter	Cloud Based System	Proposed System
Security	Partially	Yes
Privacy	Partially	Yes
Immutability	Partially	Yes
Attribution	Partially	Yes
Decentralized Storage	No	Yes
Individual Hub Centered	Partially	Yes
Decentralized Execution	No	Yes

Related Work

Satoshi Nakamoto proposed a peer-to-peer network using work-proofs to record the general history of transactions. Nodes can leave the network at will, accepting the work proof chain as evidence of what happened when they left [1]. Marko Vukolić briefly observed the state of the art and the growing directions towards scalable blockchain. He distinguishes between Proof-of-work (PoW) and Byzantine fault-tolerance (BFT) consensus protocols and focus their respective advantages [3].
Wu proposed blockchain technologies are used to promise both data integrity and non-rejection, and ciphertext can be quickly developed using pre-encryption technology. Also, characteristics

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

are veiled in anonymous access control structures using the Attribute Bloom filter. When a secret key is mistreated, the source of the abused secret key can be reviewed. Safety and performance analysis show that the proposed project is safe and efficient [4].

To obtain a reliable and flexible system, Abdelghani propose a new confidence-rating model that can detect malicious nodes [5]. Wenjuan suggest a machine learning-based approach to assign penetration sensitivity based on skilled acquaintance and design a trust management model that allows each IDS to deliberate their detection sensitivity by evaluating the reliability of others. In the evaluation, he examines the efficiency of their proposed method under different attack scenarios [6].

Zhou confess the traditional trust is replaced by a third-party smart contract. Their program uses hyperledger fabric where enforcement is implemented by a consensus mechanism, which ensures the safety of blockchain [7]. Vora proposes a plan to achieve all the stated functions without disclosing any information about the contents and access methods of the recovery party [8].

Thakkar steered a complete experiential study to comprehend the performance of the allowed blockchain platform HyperLeader Fabric, with varying values assigned to configurable parameters such as block size, channels, state database choices, endorsement policy and resource allocation [9]. Sukhwani design the PPFT consensus process using stochastic reward nets (SRNs) to calculate the average time to complete a consensus concept for networks up to 100 peers [10].

Gorenflo propose hyperledger fabric blockchain structure can be redesigned to support approximately 20,000 transactions per second [11]. Gervais introduce a new size framework for analyzing the security and performance implications of various consensus and network parameters of PoW blockchains [12].

Proposed Work

In our proposed system, several organization hubs are organized and interconnected in a well phased manner. In this paper, several organizations in the system are represented as Individual Hub 1, 2, 3, . . . N. For example, image database of defense sector, medial sector, railways, airport, educational institutions, startup companies, etc. swarms a set of logical peers to produce a block chain topology. Here, the individual hubs have the privilege to interact with the overall system by different types of transactions through blockchain topology. Since the database contains secure data in several sectors, the entire control is maintained by anyone sector which has the highest priority. Here we name the controller as Admin. All the individual hub has the right to create, issue and revoke data but deleting the data from existing system is not permitted. The transactions are recorded in the ledger and it no longer can be deleted by anyone. The entire blockchain system is controlled and monitored by the core components of the Blockchain framework such as Admin, Individual Hub, Ledger, Endorser, Orderer and Channel. The entire framework is shown in Figure 1. These core components will take care of the entire transaction process with respect to individual hub policies.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

