How to Cite:
Kumutha, K., Jayalakshmi, S., & SriPriya, P. (2022). Data security mechanism of hyperledger fabric and its application in academic documents verification system. *International Journal of Health Sciences*, *6*(S3), 4394–4403.
https://doi.org/10.53730/ijhs.v6nS3.6821

Data security mechanism of hyperledger fabric and its application in academic documents verification system

Kumutha K.
Assistant Professor in the Department of Computer Applications, Tagore College of Arts and Science, Chrome pet, Chennai
Email: kumutha.k@gmail.com

Dr. S. Jayalakshmi
Associate Professor at Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College (VTMT), Chennai, in the Department of Computer Science and Engineering
Email: jayalakshmi.research@gmail.com

Dr. P. SriPriya
Professor in the Department of Computer Applications, Vels Institute of Science, Technology and Advanced studies (VISTAS), Pallavaram, and Chennai
Email: Sri.scs@velsuniv.ac.in

***Abstract*---**Blockchain technology ensures that data is tamper-proof, traceable, and trustworthy. This article introduces a well-known blockchain technology implementation—Hyperledger Fabric. The basic framework and privacy protection mechanisms of Hyperledger Fabric such as certificate authority, channel, Private Data Collection, etc. are described. As an example, a specific business scenario of an academic documents verification system m is figured out. And accordingly, some design details about how to apply these privacy protection mechanisms are described. The information of each enterprise in the blockchain needs to be shared, in this process, the privacy of ADVs needs to be protected, and we need an algorithm to protect privacy. Data sharing is not implemented in the traditional academic documents verification system. Therefore, the privacy protection requirements are different from those in the academic documents verification system based on blockchain. Therefore, the local database should also establish a corresponding hash value of the private transaction data and implement mapping with the private database on the chain to achieve traceability based on the same hash value.

***Keywords*---**blockchain, distributed ledger technology, data security, academic documents verification, hyperledger fabric.

Introduction

This page Blockchain technology increases the reliability and sharing of transaction data, but also increases the risk of exposing a company's business data. In fact, the company doesn't want its competitors to know information such as prices and costs, so how to effectively protect different types of data with blockchain network systems is an important issue. On the one hand, academic document verification systems require proof of verification to solve the problem of issuing fake certificates and eliminate the high cost of the verification process. Blockchain technology can make transaction data irreversible and traceable, reducing credit risk. Academic institutions, on the other hand, often need ADV business information when conducting credit assessments for ADV based on blockchain technology. At the same time, it is necessary to share the information of each company on the blockchain. This process needs to protect the privacy of ADV and requires a privacy protection algorithm. Data sharing is not implemented in the traditional scholarly document review process. Therefore, data protection requirements are different from blockchain-based document validation requirements. Traditional document validation business processes use several privacy protection methods, such as authorization codes and randomized read access control. Benefits of these methods include enhanced risk identification of document validation networks and authentication of a smaller set of tags. Guaranteeing privacy, reducing trust issues between supply chain owners and tag makers, reducing computational and communication overhead, and reducing computational overhead. Hyperledger Fabric is a well-known implementation of blockchain technology. This white paper describes the data protection mechanism and its application in academic document review scenarios.

Related Work

Blockchain

Blockchain is a system that does not rely on the trust of electronic transactions. This shows how the double payment problem can be ended. Use peer-to-peer networks to resolve the history of each transaction and later record the history of each transaction. Broadcasting to an intruder is computationally impossible if the legitimate end of the system controls most of the CPU power. Due to its decentralized and temperamental validation characteristics, it has numerous applications such as decentralized cryptocurrencies, cross-border payments, blockchain Internet of Things (IoT), supply chain management, all ledgers, and more.

