A Private Blockchain-based Distributed Ledger Storage Structure for Enhancing Data Security of Academic Documents

Conference Paper · March 2023

CITATIONS
0

READS
204

2 authors, including:

Kumutha Parthiban

7 PUBLICATIONS **45** CITATIONS

SEE PROFILE

Grenze International Journal of Engineering and Technology, Jan Issue

A Private Blockchain-based Distributed Ledger Storage Structure for Enhancing Data Security of Academic Documents

Kumutha.K[1], Dr.S.Jayalakshmi[2] and Dr.Y.Kalpana[3]
[1]Research scholar, VISTAS, Assistant Professor, Department of computer Applications, Tagore College of Arts and Science, Chennai, India
Email: kumutha.k@hotmail.com
[2]Associate Professor, Department of computer Applications, VIMT, Chennai, India
[3]Professor, Department of Information Technology, VISTAS, Chennai, India
Email: kalpana.scs@velsuniv.ac.in

***Abstract*—Initially the Blockchain technology was used to implement different digital currencies. Nowadays blockchain is adopted as a common technology to be used in various business applications. Blockchain based solutions have underlying features like security, tamper proof, transparency and consensus. Apart from that, history of data can be maintained on a blockchain network that can be retrieved from any place and at any time. Blockchain provides immutability which is a solution to avoid faking of certificates. This Paper presents a blockchain based solution to issue certificates and prevent fake certification by using digital signature to enhance the data security long with proof of validity smart contract is used to access the blockchain network with valid key. The proposed permissioned blockchain based academic certificate repository system provides and manages degree certificates as assets for educational institutes. Academic certificates and e-certificates can be securely shared and distributed by students and learning institutes through this application.**

***Index Terms*— Blockchain, Hashing, Hyperledger Fabric platform, Digital signature and Digital watermarking, Proof of Validity.**

I. INTRODUCTION

The future internet is blockchain technology. The first blockchain is Bitcoin which is introduced by Satoshi Nakamoto; it is Bitcoin that came into existence in 2009[1]. Now the Bitcoin became more popular. Bitcoin is the most popular digital money used on peer to peer network in the case of the blockchain. The features decentralized, distributed, secure and faster, transparent, and immutability are more beneficial abilities compare with the existing technologies. Data structure used in blockchain technology is like linked list data structure that preserves details of data and its transactions through a distributed ledger technology publically. The great advantage of blockchain enables most of the authors made to implement the educations system. It can store student details such as degree certificates and history of the provider and the address of the student's data in the network. The blockchain technology uses several consensus algorithms and common procedure execution through the distributed public ledger, business logic (smart contract), and cross- chain concepts. There are several blockchain development platforms are available. Each one has its own feature. This research paper

Grenze ID: 01.GIJET.9.1.541

analysis overallfeature of Ethereum and Hyperledger fabric platform and based on this suggest suited platform implement the use case. These techniques maintain a change of the data integrity by keeping the attributes of transactions such as time, space, and instantaneous multifunctional overlays with constraints such as recordable, traceable and determinable, cost and tradable procedure, etc.,

This research suggests Hyperledger fabric Framework proposes a certificate verification system to avoidthe fake and provide high level of security. And also this paper presents the proposed certificate verification system design and its process how does it support to enhance the data security by mean of digital signature and water marking technique to provide tamper proof.

II. Basic Concepts of Blockchain Technology

Blockchain is distributed ledger technology that maintains linked list database with any type of records like transactions, contracts and events. All these data are distributed to all the peers over the network which is public ledger preserved chronologically as linked list digital blocks. A blockchain technology has these features and capabilities make the distributed ledger as transparent, highly secure, publically distributed, decentralized and with maximum storage space and speed and minimum cost. Blockchain uses the technique of SHA-256 hashing method in a block as signature and considers all records, transactions are happened. A block has previous block hash which ensure the data transparent and in turns immutability. This SHA-256 hashing algorithm take any length of statements as input and always gives fixed n-digit string as output by using cryptographic hash function [5].This feature enhance the security of data stored in blockchain network.

A. Figures and Tables Hashing

A SHA-256 algorithm used in blockchain which is a small code of 256 defined length that can be used as a fingerprint for a digital document and it is part of encryption technology. A hash generator always gives unique id for any string of text. If one character in a data is changed, it will automatically create a different hash id. So it is very difficult to modify the data which is stored as block in the blockchain network. The transactions is stored as block in blockchain, where each block is secured by using this SHA-256 hashing algorithm and hash of the previous block. If one block is changed it will affect the next block due to maintaining the previous block hash. So this ensure all parties to guarantee that no one can modify the data on the blockchain.