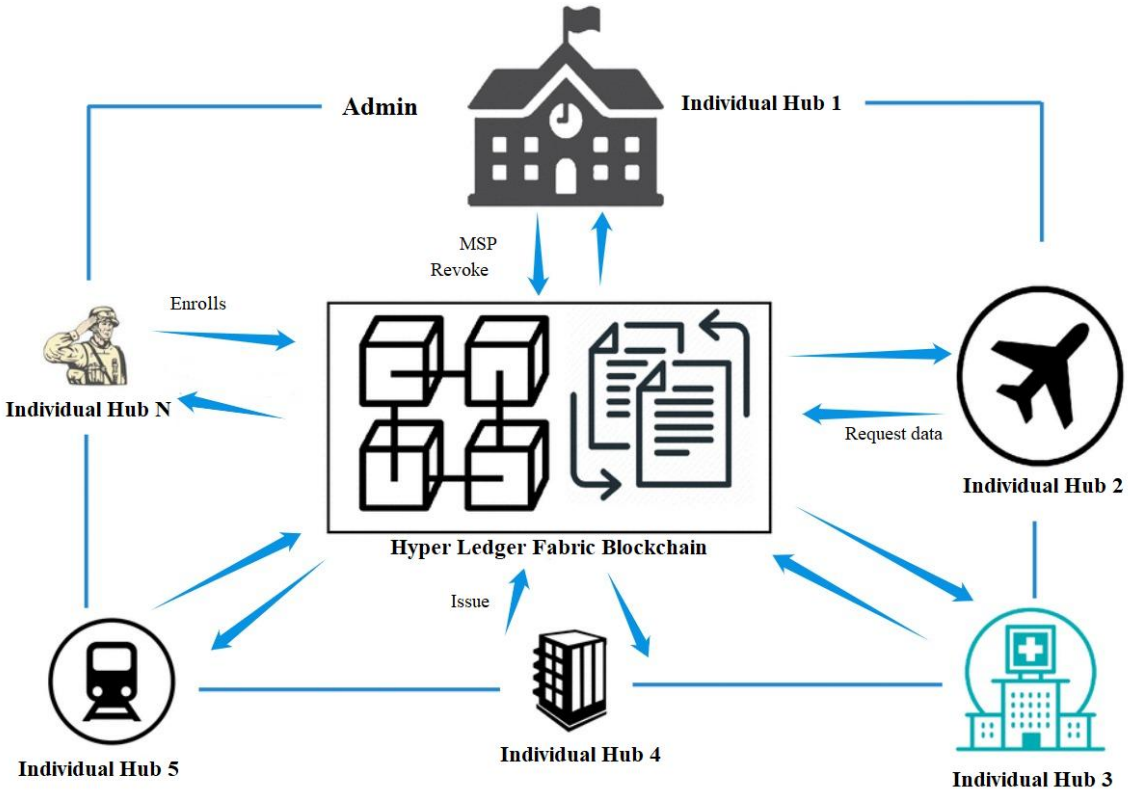

Figure 1. Proposed Hyperledger Fabric System

Here we used hyperledger fabric which has the ledger in which individual hub can manage their transactions. In addition to ledger, hyperledger fabric uses smart contracts through which individual hub can manage their transactions. Here the individual hub can do their transactions by enrolling themselves as a member of the system through Admin. It is the only way to permit unknown identities to have their transactions in the system. Here group of individual hubs can have their own channel i.e., creation of a channel is permittable so that separate ledger is possible which can be accessed within their own trustable network.

It is necessary to record the transactions in the ledger. Here the individual hub must participate in consensus process, where the transactions are ordered in blocks. To record the transactions on the ledger, we must establish the order of transactions. Raft ordering service is implemented in our design since admin can select a subset of available orderers and modify the ordering nodes.

Smart contracts in hyperledger fabric are written in chaincode. Here we have developed an application that is external to the blockchain to interact with the ledger. The following services are necessary to interact with the ledger from individual hub for transaction.

- Create: When a data is added, each individual hub will receive the notification
- Issue: When an existing data is requested, individual hub will send the data
- Revoke: Admin warns the individual hub to suspend the data

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

It is necessary to consider that the transaction ensued is valid. The set of peers on a channel that must execute chaincode which has an endorsement policy and endorse the execution results. These endorsement policies outline individual hub (through their peers) that "approve" the execution of a project.

Privacy is the major concern of our entire work. That is why all individual hub has the right to interact among themselves, but admin plays a major role in transaction of data among them. Admin can deny any transaction to be happened in the block chain.

Implementation

In this section, the smart contract process is explained for our blockchain system. Meanwhile, the blockchain based system architecture is proposed. Different methods and configurations are used for block transaction in the network. In our proposed system, a private key and shared symmetric key enable the system to be shared to all the individual hubs available in the blockchain network.

In this section, the system architecture based on blockchain is explained. Our proposed system architecture has two major divisions. One is admin and other is individual hub. Here the individual hub can have all right in the system to create, issue and revoke data but the admin has the complete control of the system to approve those changes and to add or remove any data in individual hub. And even to permit the individual hub into the system or deactivating the hub in the system by participating in further transaction process.

Create

When an individual hub wants to create a data in the system, it must enroll itself to the blockchain system. Then admin do approve the hub to be the part of the blockchain system to participate in the transaction process via Membership Service Provider (MSP). It is wish of the individual hub to create a new channel or existing channel to have the record of the transactions on the ledger. Once the hub get itself enrolled, admin do assign a unique ID and private key to the individual hub. Now the hub can add the data with ID, facial features, location, current status, etc.

