Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 5- Issue 2, Paper 37 August 2022

Performance Analysis of E-certificate generation and verification using Blockchain and IPFS

Manjula K Pawar, Prakashgoud Patil , Ridham Sawhney ,
Prem Gumathanavar , Shraddha Hegde , Kavya Maremmagol
Computer Science and Engineering
KLE Technological University
Hubli, India

Abstract— For many years to the present, people have used strong copies of degree certificates to prove graduation.But in recent days, due to advanced technology, these certificates have been forged. As a result, undeserving people get job opportunities, which tarnishes the image of these paper certificates. Therefore, overcoming such certification problems using blockchain technology is encouraged. Blockchain is a system of storing information that makes it difficult or impossible to repair, hack a system, and save paper costs. With the help of blockchain, an anti-forge, fixed, e-certified e-certificate is produced.Students will not be able to manipulate the content of e certificates. The function of this system is that: a computer file (e-file) of the certificate ie. The institution produces the e-certificate. At the same time, that student's record is kept in blockchain blocks using hash values. The hash value is generated from IPFS (Interplanetary file system) network. Accompanying e-certificate, associated unique serial number (unique id) were also given to the applicant. The searching system (e.g. The Company the applicant applied for) can verify the authenticity of the e-file using a unique hash value based on the data stored in the blockchain. The proposed method improves the performance concerning storage and speed.

Keywords— ***Blockchain, IPFS, e-certificate, storage, speed, scalability.***

I. INTRODUCTION

The advancement in trending technologies, usage of the internet, and mobile devices have changed the lifestyle of people and the way they think.[2] Due to this, various currencies are growing, such as Bitcoin,ethereum, and ripple.People are adapting the blockchain for transactions because of its flexible investements[3]. Blockchain includes a separate and intangible website with great potential for a variety of uses. Blockchain provides a different and virtual web site with a wide range of capabilities. A distributed network where millions of users are located worldwide [2]. Peer-to-peer (p2p) network, users can create static records, and functions can only be reviewed once it has received the consent of all the participants in the network and is also known as a one-time, multi-component technology.

With the technology improvements, data protection has become very important. Data has been considered as an official for the students in an organization, and their academic achievements are reflected in certificates.The data can be informal such as research data, skills data, online learning experience, and individual interests.Today, there are many forging or fraud certifications of students, and counterfeiting of educational certificates is increasing [7,8].This needs to be prevented.Hence in the proposed methodology, this problem has been resolved by adapting Blockchain technology because of its several immutable, transparent, and security characteristics. In addition, it also ensures other features such as reliability, trustworthiness, and authority. By using this technology, in this proposed work e-certificate is generated.There may be chances that students may lose their certificates. Re-applying for the hardcopy of the certificate is time-consuming. Hence in proposed methodology, which generates an e-certificate that helps for saving paper, time, and cost.

The paper proposes a decentralized application and designed certificate system based on ethereum blockchain. The ethereum performs synchronization using IPFS (Interplanetary File System) network. By integrating Blockchain with IPFS, the system improves the efficiency of operations at each stage.It improves storage, saves paper costs, stops forgery of documents, and provides accurate and reliable information on digital certificates. Space, time, and throughput are factors of scalability [11, 12, and 13]. The proposed method improves scalability.

II. RELATED WORK

In paper [1] author describes blockchain structure and different types of blockchain, namely public blockchain, private blockchain, consortium blockchain...Attached with the complexities that occur in various kinds of blockchain.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 5- Issue 2, Paper 37 August 2022

In paper [2], the author describes information about smart public contracts, smart authorized contracts, and the use of smart contracts. The smart contracts also discussed future trends and described better solutions to open research challenges.

In paper [3] provides information on the design and implementation of the aggregate number of local files in a blockchain, taking care of the privacy of the data.Further discussed how it prevents middleware from tempering the actual data.

In paper [4], the development of a certification process was proposed as a blockchain model for certification of completion certificate. The possibility of forgery of certificates will be reduced, and confidentiality, security, and legitimacy of certificates will increase.

In paper [5], three user groups are involved in the program: schools or certification units provide certificates, access the system, and browse the program website. When students meet certain requirements, authorities issue a certificate for the program.Once students have received their certificates, they can inquire about any certificate they have received.

