Grenze International Journal of Engineering and Technology, Jan Issue

Blockchain based Privacy Preserving Student's Certificate Storage, Distribution and Verification

Athulya C. Shaji[1] and Dr. Anitha V. S[2]
[1-2]Govt. Engineering College, Wayanad, India
Email: athulyashaji@gecwyd.ac.in, anithavs@gecwyd.ac.in

***Abstract*—The blockchain is a chain of blocks with each block header containing a hash of its preceding block. Blockchain technology transforms the existing centralized system, trusting the third party, into a decentralized system that can exchange or store information within a trustless environment while preserving privacy and security. The transactions and data stored in the blockchain are not pursuant to the control of any mediator. The technology is now widely used in medical records, education, supply chain, and IoT.**

The paper implements a prototype model of a decentralized application for an education record verification and sharing system. In the current education system, institutions manage their data on a centralized server. Students are handed over a certificate as a hard copy at the end of the course. In this scenario, corroborating the authentication of a hard copy is very difficult because counterfeiting the original certificate is effortless.

In this paper, we introduce a blockchain-based proposal to substantiate the authenticity of transcripts and share them. Blockchain-based applications can hasten the transcript corroboration and sharing process by transforming the centralized approach into a decentralized one. The users of the blockchain- based system get lifelong authorized access to their transcripts and can share them with other institutes or organizations. We use IPFS blockchain-based decentralized cloud for storage, it can minimize the cost up to 86% and proxy re-encryption provide secure exchange without compromising the complexity.

***Index Terms*— Distributed Systems, Blockchain, Ethereum, IPFS, proxy re-encryption.**

I. INTRODUCTION

Corroborating the authentication of certificates is one of the educational field's significant challenges. The fundamental cause for this trouble is the complex procedures to verify the authenticity of transcripts. The traditional way of verification involves forwarding requests to the particular university and sending back the confirmation about the authentication of the certificate. The universities hold their students records in a centralized server and involves manual verification, making the process more complex and time-consuming. Maintaining data on a centralized server is more vulnerable to attack than in a decentralized system.

Transcript corroboration or detecting forged certificates is an intricate, expensive, and time-consuming process. It shows the demand for a system for transcript corroboration which is expeditious and affordable without compromising privacy and integrity. The system assists students to be the curator of their certificates and allows easy sharing with full authenticity. In this way, students can obtain their entire educational certificates on a single platform. Blockchain is a new technologythat transfers our notion of centralization to decentralization.

Grenze ID: 01.GIJET.9.1.519

Centralized systems are in a trustful environment but the blockchain introduces a secure decentralized system within the trustless environment. The completed transactions are recorded into a public chain that is tamper-proof. The first paper on blockchain technology was introduced [1] by Satoshi Nakamoto in 2008. All nodes in a blockchain retain a local copy of the global data and the system assures consistency among local copies. The blockchain network is a network of nodes connected like a mesh network. Any node can generate transactions and broadcast them to the network. All the nodes that receive the transaction request validate the transaction. A verified transaction can involve crypto-currencies, contracts, records, or anything of value. There are special nodes in the blockchain network called miners they collect all the verified transactions from all other nodes and create a block. The creation of the blocks involves solving complex puzzles. The first miner who solves this puzzle can add this block to the blockchain and get the reward for mining. The updated blockchain is broadcasted among the network.

This paper uses blockchain technology to implement a prototype model for student certificate storage, distribution, and verification. For cost reduction of on-chain storage, we choose off-chain IPFS for certificate storage. The IPFS can't preserve privacy, so to preserve the privacy and easy sharing of the certificate encrypt using NuCypher's proxy re-encryption algorithm. Proxy re-encryption can share the existing encrypted data with a third party without decrypting the same. The algorithm re-encrypts the data with a special key, which is the combination of the private key of the first party and the public key of the third party key, so the third party can decrypt it with his private key. This makes the sharing of certificates easy and preserves privacy.