B. Hyperledger Fabric

The Linux Foundation, which established the ecosystem in December 2015, manages Hyperledger. The framework is open source and a modular architecture is supported. Two types of modes are available on Hyperledger: the validating nodes and the non-validating nodes. The validation nodes verify transactions, manage the ledger and perform the BFT consensus protocol. It follows the execute- order-validate paradigm. IBM and Digital Asset had been the two agencies that constructed the preliminary model of Fabric [2]. It alternatively suffers from two drawbacks. First, it has lacks validated applications and secondly, lacks of skilled programmers able to use this technology.

C. How does "Blockchain" support to maintain academic Records?

This paper deals about the academic records containing students files, certificates and other details which is contains information's directly related to a student's historical academic records like year of admission, passed and receive certificates . To keep this kind of academic record in a blockchain technology gives high security and immutability of data. All the educational institute has the responsibility of keeps student's records for a long time. Blockchain based educational repository has more benefits than the existing technologies [3][4]: i) The immutable ledger technology generates chronological list of transactions in real time is very useful for verifying academic degree certificates, student complete report and maintain the students honest about their achievements[5]. ii) In real time use case, more than 600 MIT graduates of 2018 decided to get their diplomas degree as digital certificate on Blockcerts' blockchain. Therefore, the student's academic certificates will be maintained in blockchain so that in future employers can verify them at any time and from any place. This avoids students from submitting fake degrees to the employers. Finally the academic documents are managed by using blockchain technology benefits the encrypted hashing of records and makes more reliable and maintains all academic documents safe and easy to share and access[6].

III. Related Work

Initially the blockchain technology is used in development of cryptocurrency like Bitcoin but in recent years blockchain technology used in a business applications like supply chain management, identify management,

health care and educational institute to issue the certificate through blockchain to avoid the fake certificates. Blockcert Wallet is blockchain based application to issue and verify the academic records by MIT which is based on Bitcoin. It permits for instance issue the certificate after the completion of diploma degree through blockchain network virtually [7][11]. This is hyperledger based application to issues and maintained academic documents which is differ from MIT blockcerts wallet in has platform and type of blockchain. Where the smart contract (Chaincode) has been developed to control the collations among the various educational institutes to access the details in more secure and safe.[16][17]. MongoDB and couchDB used as external entities to maintain the student's details in this system by means of using intelligent contracts.

IV. ALGORITHM USED TO ENROL THE ISSUER AND VERIFY THE CERTIFICATES

This section illustrate the pseudo code to verify the proof of authenticity(Figure 8) and enhance the security of the certificates the digital water marking technique is used and stored in the Mongo DB for future referenceD. Abbreviations and Acronyms

A. Digital Signature

The proposed hyperledger based application uses digital signature and water marking algorithms to encrypt and decrypt the certificates. This RSA algorithm is computationally expensive and time consuming. The most important reason of using hash instead of data directly for signing is efficiency of the scheme. Every academic institutes and students can have public and private key Paris. The issuer and owner data are hashed and hash value and signature key are submitted to the signature algorithm to generate digital signature then this would attached with the academic certificate. These are send to the blockchain network to store the issuer details and certificate as in the encrypted form [12].

B. Proof of validity

In this proposed system used the proof of validity smart contract (chain code) is shown in figure 4 to validate the originality of the academic institutes by using membership service provider in the fabric certificate authority can issue the certificate to enroll in the blockchain network as node , each and every member of the network have two keys public and private keys and also they authenticated with digital signature, all the issuers authenticity List An[] is created when new issuer are added (An=A+An{}) after validate their signatures and key are valid by using verification algorithm. If the issuer address are same then certificate are added in that particular students MongoDB to maintained students information in off-chain mode or else create a new student and added into the blockchain network or else generate the duplicate keys error message. And also count the each student's certificate issued by the same institutes to the particular student Verify_ Count is incremented each time the same student will not receive certificate from the same academic institutions.