In paper [6] explains the process of producing an e-certificate where planning language can be used to create a block containing individual student details.Further, provide clarity how it provides forge certification generation in the system.

III. PROPOSED MODEL

The working processes of the system are shown in Fig1 and Fig2.The institution will first log in to the interface by entering the right credentials. After checking their username and password, they will be redirected to an interface where the institution can upload the document containing student details like name and USN(University seat Number). After uploading, the data is stored in IPFS [14, 15, 16, 17, 18] and in the blockchain.The blockchain contains the hash of IPFS. A transaction is created, and the transaction hash contains IPFS hash.If any data in IPFS is altered, then this hash will be changed. During verification, the company or firm that takes the interview should log in with their credentials.

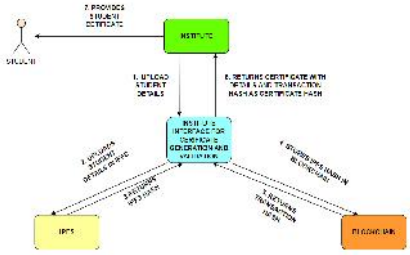

Fig. 1. E-Certificate generation architecture

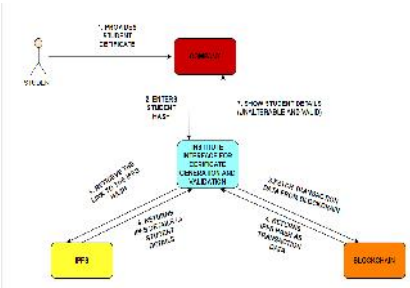

Fig. 2. E-Certificate validation architecture

successfully logging in, they enter the hash value .Our interface checks in blockchain blocks whether a given transaction hash is valid or not.If the transaction hash matches, then the student has verified else,it is clear that the student or applicant has tried to manipulate the details.

A. Algorithm for the proposed methodology

Generation

1. Institute will insert the student's details into IPFS and receive a hash from the IPFS.
2. Then the institute will insert the received IPFS hash into the blockchain network and receives the transaction hash from there.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 5- Issue 2, Paper 37 August 2022

3. Then the institute will provide the certificate to the student comprising of student degree details and the certificate hash i.e., transaction hash.

```
void add_details(student_detail)
{
    X=upload_in_IPFS ( student_detail )
    //X will contain hash received from IPFS
    Y=upload_in_Blockchain ( X )
    // Y will contain the transaction hash received from blockchain
    Certificate_Hash=Y;
    Attach_with_certificate ( Certificate_Hash )

}
```

Validation

1. When any verifier (institute/company) receives certificate.
2. Verifier will pass the certificate hash into to institute interface.
3. In Institute interface, data will get fetched from the blockchain i.e nothing but IPFS hash.
4. Then the institute itself shows the details fetched from the IPFS hash, which is true/immutable details of the student.

```
Student_detail  fetchDetails ( Certificate_Hash )
{

  If  (VALID(Certificate_Hash)==  true)
  {
    X= get_data_from_blockchain ( Certificate_Hash ) ;
    //X=> data fetched from blockchain(IPFS HASH)
    If (VALID(X) == true) // to check valid IPFS hash
    {
      Y=get_data_from_IPFS( X );
      //Y=> data fetched from IPFS (student details)
    }

  }
  return Y;
}
```

IV. IMPLEMENTATION

Fig 3 shows a login page where university authorities can give valid credentials, and even interviewers can log in. After logging in successfully, the interface routes to their respective pages i.e., for college authorities, it routes to the file uploading page, whereas it routes to verifying page for interviewers. In Fig4 if credentials are not valid, it gives a pop-up message saying THAT credentials are invalid.Through this we ensure that only the authorized people can upload data (college authorities) and verify students (company authorities)

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 5- Issue 2, Paper 37 August 2022

Fig. 3. Login Page

Fig. 4. Invalid Credentials

Fig. 5. College interface

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 5- Issue 2, Paper 37 August 2022