The remainder of this paper is organized as follows. Section 2 reviews the existing works and their limitations. Section 3 describes the methodology used in this system. Implementation details are included in Section 4. Analysis and discussion are presented in Section 5. Finally, we conclude in Section 6.

II. Related Work

Blockchain reveals its potential in industry and academia. Currently, most blockchains are used in the financial domain. There are many more applications for different fields trying to implement blockchain to enhance security of their system. Blockchain technology creates a decentralized environment where transactions and data are not pursuant to the control of any mediator. This section describes different applications of blockchain in the educational field.

Cheng et al. in 2018[2], developed a decentralized application for a certificate inspection system based on the Ethereum blockchain. The forgery of certificates becomes very common. The main reason for that is making a fraudulent copy is very easy and the verification process is very difficult. The method for issuance of a digital certificate in the system is as follows. Generate an e-certificate then calculate its hash value and store it in the blockchain. The system automatically generates a related QR code and inquiry string code and affixes them to the paper certificate. The students can prove the authentication of the certificate by scanning the QR code via mobile phone or through website inquiries.

Kuvshino et al. in 2018[3] developed Disciplina, the first blockchain to create a verified personal profile for academic achievements. They propose a system for publicly verifying data produced by large universities, small institutes, schools, and online educational platforms. Disciplina platform is based on blockchain technology that aims to transfer the way educational records are generated, stored, and accessed. Nodes of the blockchain should store all grades issued by institutes from all over the world. In public ledgers, distributed storage is expensive and educational institutes have no incentive to pay for every grade they issue. So storing educational records in the public chain is economically unjustified.

Turkanovic et al. in 2018[4] introduced a credit transfer system for the higher educational institutes (HEI) based on the European credit transfer and accumulation system (ECTS). Currently, most of the HEI keep data on their own centralized server. Access to the data is limited to the institution's staff and dedicated online systems. The peers of the system are HEIs and the users are students and organizations. Each student registered under any HEI will have a dedicated wallet. When the student completes the course, HEI transfers the corresponding credit to the blockchain address. For security purposes, the system assigns a 2-2 multisignature address for students with home HEI. Any accredited HEI can join the network; while joining HEI have to create a network node. The fully functional node broadcasts messages across network. HEI will not have to mine transactions because it uses DPoS (Delegated Proof Of Stake) consensus protocol. In DPoS, any HEI can register as a delegate, and then all other HEIs vote and select one HEI as delegate. The selected HEI conform transaction and seal the block.

Lucas et al. in 2018[5] presented a proposal and implementation for the digital certificates and academic credits for higher education in the Brazilian education system. They propose a transparent model based on blockchain,

in which the university uploads students' data with their academic credits in the blockchain using the Brazilian Public Key Infrastructure. These details stored with the help of smart contracts enable the reliable and delegated delivery of certificates via the corroboration of a historical repository and the firing of transactions using smart contracts.

Jerinas et al. in 2019[6] proposed a blockchain-based system for administrating certificates called UZHBC (University of ZuricH BlockChain). They presented a prototype adapted to the UZH's needs to store and validate certificates delivered by its department. The initial step is to decide on the provisions of the university's stakeholders to build an initial prototype that demonstrates the functionalities and highlights the advantages. Subsequently, other improvements are foreseen as future work.

Ahmed et al. [7] introduced a permissioned blockchain- based system to permit institutions to securely and reliably transfer and validate educational records at the student's request. Permissioned blockchains, such as Hyperledger, provide a more extensible and affordable, and private solution for enterprise applications. The main purpose of this proposed system is to deal with the constraint of existing solutions by providing a secure, provable, and tamper-proof technique for the inspection of academic certificates between authorities using blockchain technologies.

Sugandha at al. [8] present the Blockchain for education platform as a realistic model for issuance, corroborate and distribution of the certificate. They proposed a platform TUDoc-Chain that authorizes the academic certificate on distributed public Blockchain and provide the transparency among the students, institute, and third-party stakeholders. The identities of individuals who participated in the system are accessed by the smart contract built on the ethereum platform using solidity [9]. Interplanetary File System (IPFS)[10] used as a distributed public network. IPFS produce the content address corresponding to the size of the transaction content.