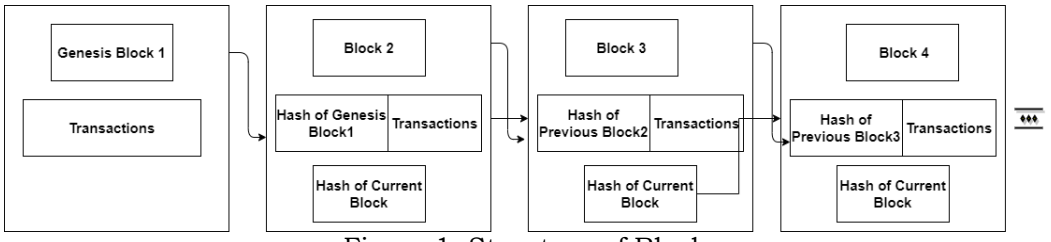

Figure 1. Structure of Block

The Academic certificates issued by educational institutions are important documents for students and graduates. Proof of Education Certificate and eligible to apply for higher studies and employment. Advances in information technology and the availability of low-cost and high-cost equipment enable fraudulent access to important documents such as identity cards, certificates, and passports. Traditional document verification is expensive and the time-consuming process of human intervention can lead to academic credential fraud (Macrinici, D., Cartofeanu, C., Gao, S., 2018), The trends in information technology in recent years become solutions for all the problems such as data protection, consistency, and reliability are more important than ever. The job aspirant requires educational certificates to be verified during interviews and higher studies. In some situations, the employer can take a longer time to verify the originality of the certificate, during this verification, candidates have to wait for more days to get the offer letter, overall it consumes the time of job aspirants. In this paper, the goal is to propose a potential solution for academic certificate issuing and verification using blockchain technology (Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen., 2017).

Hyperledger fabric

Results The Linux Foundation established the Hyperledger project in 2015 to advance blockchain technology across industries. If Hyperledger Fabric is different from other blockchain systems, it is privately allowed. Instead of an open and unauthorized system that allows unknown identities to join the network (requires protocols such as Proof of Work to validate transactions and protect the network), members of the Hyperledger Fabric network are Trusted Membership Services. Register through the Provider (MSP). Hyperledger Fabric also offers several pluggable options. Ledger data can be stored in multiple formats, the consensus mechanism can be switched, and various MSPs are supported. Hyperledger Fabric also provides the ability to create channels, allowing groups of participants to create individual ledgers.

Data security mechanism

The privateness safety measures of Hyperledger Fabric consist of the subsequent 4 aspects: Firstly, uneven cryptography and zero-information evidence separate the transaction information from on-chain records, protective privateness from the underlying algorithm. Secondly, the virtual certificates control provider ensures the legitimacy of the organization at the blockchain. Thirdly, the layout of multi-channel separates the statistics among one-of-a-kind channels. Finally, privateness information series in addition satisfies the want for the isolation of privateness information among one-of-a-kind agencies in the equal channel. In

the above measures, the two maximum distinct techniques are channel and privateness information series. The channel is devoted to blockchain privateness safety, permitting the information at the channel to be remoted separately. The peer at the equal channel stocks a ledger, the transaction peer wishes to gain the popularity of the channel earlier than it is able to be a part of the channel and transact with others.

The blockchain transaction procedure entails privateness. Accordingly, Figure.2 suggests this procedure. 1. The University Issue the documents and submits the provide request to name the chain code characteristic to the endorsement peer of the non-public information set authorization, and the non-public information is dispatched via the provisional area with inside the provide. 2. The endorsement peer simulates the documents and verify the non-public information in a neighborhood transient repository with inside the peer. The endorsement peer disseminates the non-public information to the legal peer through the gossip protocol. 3. The endorsement peer returns the general public information, which include the hash value of the non-public information key-fee pair, to the employers. 4. The owner of the documents utility submits the documents to the sorting provider peer, and the sorting end result is sent to every block. These blocks containing hash values are allotted to all peers. Each peer above the channel can use the hash of the non-public information to affirm the transaction without understanding the precise non-public information. 5. When filing a block, the legal peer can use the gathering coverage to decide if it's far legal to view non-public information. (Dinesh Kumar K, Komathy K, Manoj Kumar D.S., 2019).