Chain code logic for the node Authenticity to verify the certificate

1. **Inputs: A_n{}**
2. **Verifying Authenticity_List(A_n):**
3. **On Issuing (A)**
4. **If (Addressee A_n{}):**
   A_n{}=AA_n{}
5. **Else**
   A has duplicate public Keys
6. **Rules:(A.address):**
7. **If (AA_n{} AND A has not issued the same certificate):**
   Verify count=Verifiy_count+=1
   Return (ture)
8. **Else**
   Verify_count=Verify_count is not incremented

A_n{} ->Node in the Authenticity_list
A->Verifying Authenticity
N->Node in the blockchain network

Figure 2. Pseudo code of the Proof of Validity to verify the certificate

V. THE HYPERLEDGER FABRIC CERTIFICATE DESIGN

A. Entities

The hyperledger based certificate verification system will require educational institutes (Issuer), students (Receiver) and verifier (employer) as peer nodes in this design act as users. Issuers use the private key to sign the academic certificate and add digital signature. Digital water mark is used on the certificates to protect the contentof certificate. Then the network will create unique hash value for each certificates and the data stored in encrypted format. Using this unique hash value students, educational institutes and employers can access the certificate from the blockchain network. This guarantees stability of data and contents of certificates. Academic institutes can initiate Smart contract (Chaincode), digital watermark and signature to validate the academic certificates at every level of endorsement. As a result, students or employers receive the e-certificates in real- time. The process of the dataflow is illustrated in the Figure 3. The educational institutes offers the students to collect a blockchain credential and the students accepts offers, sending their hash IDs and issuer hashing the credential on the blockchain then send that address to students. Finally, the students can share their credential to employer for verification.

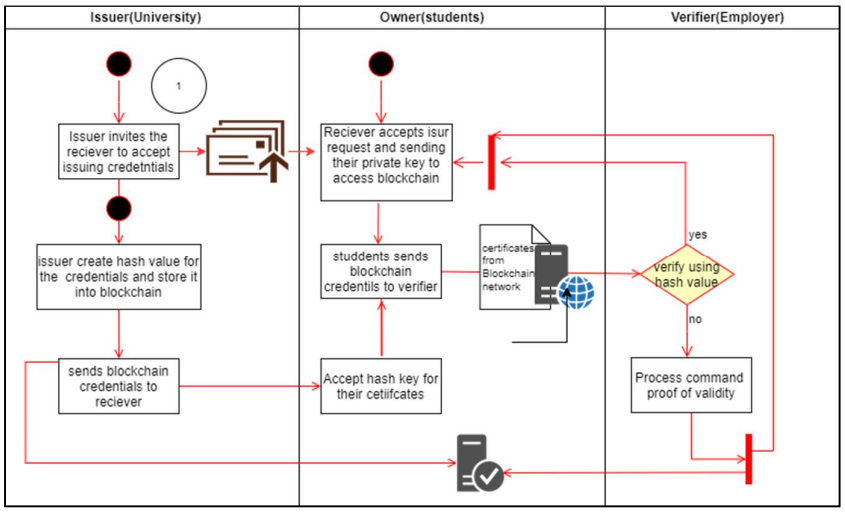

Figure 3. Dataflow diagram of the proposed design

B. The proposed Business Network

This prototype system uses Hyperledger fabric as blockchain framework with distributed ledger mechanism. The Fabric CS server enables authorization services and smart contract (chaincode) mechanism executes based on business logic which is defined by the educational institutes and other organizations. This system has various modules such as endorsement policy for user authentication, certificate authority, student information, recruitment information and academic certificate details. The Prototype system architecture Figure 4 also provides user interface via web application along with Fabric server API and Docker composer CLI (Command line interface) commands to customize the system when it is required. As shown in the Figure 3, users can authenticate their identities using document verification module via web interface. Further, they can obtain certificates from Hyperledger Fabric (CA) server with their private keys and passwords. Users, depending on their authorization, can request a query or update information related to students or recruitment with the web interface and CLI. The academic certificate can act as digital asset to be used as transaction between components in the system. The following steps illustrate a transaction flow between the components of blockchain framework. Users are enrolled via MSP into the peer to peer blockchain network.

- Issuer issue the certificate to the students and upload it via API server using document encryption anddecryption module the certificate are hashed and digital watermarked.
- A client submits a proposal transaction to endorsing peers.
- Endorsing peers execute the chain code, sign (endorse) and return the transaction to the client.
- Chain code run on network based on Proof of Authenticity (PoA) using digital watermark technique toimprove the security of student data stored in off-chain MongoDB.
- Then the orderer node get the endorsed transactions to be schedule to execute that transaction.

- The endorsed transactions are added into new block by channel based on the service of orderer node. Then,the ordering node returns the created block to a leader peer associated with a channel.
- Finally, transactions are validated by peers and append this validated block to the blockchain.

