Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 224 (2023) 163–168

Procedia Computer Science

www.elsevier.com/locate/procedia

The 20th International Conference on Mobile Systems and Pervasive Computing (MobiSPC)
August 14-16, 2023, Halifax, Nova Scotia, Canada

Secure Sharing of university Data Using Hyperledger Fabric and IPFS system

Khaoula Marhane[a,*], Fatima Taif[a], Abdelouahed Namir[a]

[a] *University HassanII Faculty of sciences Ben M'sik, Bd Commandant Driss Al Harti ,Casablanca 20670,Morocco*

Abstract

the universities across the country rely on sharing data, often sharing student information with those outside the institutions and the university often sharing the data with the her providers the services and the projects. While the general rule from education records cannot be disclosed a anyone. In this paper we proposed hyperledger fabric in same university for connected all faculty and knowledge sharing with we use the InterPlanetary File System (IPFS) for the storage of tendering document.

Keywords: Blockchain, Hyperledger Fabric, Secure Sharing data, IPFS

1. Introduction

Hyperledger Fabric is a 'permissioned' blockchain architecture, providing a consistent distributed ledger, shared by a set of 'peers.' As with every blockchain architecture, the core principle of Hyperledger Fabric is that all the peers must have the same view of the shared ledger, making it challenging to support private data for the different peers. Extending Hyperledger Fabric to support private data (that can influence transactions) would open the door to many exciting new applications, in areas from healthcare to commerce, insurance, finance, and more. In This paper we use

[*] Corresponding author.
E-mail address: khaoulami@gmail.com

10.1016/j.procs.2023.09.024

hyperledger Fabric for defines how members of the University community can secure share public or private unit record data and or aggregate-level administrative data with University faculty and researchers. This procedure applies to all providers for university, including individuals and units.

2. BACKGROUND

2.1. Related Work

The authors [1] [2] discussed the possible use of blockchain in various education related applications such as management of school records, tracking of school assets, management of student privacy, parental opt-in/opt-out permissions, and distribution of public funds or private grants. In [3], authors presented the use of blocks to store assignments, awards, research works, etc. However, the paper does not propose any architecture or implementation strategy. The paper [4] proposed a mobile application to store and verify student certificates using Hyperledger (permissioned) blockchain. Records are stored encrypted in order to guarantee privacy. Authors compared previous existing works with their prototype in terms of on-chain storage and scalability.

Authors in [5] put forward a blockchain framework to enable the exchange of students' registration data from school to learner to businesses (and vice versa). It makes use of a centralized database to extract learner data, which makes the architecture partially decentralized. The paper does not cover implementation details as well as experimental analysis. The work [6] is a case-study on the BlockCert which is a blockchain platform to store students' degrees and is implemented by Massachusetts Institute of Technology (MIT). Each stored credential has a unique URL which can be shared with others. Receivers of the shared URL can cross verify its authenticity by visiting the official website and passing that URL as an argument. Authors in [7] presented a blockchain-based architecture to store educational records on the blockchain. The work suggests that storing educational records on blockchain reduces the cost of storage as compared to that encountered with cloud storage. Privacy is obtained via the management of access control in the smart contracts and requires secure storage at the different database providers. However, the work does not carry any implementation nor any test-based result.

2.2. Blockchain

A blockchain is a continually evolving, tamper-evident, shared digital ledger [8]. It holds the records of the transactions such as the exchange of assets or data between the peers in a public or private peer-to-peer network. The ledger is shared, replicated, and synchronized among the member nodes in the network. This ledger holds the records permanently in a sequential chain of cryptographic hash-linked blocks.

Without the involvement of a central authority or third-party mediator, the participant nodes in the blockchain network govern and agree by consensus on the updates to the records in the ledger. These records cannot be altered or reversed unless the change is agreed by all members of the network in a subsequent transaction.