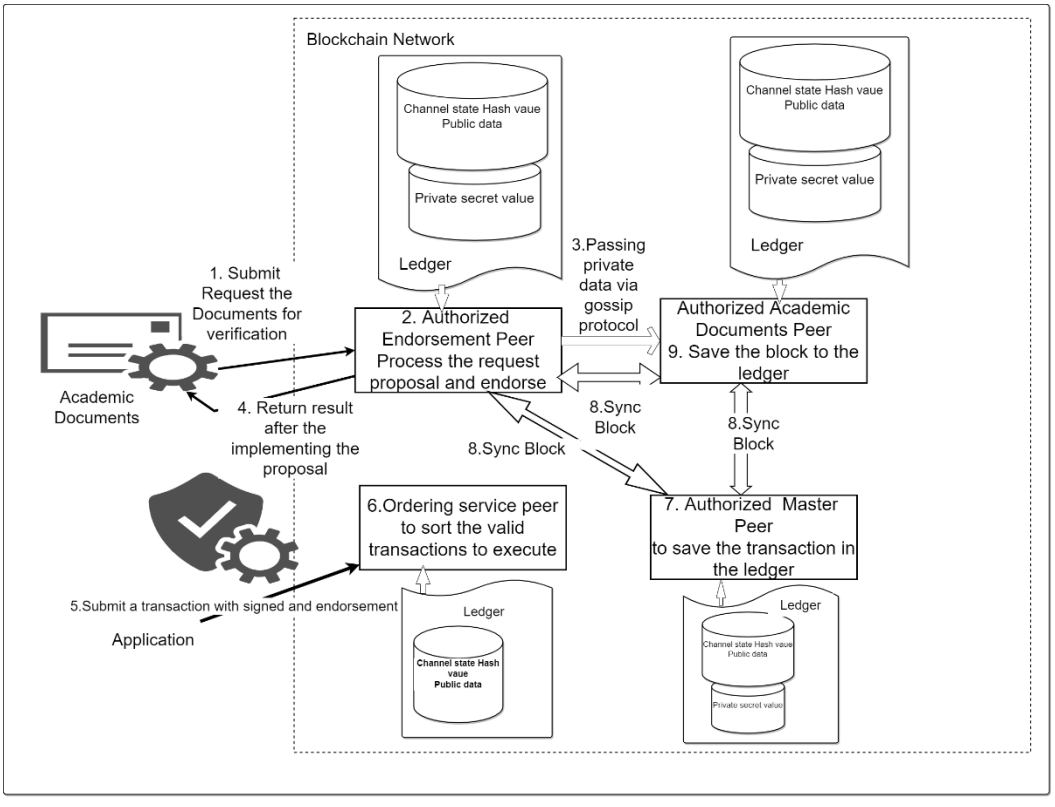

Figure 2. *Two Placement processes involve the sharing Academic Documents between ADV A and ADV B.*

The authorization peer will test the neighborhood transient information keep first of all to decide if it has obtained non-public information while the chain code is endorsed. If not, they'll try to gain non-public information from different peers. It then verifies that the hash of the non-public information and the hash with inside the block's public statistics are constant and commits the transaction and the block. When a member of a non-public information series stocks non-public information with different agencies, including while a member of the gathering has a dispute or in the event that they need to switch the asset to a 3rd celebration. The third-celebration can calculate the hash of the non-public information and test that the hash fee is constant with the hash at the channel ledger, accordingly proving the lifestyles of the transaction. For very non-public information, after a duration of time, the organization that stocks the information hopes or requests for well-timed elimination of the information keep for coverage reasons, leaving simplest the hash of the information as proof that the transaction can't be tampered with. In a few cases, non-public information wishes to be saved with inside the peer's privateness database till it is able to be replicated to a database outdoor of the blockchain. This information wishes to be saved with inside the peer till the chaincode academic procedure is used.