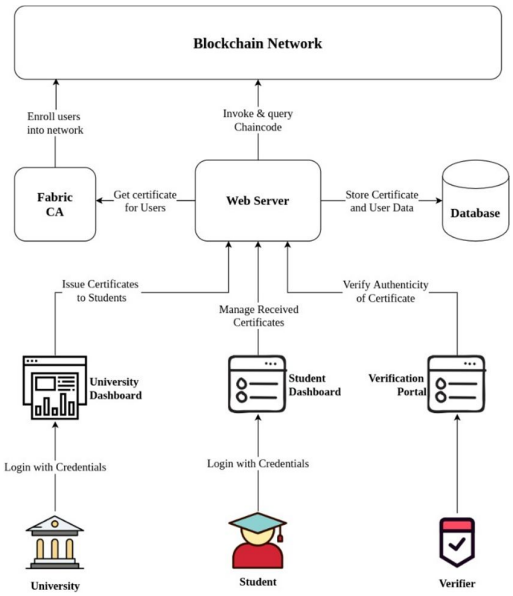

Figure 4. Prototype system

C. Blockchain-based Educational Records Repository Implementation

In order to implement this application the Hyperledger Fabric 2.1.0, node, MongoDB 4.0 and NPM are installed. The hyperledger fabric is used to implement the blockchain network to execute smart contract (Chaincode). Fabric CA I used to admit the members in the network [12]. Node.js used as backend of the web application to express framework and also chaincode is written in Node.js. The students and educational institute and organizations details are stored in MongoDB database.

The front end of the web application is developed using bootstrap, ejs and jQuery. The blockchain network uses include educational institutes, students and certificate verifiers (Employers). The educational institutes can issue the academic certificate, view academic certificates issued and endorse verification and digitally sign academic certificates. The students can receive academic certificates from the educational institutes, view and manage the received academic certificates. And also they can share their certificate with third party at the time of job recruitment or applying for the higher studies for verification. The employers can receive the data from students and verify certificate authenticity with blockchain platform. This academic certificate repository from the Docker composer perspective, has a composed of files which defining assets, participants and transactions. The node.js script file is responsible for maintain a set of scripts such as certificate schema, issuer schema and verifier schema. The JSON file is used to store the data about the certificate. This illustrate the certificate verification schema format issued in this application. These JSON file schemas can be assist to rich query. A traditional database used table structure as relational model to store records. Instead the relational database MongoDB use the <key, value> form to store the state of the database in ledger too. This form gives more security since it is JSON form and very difficult to access by applications developers [14] [15]. So in this application used JSON format to store the data and enhance the query. The script contains functions and definitions of the transactions to be used in the blockchain network. When transactions are submitted and structure are composed then the transaction process is automatically invoked by node.js chaincode functions to verify the certificate by the employers based on their object have given by the students (Figure 5).

D. Results

Hyperledger Fabric is a private blockchain since the students details are not in public domain. The access rights could be customized as per the requirement of the educational institute as well as y the students. That means student would not like to share their diplomas instead only their master degree to share for verification. The students will only can see their diplomas once issued.