The above mentioned works have many limitations. Among those blockchain technologies Ark, BitCoin, and Ethereum, the Ethereum blockchain provides features like smart contracts. It is useful in building general-purpose applications other than crypto-currency. The size of the blockchain becomes an issue with larger network. So the best way to store the certificate is to store it outside the chain. IPFS, FileCoin, and Swarm are some blockchain-based decentralized storage. All these are in the developing stage, and IPFS is a more mature work compared to others. The use of smart contracts also improves the efficiency of the system. The major limitation found in the literature survey is that they do not provide any privacy when storing the certificates. Distribution of certificates to a third party through these approaches is also difficult. To solve these problems the proposed system uses IPFS for storage and uses a smart contract to improve the efficiency of the system. The use of the proxy re-encryption [11] method solves the issue of privacy preserved distribution.

III. Proposed Solution

Blockchain is a new technology that transfers concept of centralization into decentralization. Centralized systems are created on top of a trust-full environment, but the blockchain introduces a secure, decentralized environment within the trust-less environment. Blockchain is first introduced for digital currency like bitcoin. Now the use of blockchain is changedto create a secure decentralized system. Developers are using blockchain technology for various applications and lots ofresearch works are in progress to enhance the efficiency.

A. Architecture

The proposed system mainly contains three types of users. The first user is the institution that is responsible for providingcertificates to students. Second is the students who are trained under the institution. Finally, the third party can verify the certificates of students.

1) *University:* The certification system creates a certificate for each student and stores the certificate inside blockchain-based decentralized storage. They can allow students to access their certificates through this system.
2) *Student:* When students pass the authentication process, then they can download the certificate. The students become the custodian of their official educational records and also theyget lifelong access to their records
3) *Third party:* They are the company or any other institute that wants to verify the certificate for the recruitment or admission purpose. Any third party can verify the certificate through the system with the permission of the student. The Fig. 1 shows the architecture of the proposed system.

B. Module Descriptions

We can divide the entire system into two main modules. The first one is the issual of certificate by the university and the second is verification of the issued certificate.

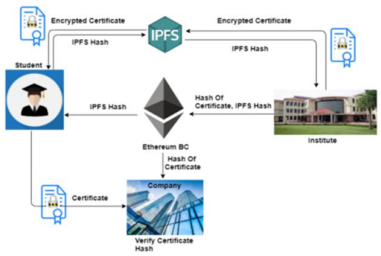

Fig 1. System architecture

1) *Issual of certificate:* The University generates an e-certificate and encrypts and stored it in the IPFS. The IPFS returns a unique cryptographic hash value representing the uploaded data. Details of encryption and IPFS hash are sentto the smart contract. Smart-contract verifies the details and creates a transaction and signs, and confirms. Fig. 2 shows theprocedures of certificate issual.
2) *Verification of certificate:* The third-party can be any company or institution that wanted to verify students' educational certificates. When verifier needs to access the certificate,verifier sends a request to student with verifier's public key. Stu-dent then generates a re-encryption key with student's private key and verifiers public key and send to the proxies (nodes in blockchain) in the network. Proxies re-encrypt the certificate and send to verifier, then verifier can decrypt certificate with its own private key. Fig. 3 shows the certificate verification process.