Applications in Academic documents verification

In order to explain the packages of the privateness safety mechanism of Hyperledger in Academic files verification. As an example, Figure. 3 indicates a particular Academic files verification situation. There is a central university, three educational institutions AIs (better schooling institutes), placement establishments, and authorities departments with inside the educational files verification system. Suppose there are placement companies processes, the authorities sector (O1), the center educational institutes (O2), the e-studying group A (O3), the ADV A (O4) and the ADV B (O5) belong to the primary placement Fig. five); authorities departments (O1), center educational institutes(O2), e-studying establishments B (O3), ADV (O4) and ADV (O5) belong to the second one placement commercial enterprise manner (Its Fig. five placement commercial enterprise manner situation data propagation direction is indicated with the aid of using a dotted line).

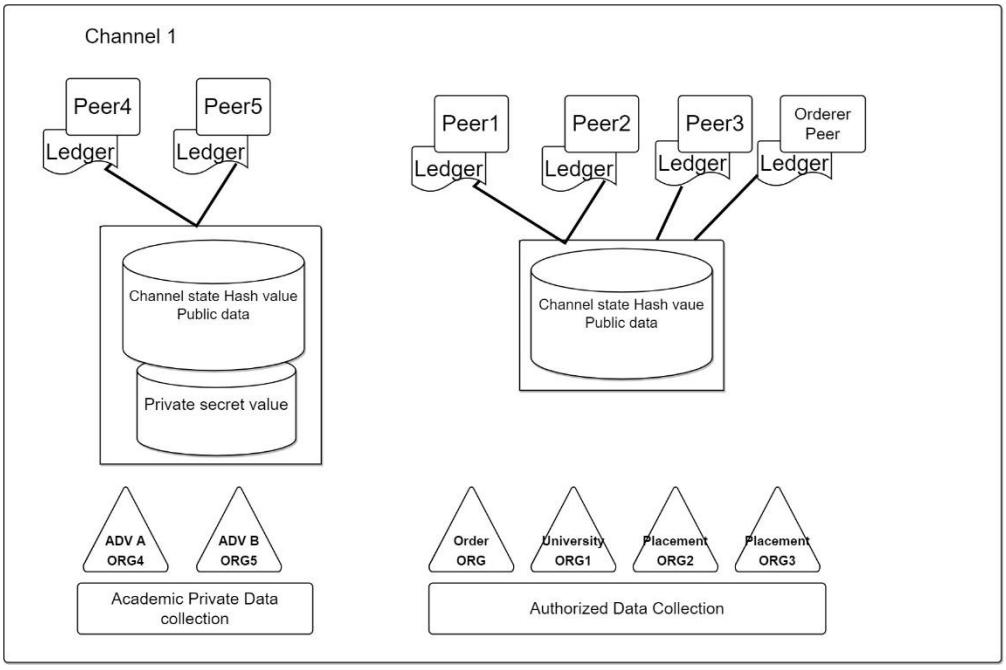

Figure 3. Two business processes involve the transaction of information between ADV and the main institute

In Academic files verification, because of the lengthy verification system and lots of companies involved, the subsequent necessities need to be met for privateness safety. The academic situation is defined as follows: All the above institutes have entered the blockchain community. There are placement enterprise approaches. In the primary placement enterprise system, transactions arise ADV B and ADV A, different transactions arise among ADV A and the middle instructional establishments. ADV B collaborating within side the files verification did now no longer get hold of the development permission after receiving the educational files verification request order of ADV A, and ADV A did now no longer get hold of the development permission from the middle instructional institutes. ADV A and ADV B wish to get authenticity via applicable virtual signature and hash keys gain from instructional organization A, to confirm the files for issuing. In the second one placement enterprise system, ADV C additionally offers with ADV A., ADV B, and ADV C are a part of ADV A, and there's an aggressive dating among ADV B and ADV C. ADV A and the middle instructional institutes generate instructional files for the scholars for his or her achievements, and educational organization B offers authenticity offerings for the second one placement enterprise system to confirm the originality of the files. In summary, the subsequent privateness safety necessities exist in those companies at the blockchain:

- Documents sharing is secure and reliable
- ADV B does now no longer need any transaction conduct among itself and ADV A to be acknowledged through ADV C.
- ADV B does now no longer need files info associated with privateness to be exceeded to placement organization A

- The middle personal records of every unit desires to be absolutely personal.