Consensus mechanisms in blockchains offer the benefits of a consolidated and consistent dataset with reduced errors, near-real-time reference data, and the flexibility for participants to change the descriptions of the assets they own. Moreover, none of the participating members own the source of origin for information contained in the shared ledger. The blockchain leads to increased trust and integrity in the flow of transaction information among the participating nodes [9].

2.3. Hyperledger Fabric

Hyperledger Fabric [10] is a distributed ledger by IBM and Linux foundation. Its modular architecture delivers a high degree of confidentiality, resiliency, flexibility, and scalability. The Hyperledger project was started in 2015 and launched in mid-2017. The Hyperledger Fabric is a private and permissioned blockchain, in which identities of all the participants are known. It is designed to support the pluggable implementation of different components to support complexities that exist across ecosystems.

Fabric supports modular consensus protocols, which allows the system to tailor to particular use cases and trust models. Hyperledger Fabric can store data in multiple formats, and it is also the first blockchain system that runs distributed applications written in standard, general-purpose programming languages, without systemic dependency on a native cryptocurrency [11].

2.4. Transaction Life Cycle in Fabric

Hperledger Fabric employs the execute-order-validate-and-commit transaction model. Figure 1 shows the transaction flow in Hperledger Fabric platform.

1.Initiation of transaction: The client is the initiator of the transaction. Initially, a request proposal is created to invoke a chaincode function. Next, this proposal is signed by the client and submitted to the channel on which the chaincode is deployed. As per the policy of endorsement regarding chaincode, the client expects a number of endorsements to receive.

2. Execution of transaction: A client submits a signed transaction to the endorsing peers. Each endorsing peer verifies if the client is authorized to invoke the transaction, then speculatively executes the transaction against its local blockchain state. This process is done in parallel without coordination among endorsing peers. Output of the execution, which consists of a read set and a write set, is used to create an endorsement message. The peer signs the endorsement and sends it back to the client.

3. ordering requests: A client receives all the endorsements and then examines, compares, and verifies whether it has fulfilled all the requirements according to the endorsement and policy of the chaincode. For a read operation, the client does not send an ordering request. If the request is for a chaincode invocation, i.e., write, the endorsements are consolidated into a transaction and submitted to the orderer by the peer. The transaction and order are then verified by the orderer according to the channel.

4.Transaction validation and commit: The orderer delivers all ordered transactions within blocks to all peers on the channel. According to the endorsement policy, the transaction is verified by the peers, and if all the checks are correct, then the peers add the corresponding block to the ledger. It is mandatory for all the peers to commit (commit peer) the transaction. The endorsement can be done by only a particular subset of peers in the channel, and these peers are known as endorsing peers.

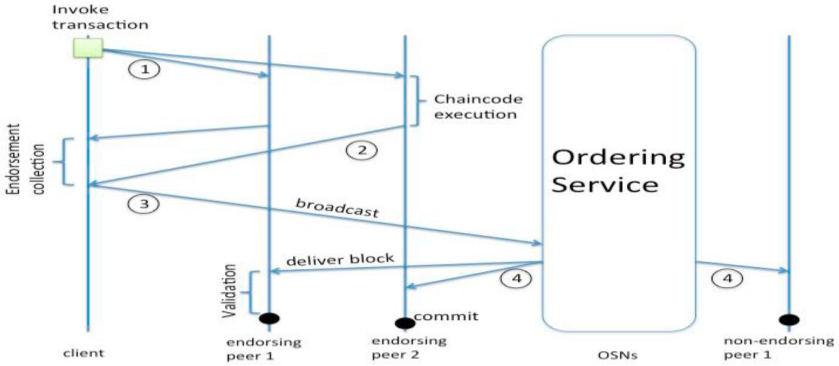

Fig. 1. Transaction life cycle in Fabric

3. PROPOSED SCHEME

3.1. System Architecture

Many universities that use private blockchain technologies use it for features like security, high-availability, data-immutability and decentralized network. Any blockchain framework is suitable only for small data sets. The dissemination of large data will create a lag on network. This lag may not be acceptable in a universities system. We

need a solution to this problem.
The proposed Model provides a solution for exchanging digital tendering documents of large data inter faculties' member in university over permissioned blockchains with we use IPFS.
The proposed framework has four main functionalities:
1) creation the hyperledger Fabric system.
2) The ability to upload digital documents to IPFS.
3) Send and receive documents.
4) Maintaining the security standards; Confidentiality, Integrity