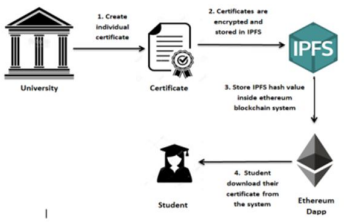

Fig 2. Issual of certificate

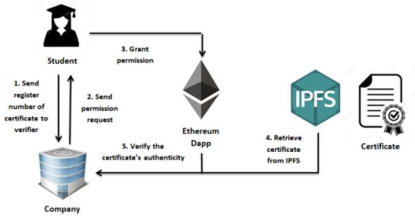

Fig 3. Verification of certificate

IV. Implementation Details

The paper implemented a prototype model to demonstrate how the institution can send certificates to student through blockchain and make the student as the custodian of their official record. For the prototype model implementation use truffle framework for smart contract compilation and migration, Ganache[12] as a blockchain simulator, Rinkeby Testnet[13] to test application and Web3.js[14] for interacting with local or remote ethereum node. To solve the storage issue in blockchain we use IPFS the decentralized storage.

There are a total of eight functions; they are: student registration, institution registration, issue certificate, get certificate, certificate verification, certificate encryption, certificate decryption.

The Student Registration algorithm, Algorithm 1, stores the public key and personal details in the smart contract as a transaction. The function will return the transaction id, we can trace the transaction with the transaction ID.

Algorithm 2: The institution registration algorithm also savethe public key and identity information in the smart contract, then it return the transaction ID.

Algorithm 3: The issue certificate algorithm encrypts the certificate with students public key using umbral proxy re- encryption method. Then the encrypted certificate is sent to IPFS, IPFS returns the IPFS hash as the address of the stored file. The PUSHDATA function sent student's public key,certificate unique ID, certificate hash and IPFS hash to the smart contract and it will return the transaction ID.

Algorithm 4: The get certificate algorithm is run by the student to get the certificate issued by the institution. The student can retrieve the encrypted certificate from IPFS with IPFS hash and decrypt with student's private key.

Algorithm 5: The certificate verification algorithm is runby the company. When student give the access right to any company who can verify the certificate. The company can access the certificate only if they have access right provided by the student. The output of this function is to Boolean, indicate success or failure of verification.

Algorithm 1: Student Registration
Input: Student's public key(pKs), Student's details(data)
Output: Transaction ID(trnID)

```
function REGISTERRECIPIENT(pKs, data)
    trnID ←PUSHDATA(pKs,data)
    return trnID
end function
```

Algorithm 2: Institution Registration
Input: Institution's public key(pKi), Institution's details(data)
Output: Transaction ID(trnID)

```
function REGISTERISSUER(pKi, data)
    trnID ←PUSHDATA(pKi,data)
    return trnID
end function
```

Algorithm 3: Issue certificate
Input: Students's public key(pKs), Certificate number(Cert-no), Student's certificate(certificate)
Output: Transaction ID(trnID)

```
function ISSUECERTIFICATE(pKs, Cert − no, certificate)
    encrypted − certificate ←umbralENCRYPT(pKs, certificate)
    ipfs − hash ←PUSHIPFSDATA(encrypted-certificate)
    Cert − hash ←GETHASH(certificate)
    trnID ←PUSHDATA(pKs,Cert-no,Cert-hash,ipfs-hash)
    return trnID
end function
```

Algorithm 4: Get Certificate
Input: Certificate, number(Cert-no), TransactionID(trnID),Student's Secret key(sKs)
Output: Certificate(decrypted-certificate)

```
function GETRECIPIENTCERTIFICATES(Cert - no, trnID)
ipfs — hash←GETDATA(Cert-no,trnID)
    encrypted — certificate ←GETIPFSDATA(ipfs-hash)
    decrypted—certificate ←umbralDECRYPT(encrypted-certificate,sks)
return decrypted - certificate
end function
```

Algorithm 5: Certificate verification
Input: Certificate number(Cert-no), Transaction ID(trnID), Student's public key(pKs), Certificate
Output: Boolean

```
function VERIFYCERTIFICATE(Cert − no, trnID, pKs)
    cert − hash ←GETDATA(Cert-no,trnID,pKs)
    generated − hash ←GETHASH(certificate)
    bool ←compareHash(Cert-hash,generated-hash)
    return bool
end function
```