Privacy safety layout of c institutes. In reaction to the above privateness safety necessities, the verifications privateness safety layout of the educational files verification primarily based totally on Hyperledger Fabric is as follows:

- All companies becoming a member of the blockchain need to be authenticated on the CA to save you unlawful companies from becoming a member of the community to scouse borrow person privateness. The viewing rights of the personal records may be similarly subdivided. In the situation of the league chain served through the Hyperledger, many organizational relationships at the channel are complex. Therefore, privateness records of various levels of encryption may be given at exceptional degrees consistent with the character of the transaction pastime and the socio-financial dating among the companies. However, competition won't be capable of have complete get admission to the applicable records of this transaction.
- Establish exceptional channels for exceptional enterprise approaches. In this case, the two placement enterprise approaches shape channels to make certain entire separation of records among ADV C and ADV B. Based at the channel fashioned through the primary placement enterprise system, set up a personal records set which include ADV B and ADV A, and a personal records set which include ADV A and middle instructional institutes, and additionally within side the second placement enterprise system. Establishing comparable collections of personal records to make certain that personal records is handiest disseminated to each events to files verification. Other records is supplied to different instructional establishments for chance evaluation and supplied to authorities control for statistical and regulatory purposes.
- For the middle personal records inside every company, the company plays uneven encryption and transmits hash of records to the blockchain. This technique ought to additionally be a part of the Hyperledger Fabric's privateness safety mechanism. In addition, the garage version for personal records ought to be similarly designed (Dinesh Kumar K, Senthil P, Manoj Kumar D.S.,2020).

At present, Hyperledger's garage of personal records is saved within side the privateness database of the peer. (E. Androulaki et al., 2018). However, this technique makes it not possible to absolutely take advantage of the traceability of the blockchain, and the very last traceability is handiest the hash of the files, which cannot be tested at the chain. Therefore, the nearby database ought to additionally set up a corresponding hash cost of the personal transaction records and put in force mapping with the personal database at the chain to attain traceability primarily based totally at the equal hash cost. The records may be similarly encrypted consistent with the attributes of various login customers after the privateness records is saved within side the database of the company. Even if the equal purchaser is of the equal company, the person that manipulates it can be exceptional, so it's far essential to encrypt the records to exceptional levels consistent with the attributes of the login person.

For example, an administrator in an company has the proper to view all the records within side the peer database, and traffic within side the company can handiest see the encrypted records. The permissions of various friends within side the equal company to view records ought to additionally be exceptional. This is a development path of the privateness safety layout on Hyperledger Based on this, the privateness records safety mechanism of the Hyperledger Fabric protects the personal records within side the instructional files verification.

The privateness records series layout of ADV A and ADV B is proven in Figure. 3. compared with the conventional verification system, the blockchain-primarily based totally verification approach realizes the allotted garage of the ledger. Each peer shares the equal ledger regionally in order that the ledger is authenticated through a couple of events. It is tough to tamper with the ledger. Therefore, this manner achieves decentralization. Hyperledger Fabric achieves the isolation of personal records via the approach of personal records series and channel. While the conventional verification approach protects privateness through putting the login password, which has protection risks, and the records isn't always authenticated through a couple of events. The ledger isn't always true. Correspondingly, Table 1 lists the variations among blockchain-primarily based totally verification approach and conventional verification.