Issue

When an individual hub wants to request a data to verify the person in other hub, it will process it requests through ordering service. Though individual hub responds immediately, the data will be permitted only if admin permits. Here we follow Raft ordering service and the data being exchange through its procedure. Later admin checks the individual hub trust parameters such as confidentiality, security, necessity of verification and then it issues the data available in database.

Revoke

Once the requested data is cleared from one hub to other hub and if it does not clear the admin regularities then admin do revoke the access of data from destination hub. Also, if there is a duplication of data in two hubs then admin can revoke the data through updating the status without the permission of the individual hub. The duplication of data can be raised as a query

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

from any individual hub. All hub in the blockchain system has the option to raise a query about any data that is available in the system. The response is decided by the admin.

Performance Evaluation

In this section, the evaluation of the proposed architecture is explained with simulation parameters. The assessment cases describe latency, throughput and block time.

The experiment is conducted based on number of epochs of writing the transaction in the ledger with number of transactions in each epoch. The performance of the blockchain is evaluated by the transaction time.

The analysis of hyperledger fabric platform is done using experiments with the following parameters. Let us do the transactions with respect to individual hub and number of peers. Then we do calculate the parameters such as latency and throughput.

Here we have taken measurements for the transactions by 1Hub-1peer, 2Hub-1peer and 2Hub2peer to illustrate the observations. After concluding Hub and peer, the number of transactions and epochs is finalized. Here let us take 2000 transactions in 6 epochs. For the beginning experimental setup, we started from 50 transactions per second, and it is increased to 100, 200, 250, 400, 500 transactions per second.

The transaction time with respect to hub and peer is plotted in Figure Here the results have been plotted for 50, 100, 200, 250, 400, 500 transactions per second and for each epoch 2000 transactions have done. From the Figure we can observe that 1Hub-1Peer takes 180 seconds to reach 6000 transactions whereas 2Hub-1Peer reaches only 3500 and 2Hub-2Peer reaches only 2450 in 180 seconds. From Figure 2 we can observe that the time taken for transaction process increases as there is increase in number of Hubs and peers.

Figure 2. Transaction Execution Time

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

The important parameter that decides the transaction performance in blockchain is transaction latency. Transaction latency is the network-level interpretation of the time that the effect of a transaction can be used across the network. It can be mathematically written as difference between the confirmation time for transaction with respect to network threshold and the submit time that includes several timing factors such as settling time, propagation time, etc. that happens in the blockchain technology.

$$Transaction\ Latency, L_T = (T_C * N_T) - T_S \quad (1)$$

where,

T_C - Confirmation Time
N_T - Network Threshold
T_S - Submit Time

The plot in Figure 3 shows the average latency in seconds for 2000 transactions per epoch with the transaction rate of 50, 100, 250, 300, 400, 500 transactions per second for transaction in write mode. We can observe from the Figure 3 as the average latency increases due to increase in transaction rate in different epochs.

The plot in Figure 3 shows the average latency in seconds for 2000 transactions per epoch with the transaction rate of 50, 100, 250, 300, 400, 500 transactions per second for transaction in write mode. We can observe from the Figure 3 as the average latency increases due to increase in transaction rate in different epochs.