V. RESULT

We have analyzed the developed Dapp by deploying smart contracts and running on ethereum test network rinkeby. To preserve the privacy of student's certificates, we use encryption mechanisms for certificates. To compare we have implemented both symmetric key encryption (AES) and asymmetric key encryption(proxy re-encryption). Fig. 4 shows a comparison between Dapp using AES encryption and Dapp using proxy re-encryption. The smart-contract deployment cost of proxy re-encryption is 38.94% less compared to the deployment cost of AES and also the transaction cost used for issuing the certificate is 6.87% less in proxy re-encryption. To analyze the performance of our Dapp we used the ethereum test network rinkeby, all the transactions are mined in the rinkeby network. The deployment cost of smart contracts for proxy re-encryption is 34447000Gwei. Registration of an institution and a student needs to pay on average 233000Gwei and 226000Gwei respectively, which is dependent on the varying input size. The institution can issue a certificate to the student with a transaction cost of 214000Gwei. The verifier needs to request permission from the student to access their certificate for verification and the transaction fee for this is 39000Gwei. The student can give permission to the verifier with a transaction cost of 66000Gwei. Here the deployment cost of the smart contract is high compared to other transactions, but this transaction performs once so it is affordable. All the other transaction costs are affordable for institutions, students, and verifiers.

The proposed system uses IPFS to store certificates, which is the most commonly used decentralized storage. Fig. 5 compares the difference in cost while storing data on-chain and off-chain (IPFS). Dapp using off-chain stores can save transactions cost 86% more than on-chain storage. So the use of IPFS off-chain storage is affordable compared to on-chain storage.

Reading data from blockchain will take very negligible time but writing data will take some time for validation, mining and block creation. The average time for write data to the blockchain in rinkeby test network is 15s[15] according to their official site. To compute the average execution time we send 50 upload request back-to-back. Fig. 7 shows the response time of 50 requests with a fluctuating line, the strait- line with 15s indicates the average response time of rinkeby, and the next strait-line indicates with average 15.33s time taken in our local network. The change between the ascertained average time and the formalistic average time is 0.33s. The extra delay is due to the time needed for performance of smart contracts on the Ethereum and communication delay.

The Fig. 7 shows the time taken to store data in IPFS with varying file sizes. The execution time of IPFS is almost constantly increasing with the increase in file size. To upload a file with size 10 KB, 529KB, and 1088KB it takes on average 1s, 5s, and 12s respectively.

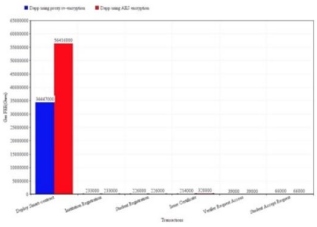

Fig. 4. Transactions VS cost in Dapp

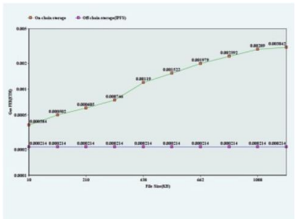

Fig. 5. Comparison between on-chain and off-chain storage using AES and proxy re-encryption

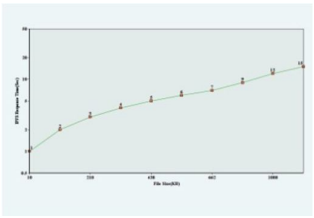

Fig. 6. Execution time for upload request on

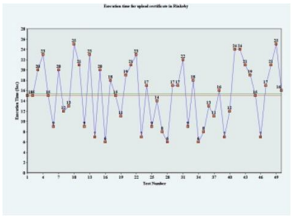

Fig. 7. Average time taken to upload files in IPFS rinkeby test network

While analyzing the execution time of proxy re-encryption used in this Dapp, All the functions require only less thanone second. The table 1 shows the average execution time for the functions Encryption, Re-encryption, and decryption. The average time taken to execute encryption function is 0.32s, decryption function is 0.49s, and re-encryption function is0.5s.