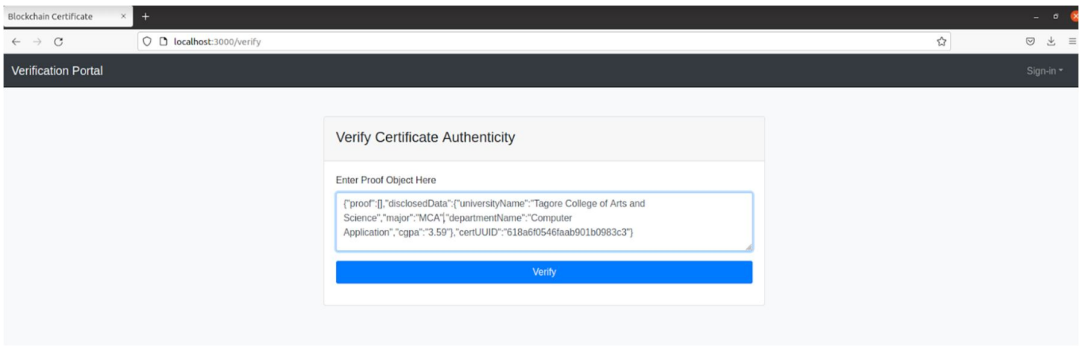

Figure 5. Verifying the certificate on blockchain network

ISSUER OF CERTIFICATE	HASH DIGITAL SIGNATURE	RECIEVER OF CERTIFICATE
c791915bc3baa1a08b8785d7716f43c0762 265b048b5427f3c8efb77e6b016ee	6232a22c3943697e990d9ae4dca21708b8bf0 1b59b39874a27c66997f06cccc7	bc176d2bd8d4dbd791a13df151c20489592 fc92e95fc44fe589d3b8f06f587c4
cbbca3eb39dcc956dec58e7ab2e1706281d 8e82c712b3e0993ee18f461232e8d	780190df5b28bea2eaa29d5320a8c44ce538a bd68929a4eb0190a300778b84f1	400063dff953caa2f535aac45888b0e9d088 e3e67730b932e38bf734b91b2f8a
ba47fe8ae2aa240b42f1702fafd285a3e98d 22e892bf02d91480fb52596fe696	666fa82081e96f07a00920106527dfeaa07d5 12301daa9267de3f4f3d04db654	cc57c6329f63acf14c82662e1c32d34bb98e 64895bbc2a07fa7d036fefabab79
550a3f8eeb2135143f22a91206a556dc207 a9dd95717f07f6ca5418ecdfa0d9d	25ed45404802db3c1f7d8a1ba1db4fc597ae9 ac1472bc04f609868ba0af8c79b	2f5bad6f2ca574d2d5e5f4db7cbf0de3ddd9 1750adfdbf28fd9b639baf2e6c25

Figure 6. Encrypted form of academic certificate

This is a hyperledger based application so it is not 'coin' based blockchain, this leads easy to implement unlike Bitcoin or Ethereum blockchain platform to use cryptocurrency to publish transaction over the distributed network. In this blockchain based application provide query to retrieve the details of students to whom certificate issued and also students can update their data on the MongoDB. All the data which stored on the blockchain network is hashed (Figure.6) along with digital water mark technique is used to enhance the protection of the data. Today's credential issues are overcome with blockchain solution and also this will improve and provides reliable solution in case of avoid the fraud and fake details stored the database.

VI. Conclusion

This paper proposes the blockchain based application to issue academic certificates with proof of Authenticity along with digital watermark a secure and safe to access. And also discussed about the efficiency of blockchain technology provides security in maintaining the academic records. But still this is growing technology many institutes try to implement this getting lack of experts gives training to their employees. Existing system does not provide much of security, there is a lot of chance to make fake certificates since it is in printed format. There are lots and lots of learning records and certificates, but there are no suitable frameworks to keep an eye on them. For the future work, it is planned to assess the adaptability issues and effects related with the sending of a massive repository. This may unite partners like universities, students, teachers and employers and project workers such that they cooperate with one another empowering huge utilization of this repository of e-certificates. In summary this will be to receive a completely normalized resource portrayal as an extra advance to a safe and secure decentralized method of presenting a more utilization of the hyperledger fabric blockchain framework.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," http://Www.Bitcoin.Org, p. 9, 2008.
[2] M. Valenta and P. Sandner, "Comparison of Ethereum, Hyperledger Fabric and Corda," 2017.
[3] Macrinici, D., Cartofeanu, C., Gao, S., Smart Contract Applications within Blockchain,Telematics and Informatics, journalhttps://doi.org/10.1016/j.tele.2018.10.004.
[4] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, "Blockchain and Smart Contract for Digital Certificate," Proceedings of IEEE International Conference on Applied System Innovation 2017.
[5] [online]Available: https://www.blockcerts.org.

[6] Dinesh Kumar K, Komathy K, Manoj Kumar D.S , “Blockchain Technologies in financial sectors and industries”, International Journal of Scientific and Technology Research Volume 8, Issue 11,pp. 942 -946, 2019.
[7] Benyuan He, “An Empirical Study of Online Shopping Using Blockchain Technology”,Department of Distribution Management, Takming University
[8] Zhenzhi Qiu, “Digital certificate for a painting based on blockchain technology,” Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.
[9] W. Diffie, P. C. Van Oorschot, M. J. Wiener, “Authentication and authenticated key exchanges,” Designs, Codes and cryptography 2(2), 107-125 (1992).
[10] “Ethereum project,” https://github.com/ethereum/wiki/wiki/ White-Paper [Accessed: 13-Jan- 2018].
[11] MIT Media Lab, “What we learned from designing an academic certificates system on the blockchain,” Medium, no. December, p. 2016.
[12] E. Androulaki et al., “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchain,” no. 1, 2018.
[13] Source: Adapted from: https://commons.wikimedia.org/wiki/File:Hash_function.svg
[14] Jerril Gilda, Maanav Mehrotra -Blockchain for Student Data Privacy and Consent International Conference, 2018 - ieeexplore.ieee.org.
[15] https://www.indiatoday.in/education-today/featurephilia/story/how-students-and- employers- can-spot-and-eliminate-fake-degrees-1725931-2020-09-27
[16] 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.
[17] Dinesh Kumar K, Senthil P, Manoj Kumar D.S “Educational Certificate Verification System Using Blockchain “,international journal of scientific & technology research volume 9, issue 03, march 2020 ISSN 2277-8616 82 ijstr©2020