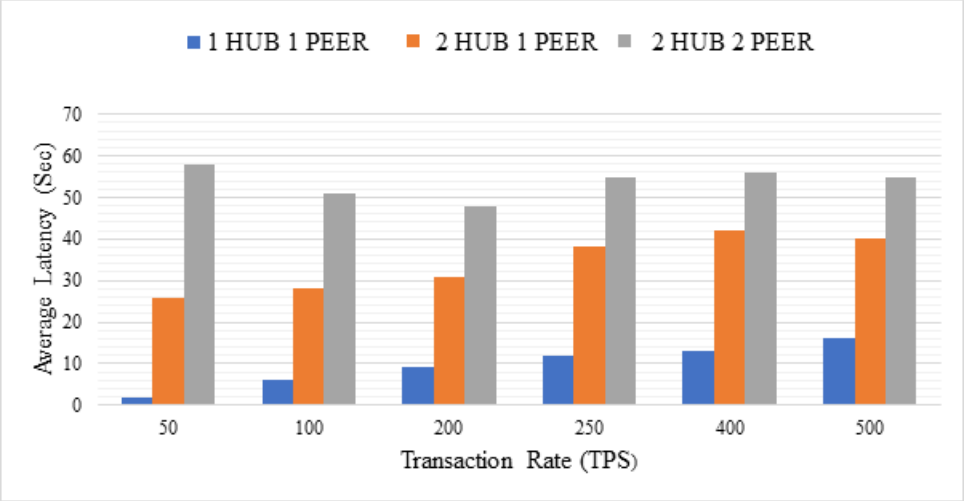

Figure 3. Transactions Average latency

Another important parameter that decides the transaction performance in blockchain is transaction throughput. Transaction throughput is the rate at which valid transactions are made by hyperledger fabric platform of blockchain system over a limited period. Here the transactions corresponding to the committed nodes in the system and not to a single node. The total committed transactions are calculated by subtracting the total number of invalid transactions from the total transactions.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

$$Transaction\ throughput, T_T = \frac{T_{CT}}{(T_{TS})} * N_C \quad (2)$$

where,

T_{CT} - Total Committed Transactions
T_{TS} - Total time in seconds
N_C - Committed nodes

Figure 4 shows the transaction throughput for 2000 transactions per epoch with the transaction rate of 50, 100, 200, 250, 400, 500 transactions per second for transaction in write mode. We can observe from the Figure as the Transaction throughput decreases due to increase in transaction rate in different epochs. With compared to the results of Figure the transaction throughput result is opposite to that of average latency. Hence from the results, we can observe that average latency and transaction throughput are inversely proportional.

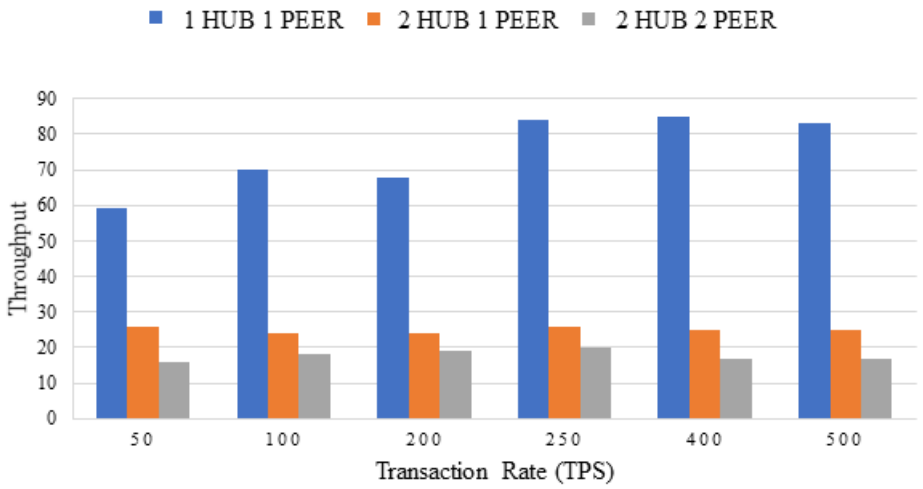

Figure 4. Transaction throughput

There are cases when query arises in our system from any of the Hub to verify the identity, so it is necessary to read the data from our system. To perform the experiments here we have taken five epochs and we must change the transaction mode from write mode to read mode. Figure 5 shows the transaction throughput for 2000 transactions per epoch with the transaction rate of 50, 100, 200, 250, 400, 500 transactions per second for transaction in read mode. Read Latency is the time between the read request is submitted from any of the Hub and the time it is answered from another Hub or when the reply is received from another Hub.