The DApp for certificate storage, distribution, and verification is fast, scalable, and privacy-preserving. The use of IPFS for certificate storage can save transaction costs compared to on-chain storage. The privacy in the distribution of certificate is provided by the proxy re-encryption.

TABLE I. PROXY RE-ENCRYPTION AVERAGE EXECUTION TIME

Proxy Re-encryption Methods	Execution time
Encryption	0.32sec
Re-Encryption	0.50sec
Decryption	0.49sec

VI. CONCLUSIONS

In this paper we have designed and implemented block chain-based academic record storage, distribution, and verification system. This prototype implementation of a decentralized application uses the fetchers of Ethereum blockchain. The highlights of the proposed system are: University canreduce the overhead of the certificate verification process,students become the custodian of their official records and third-party can easily verify the certificate. Students get accessto their complete educational credentials in a single platform and lifelong and authorized access to educational records from anywhere anytime and it is shareable.

We use ethereum blockchain and decentralized storage IPFS for certificate storage. Ethereum blockchain stores the proof of certificate by storing the hash and IPFS is used to store the encrypted certificate of the student. The privacy of certificate is ensured by implementing a proxy re-encryption algorithm umbral developed by Nucypher [11]. Compared to the traditional verification approach, cost, time, security, and privacy for the storage, distribution, and verification are efficient in ourproposed system. From the analysis, it is clear that the use of IPFS can save transaction cost to 86%. The execution time for proxy re-encryption functions is less than 0.5ms. As future work, we are planning to design a decentralized application for verifiable resumes for students.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and smart contract for digital certificate," in *2018 IEEE international conference on applied system invention (ICASI)*. IEEE, 2018, pp. 1046–1051.
[3] K. Kuvshinov, I. Nikiforov, J. Mostovoy, D. Mukhutdinov, K. Andreev, and V. Podtelkin, "Disciplina: Blockchain for education," 2018.
[4] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "Eductx: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.
[5] L. M. Palma, M. A. Vigil, F. L. Pereira, and J. E. Martina, "Blockchain and smart contracts for higher education registry in brazil," *International Journal of Network Management*, vol. 29, no. 3, p. e2061, 2019.
[6] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, "The proposal of a blockchain-based architecture for transparent certificate handling," in *International Conference on Business Information Systems*. Springer, 2018, pp. 185–196.
[7] A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar, and P. C. Hung, "A permissioned blockchain-based system for verification of academic records," in *2019 10th IFIP International Conference on New Technolo- gies, Mobility and Security (NTMS)*. IEEE, 2019, pp. 1–5.
[8] R. Rani *et al*., "Tudocchain-securing academic certificate digitally on blockchain," Ph.D. dissertation, 2019.
[9] Solidity.[Online]. Available:https://solidity.readthedocs.io/en/latest/index.html
[10] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.
[11] D. Nunez, "Umbral: a threshold proxy re-encryption scheme," *NuCypher Inc and NICS Lab, University of Malaga, Spain*, 2018.
[12] Truffle suite. [Online]. Available: https://trufflesuite.com
[13] rinkeby.etherscan. [Online]. Available: https://rinkeby.etherscan.io/
[14] Web3.js. [Online]. Available: https://web3js.readthedocs.io/en/v1.7.5/
[15] Rinkby stats. [Online]. Available: https://www.rinkeby.io/stats
[16] J. Cheng, N. Lee, C. Chi, and Y. Chen, "Blockchain and smart contract for digital certificate," in *2018 IEEE International Conference on Applied System Invention (ICASI)*, April 2018, pp. 1046–1051.
[17] J. L. de la Rosa, V. Torres-Padrosa, A. el Fakdi, D. Gibovic, O. Hornyák, L. Maicher, and F. Miralles, "A survey of blockchain technologies for open innovation," in *4rd Annual World Open Innovation Conf. WOIC*, 2017, pp. 14–15.
[18] M. Egorov, D. Nun˜ez, and M. Wilkison, "Nucypher: A proxy re- encryption network to empower privacy in decentralized systems," NuCypher whitepaper, 2018.