IPFS is a file storage protocol which is decentralized, that enables the storage, access and security of files over a distributed file system. A cryptographic hash is created for every file. The files are stored in nodes, whose indexing is done such that each file can be accessed through the node which prevents duplication.

In this paper, we consider university network in place, i.e. all faculty units are connected and knowledge sharing over permissioned blockchains with we use IPFS for the storage of tendering document.

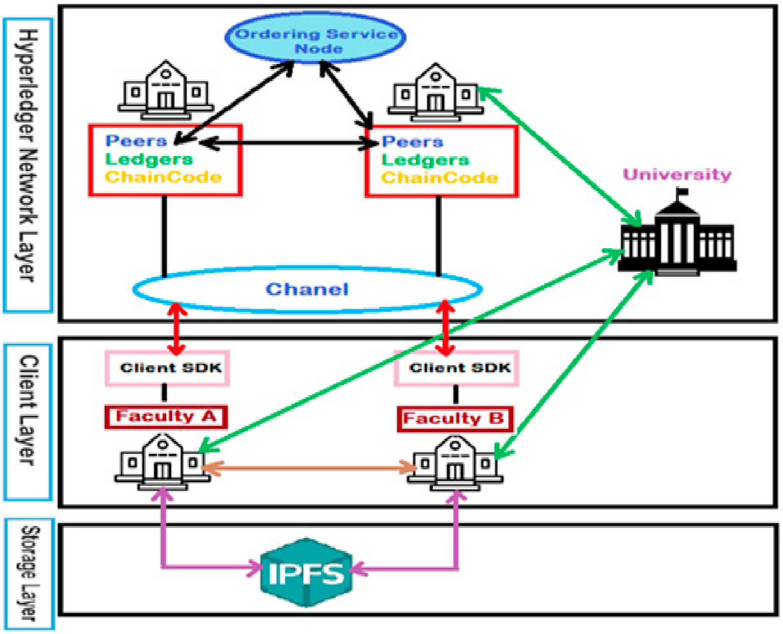

Fig. 2. hyperledger Fabric network system proposed with IPFS system

1- Hyperledger Network Layer: This includes Peers, Ordering Service Node, Channels, and Certificate Authority (CA). The CA is responsible for issuing public and private keys and digital certificates. Administrators and Peers must be authenticated by the CA to become part of the blockchain network. The Channel is a private blockchain built based on data isolation and confidentiality. The data in the channel (e.g., Ledger information and member information) is known only to the members in the channel, The Ordering Service Node only sorts and packs the transactions received in the channel and does not verify the legitimacy of the transactions, and then broadcasts the packaged transactions to all Peers in the channel. Peers are a network entity that maintains the ledger and runs the Chaincode to do read and write operations on the ledger.
2- Client Layer: Each faculty in the education IoT has an administrator who is responsible for interacting with the Hyperledger Blockchain Network. The administrator is connected to the blockchain network through the Client, which uses the SDK (Software Development Kit) to interact with the blockchain network and can access the ledger through Peers using the Chaincode, and the administrator needs to register through CA to participate in transactions in the system.
3- Storage Layer: Faculty that join the same channel will also join the channel's IPFS network, which is a distributed file system for storing and sharing data, and generating a hash address for storing data, which is a key component.