$$Read\ Latency, L_D = (T_{RR}) - T_S \quad (3)$$

where,

T_{RR} - Time when received response
T_S - Submit Time

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

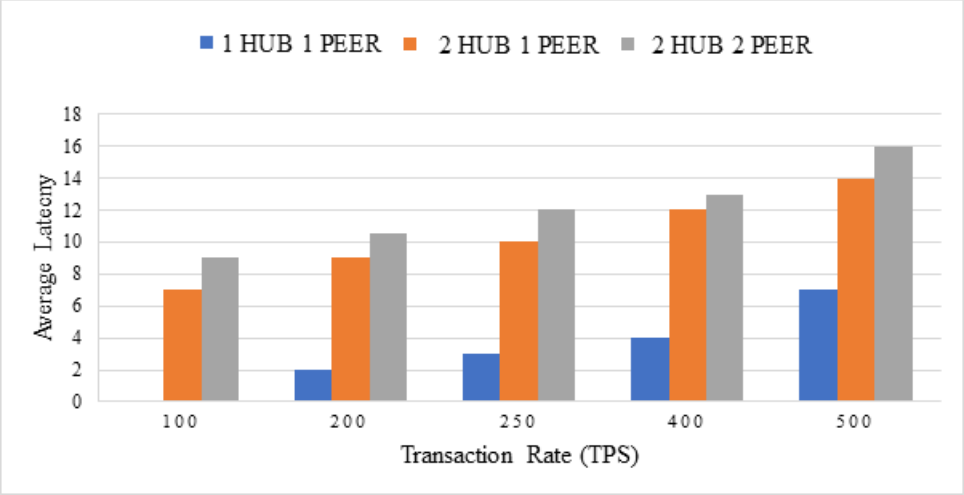

Figure 5. Average Read Latency

Another parameter which may not be the primary measurement for blockchain performance is read throughput, but the readings are quite useful. Figure 6 shows the read throughput for 2000 transactions per epoch with the transaction rate of 50, 100, 200, 250, 400, 500 transactions per second for transaction in read mode. Read throughput is the number of read operations completed in each period. It is expressed in readings per second.

$$Read\ throughput, T_R = \frac{T_{RD}}{(T_{TS})} \quad (4)$$

where,

T_{RD} - Total Read Operations

T_{TS}- Total time in seconds

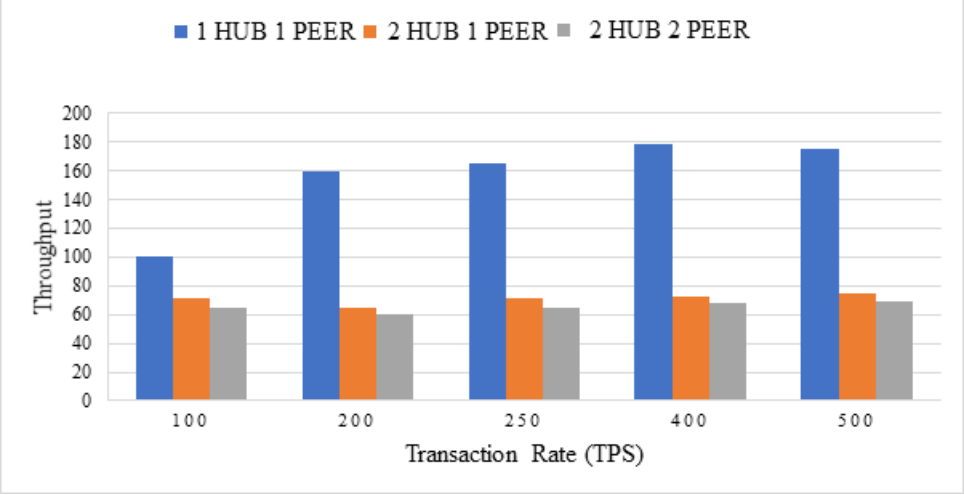

Figure 6. Read throughput

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

The second phase of the experiment deals with optimization of the entire system. Here various measurements have been taken by varying the measurement of block creation time in hyperledger fabric of our blockchain system.

Figure 7 shows the average transaction latency with varying block time for a 2Hub-2Peer system configuration in which 2000 transactions per epoch with the transaction rate of 100, 200, 250, 400, 500 transactions per second for transaction in write mode. It is observed from the Figure 7 that when the block time is increased from half a second i.e., 500 ms to 2 s, for the transaction of 100, the average transaction latency has reduced from 41 seconds to 27 seconds. Also, for the transaction of 500, the average transaction latency has reduced from 43 seconds to 36 seconds. This is the remarkable performance of the proposed system than the existing default hyperledger fabric.