Table 1
Difference Between Blockchain Based Documents verrifiation and Traditiioan Method

Blockchain based verification	Traditional verification
Decentralized distributed ledger each peer has the same ledger	Centralized storage each participant only save its own
Traceable each documents issuing and sharing is recorded	Untraceable whether the documents is recordable and sharing
Documents cannot be tampered after multiple verification	Each participant is able to modify their own documents
Channel and Private data collection in HLF are designed to preserve the data	Login password is used to protect the user data
Documents sharing and data security are both implemented	Documents sharing is not implemented

Conclusion

The blockchain has a notably quick improvement history, it become handiest used as a generation to help virtual forex bitcoin within side the very beginning. At present, blockchain generation has been separated from Bitcoin and has been carried out in lots of fields which include finance, trade, credit, the Internet of things, and the sharing economy. In the face of complicated eventualities which include the privateness safety demanding situations of the instructional files verification scenario, Hyperledger Fabric gives a number of solutions. A bendy aggregate of those privateness safety mechanisms can meet numerous privateness safety desires. Academic files verification includes distinct participants, with a huge type of eventualities and complicated enterprise

processes. This article especially introduces the privateness safety mechanism of the Hyperledger Fabric and makes use of an educational files verification case to explain. Our subsequent paintings might be to investigate the particular privateness safety desires of various instructional files verification eventualities and enhance the privateness safety mechanism of the Hyperledger Fabric, which include putting the viewing permission of hierarchical subdivision, enhancing the privateness facts garage mode, etc.

References

S. Nakamoto,(2017). Bitcoin: A Peer-to-Peer Electronic Cash System, http://Www.Bitcoin.Org, p. 9, 2008.

M. Valenta and P. Sandner, Comparison of Ethereum, Hyperledger Fabric and Corda

Macrinici, D., Cartofeanu, C., Gao, S., Smart Contract Applications within Blockchain, Telematics and Informatics, journal https://doi.org/10.1016/j.tele.2018.10.004.

Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, (2017).Blockchain and Smart Contract for Digital Certificate, Proceedings of IEEE International Conference on Applied System Innovation.

online Available: https://www.blockcerts.org.

Dinesh Kumar K, Komathy K, Manoj Kumar D.S ,(2019). Blockchain Technologies in financial sectors and industries, International Journal of Scientific and Technology Research Volume 8, Issue 11, pp. 942 -946.

Benyuan He, An Empirical Study of Online Shopping Using Blockchain Technology, Department of Distribution Management, Takming University

Zhenzhi Qiu, (2017).Digital certificate for a painting based on blockchain technology, Department of

Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C.,.

W. Diffie, P. C. Van Oorschot, M. J. Wiener, (1992).Authentication and authenticated key exchanges, Designs, Codes and cryptography 2(2), 107-125 .

Ethereum project,(2018), https://github.com/ethereum/wiki/wiki/ White-Paper .

MIT Media Lab,(2016),What we learned from designing an academic certificates system on the blockchain,Medium, no. December.

E. Androulaki et al.,(2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchain,no. 1. Source: Adapted from: https://commons.wikimedia.org/wiki/File:Hash_function.svg

Jerril Gilda, Maanav Mehrotra ,(2018).Blockchain for Student Data Privacy and Consent International Conference, IEEEXplore.ieee.org.

Online,(2020).https://www.indiatoday.in/education-today/featurephilia/story/how-students-and- employers- canspot-and-eliminate-fake-degrees-1725931-2020-09-27

Dinesh Kumar K, Senthil P, Manoj Kumar D.S,(2020). Educational Certificate Verification System Using Blockchain ,international journal of scientific & technology research volume 9, issue 03, march 2020 ISSN 2277-8616 82 ijstr©2020

S.Jayalakshmi ,K.Kumutha,(2021). Impact of the Blockchain on Academic Certificate Verification System-Review" ,EAI journal,e35, http://dx.doi.org/10.4108/eai.29-4-2021.169426.

IEEE Pervasive Computer 13(2):52–60 Belle I (2017) The architecture, engineering and construction industry and blockchain technology. Digital Culture 2017:279–284

Cachin C (2016) Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol 2016.

Iansiti M, Lakhani KR (2017) . https://hyperledgerfabric.readthedocs.io/en/release-1.2/. Accessed 5 Sept 2018 The truth about blockchain.