The administrator stores the data encrypted using AES in IPFS while constructing a Keyword-index table of the hash addresses returned by IPFS to upload to the blockchain, which greatly increases the scalability of the system. Moreover, each data transaction carries a timestamp and is permanently stored in the blockchain.

Data sharing among education IoT is realized through Channel, and different faculties; so all parties can join the same Channel for data sharing. the workflow is shown in Figure 3.

(1)Registered; (2)Encrypted data; (3)hash address; (4)Table;(5)-querying; (6)Table; (7)Request message;(8)Required message; (9)Decryption.

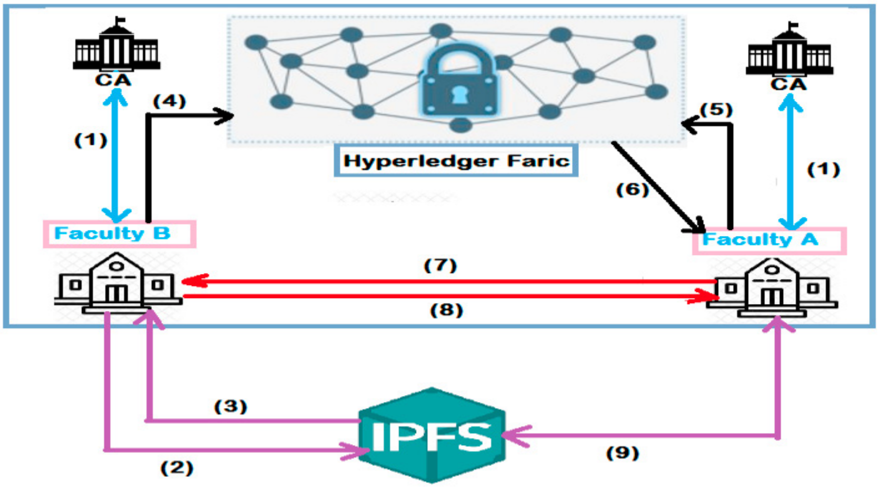

Fig. 3. Enterprise data sharing process within Channel.

4. Conclusion

This paper proposes a distributed data sharing system based on the blockchain technology in the universities. we proposed hyperledger Fabric system and IPFS technology, it provides a mixed, reliable and distributed paper we use hyperledger Fabric and IPFS for defines how members of the University community can secure share public or private unit record data and or aggregate-level administrative data with University faculty and researchers.

Now a days more research based on different applications of blockchain and IPFS are going on. For example in medical field, a healthcare record management system which will definitely useful.

References

[1] In Albeanu, 2017, Blockchain technology and education On Virtual Learning (2017), p. 271

[2] Chen G., Xu B., Lu M., Chen N.-S. Exploring blockchain technology and its potential applications for education

[3] Sharples M., Domingue J.The blockchain and kudos: A distributed system for educational record, reputation and reward European conference on technology enhanced learning, Springer (2016)

[4] Arenas R., Fernandez P.Credenceledger: a permissioned blockchain for verifiable academic credentials 2018 IEEE international conference on engineering, technology and innovation (ICE/ITMC), IEEE (2018)

[5] Andreev, O., & Daskalov, H. (2018). A framework for managing student data through blockchain. In Proceedings of X international scientific conference e-governance and e-communications.

[6] Young A., Verhulst S. Creating immutable, stackable credentials through Blockchain at MIT GOVLAB (2018)

[7] Han, M., Li, Z., He, J., Wu, D., Xie, Y., & Baba, A. (2018). A novel blockchain-based education records verification solution. In Proceedings of the 19th annual SIG conference on information technology education (pp. 178–183).

[8] Till B.M., Peters A.W., Afshar S., Meara J.G.From blockchain technology to global health equity: can cryptocurrencies finance universal health coverage? BMJ Global Health, 2 (4) (2017), Article e000570

[9] ZhaoQ. et al.Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systemsInformation Processing & Management (2020)

[10]Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[11]M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science,