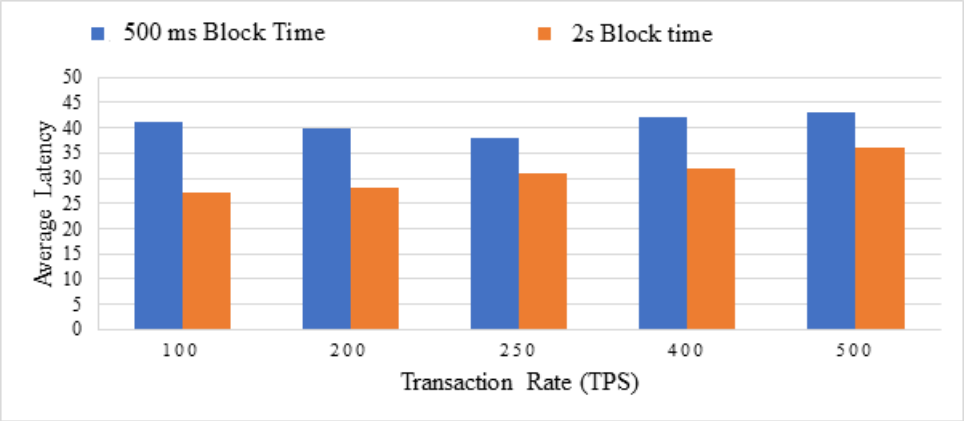

Figure 7. Average Transaction Latency with varying block time

Figure8 shows the transaction throughput with varying block time for a 2Hub-2Peer system configuration in which 2000 transactions per epoch with the transaction rate of 100, 200, 250, 400, 500 transactions per second for transaction in write mode. It is observed from the Figure8 that when the block time is increased from half a second i.e., 500 ms to 2 s, for the transaction of 100, the transaction throughput has increased from 16 to 24. Also, for the transaction of 400, the transaction throughput has increased from 17 to 24. It is observed that the proposed system gives better transaction throughput, and it has the better success rate of the transaction by varying the block time.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

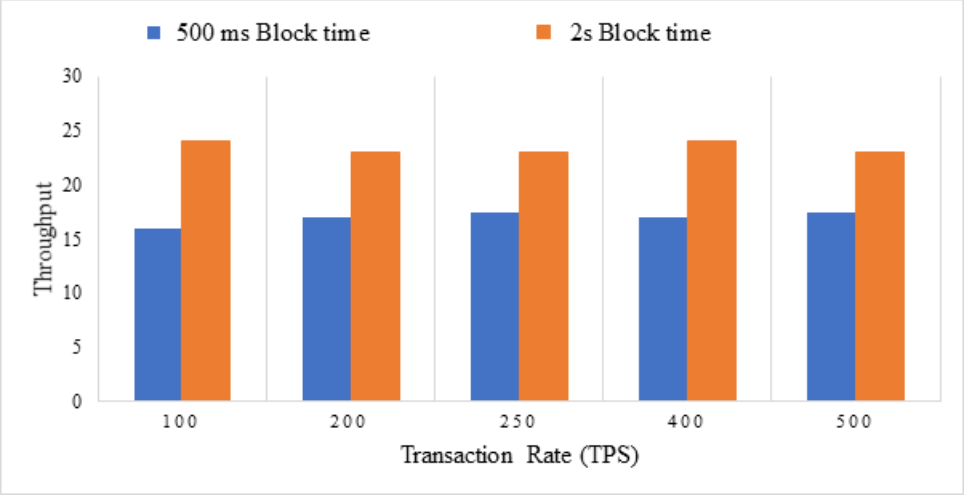

Figure 8. Transaction throughput with varying block time

To read the data from our system we have taken five epochs for our experiment and we must change the transaction mode from write mode to read mode. Figure 9 shows the average read transaction latency with varying block time for a 2Hub-2Peer system configuration in which 2000 transactions per epoch with the transaction rate of 100, 200, 250, 400, 500 transactions per second for transaction in write mode. The average read latency for the proposed system for 100 transactions per sec, has reduced from 6 s to 3 sec and for 250 transactions per sec, it has reduced from 8 s to 5 s. Also, in Figure 10 the read throughput with varying block time is shown. Here the read throughput has better performance for the modified block time. Thus, from the results obtained we can observe that the modified blockchain has the optimum performance with varying block time.

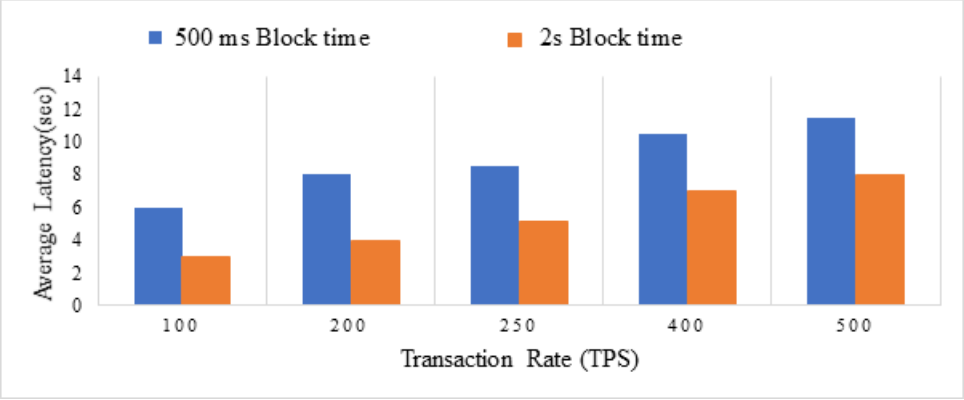

Figure 9. Average Read Transaction Latency with varying block time

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

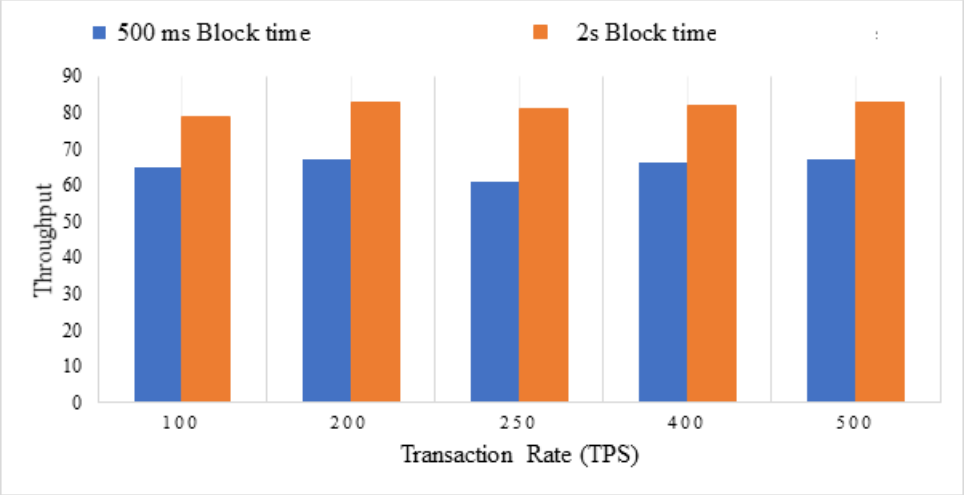

Figure 10. Read Throughput with varying block time

Finally, the average latency for the proposed smart contract process that includes Create, Issue and Revoke is shown in Figure 11. for the transaction of single database. Here we can observe that for create transaction has more delay than the issue transaction and revoke transaction is higher than the other two transactions. But we can observe that the delay between all three transaction is not having a huge value to complete our process within an expected duration of time.

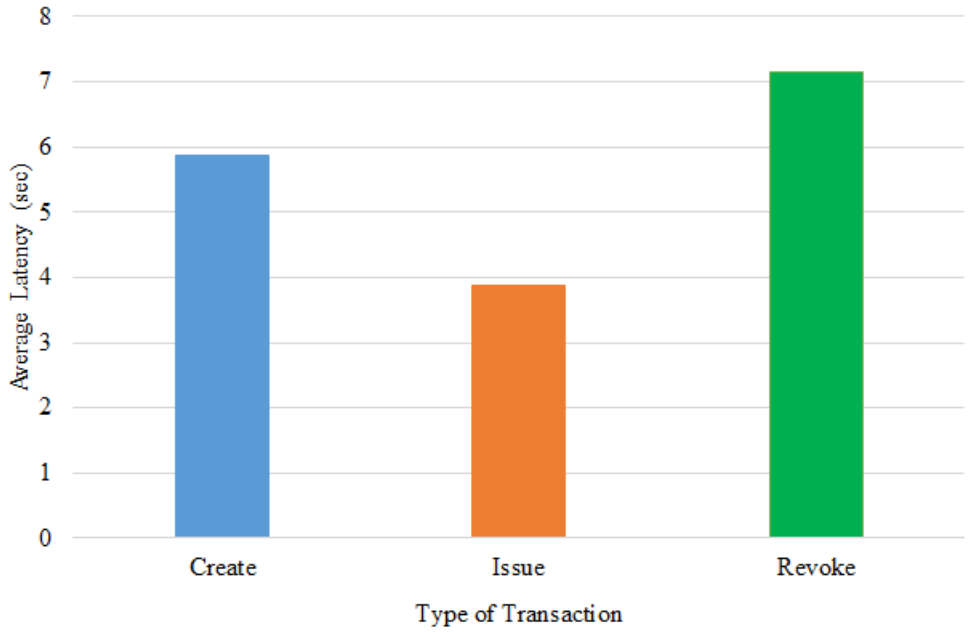

Figure 11. Average Latency

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

Conclusion

In this paper, we propose a blockchain-based approach to providing secure, reliable, decentralized, and palpable control over their image database records. The utilization of blockchain in image database systems plays a critical role in the current scenario. This will lead to automated data collection and verification processes that will not change the correct and accumulated data from different sources, provide resistance and secure data, with a lower probability of cyber-crimes. In this paper, present day challenges confronted by using the image database enterprise are discussed. We propose a system architecture and algorithm for access control strategy for individual hub to achieve privacy and security for image database in the cloud. In addition, the implementation of a proposed hyperledger fabric based on the blockchain network is discussed. The proposed work eliminates single point of failure in the system. System security is achieved through Hyperledger fabric technology as no user can change the ledger. The performance evaluation of the proposed system is completed for different scenarios by configuring the block optimization, block creation time, endorsement policy and the deferment to get the best results, as well as the proposed optimization for evaluation measurements such as latency, throughput, and network security. We outlined several limitations of the proposed solution. The proposed solution is wide-ranging enough and can be accepted for licensed or unlicensed blockchain networks.

References

[1] Nakamoto S.: Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf

[2] Hyperledger Fabric v0.6, [online] Available: http://web.archive.org/web/20160924231627/.

[3] Vukolić M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. *In: Camenisch J., Kesdoğan D. (eds) Open Problems in Network Security. iNetSec. Lecture Notes in Computer Science, (9591). Springer, Cham*. https://doi.org/10.1007/978-3-319-39028-4_9

[4] Wu, A., Zhang, Y., Zheng, X. et al.(2019). Efficient and privacy-preserving traceable attribute-based encryption in blockchain. *Ann. Telecommun*, 74, 401–411. https://doi.org/10.1007/s12243-018-00699-y

[5] Abdelghani, W., Zayani, C.A., Amous, I., Sedes, (2018). Trust evaluation model for attack detection in social internet of things. *In: Proceedings of CRiSIS*, 48–64.

[6] Li, W., Meng, Y., Kwok, L.(2014). Design of intrusion sensitivity-based trust management model for collaborative intrusion detection networks. *In: Proceedings of the 8th IFIP WG 11.11 International Conference on Trust Management (IFIPTM), Springer, Berlin*, 61–76.

[7] Zhou, Y., Liu, Y., Jiang, C. et al. (2020). An improved FOO voting scheme using blockchain. *Int. J. Inf. Secur.*,19, 303–310. https://doi.org/10.1007/s10207-019-00457-8

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4339 - 4352
Received 25 April 2021; Accepted 08 May 2021.

[8] Vora, A.V., Hegde, S.(2019). Keyword-based private searching on cloud data along with keyword association and dissociation using cuckoo filter. *Int. J. Inf. Secur.* 18, 305–319. https://doi.org/10.1007/s10207-018-0418-0

[9] P. Thakkar, S. Nathan and B. Viswanathan. (2018). Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform.*IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Milwaukee, WI*, 264-276. doi: 10.1109/MASCOTS.2018.00034.

[10] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi and A. Rindos. (2017). Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric).*IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Hong Kong,* 253-255.doi: 10.1109/SRDS.2017.36

[11] C. Gorenflo, S. Lee, L. Golab and S. Keshav. (2019). FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second.*IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South)*,455-463. doi: 10.1109/BLOC.2019.8751452

[12] Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf and S. Capkun. (2016). On the security and performance of proof of work blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 3-16.

[13] Cachin, Christian. (2016). Architecture of the hyperledger blockchain fabric. *Workshop on distributed cryptocurrencies and consensus ledgers*, 310(4).

[14] A. Sharma, F. M. Schuhknecht, D. Agrawal and J. Dittrich. (2018). How to databasify a blockchain: the case of hyperledger fabric.*arXiv preprint* arXiv:1810.13177, 2018.

[15] Membership Service Providers (MSP), [online] Available: http://hyperledger-fabric.readthedocs.io/en/release-1.1/msp.html

[16] Java SDK for Fabric Client/Application, [online] Available: https://github.com/hyperledger/fabric-sdk-java