Fig. 6. Company interface

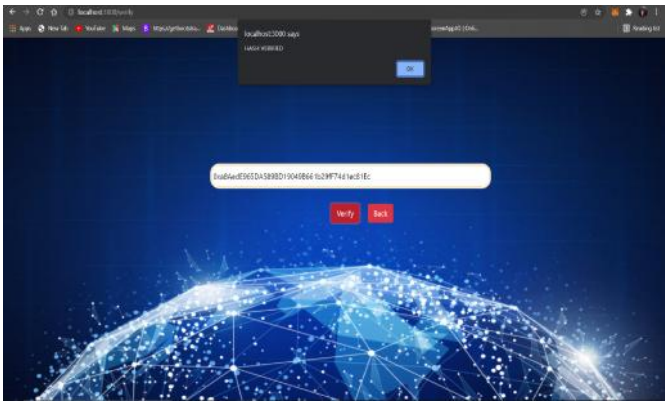

Fig. 7. Valid Hash Entered

Fig 5. shows the interface where college authorities will upload the document containing student details. Fig 6 shows the interface where company authorities can enter the hash provided by the student and verify the details. Fig 7 shows the interface where company authorities put the hash provided by the student, if the hash is valid then it gives pop-up message saying that hash verified.

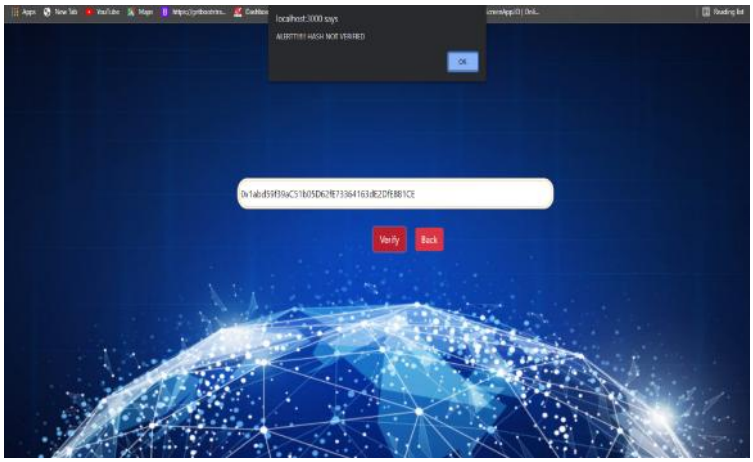

Fig. 8. Invalid hash entered

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 5- Issue 2, Paper 37 August 2022

Fig 8 shows the interface where company authorities put the hash provided by the student, if the hash is not valid then it gives pop-up message saying that hash not verified.

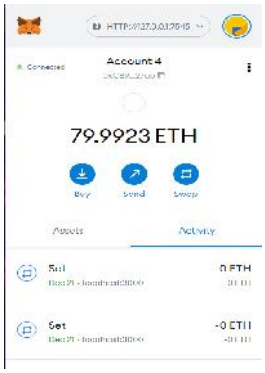

Fig. 9. MetaMask Interface

Fig. 10. Certificate Details

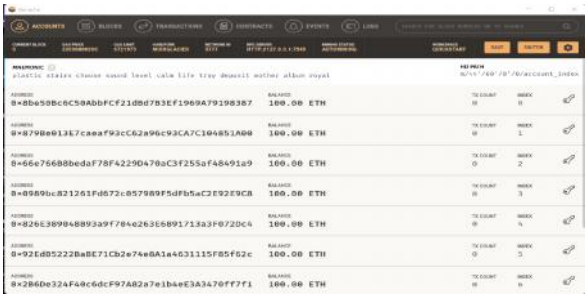

Fig. 11. Blckchain Transaction

Fig9 shows the Metamask interface where the transaction takes place.Fig10 once the hash is generated, data certificate details can be retrieved by clicking view.Fig11 shows blockchain transaction design in Ganache.

V. RESULTS AND ANALYSIS

In the Fig12 graph, the red color line indicates the time to generate a hash for each transaction before using IPFS. The blue line indicates the time taken to generate a hash for each transaction after using IPFS.The graph shows that the time to generate hash is less when IPFS is used when compared to the time taken to generate transaction hash without IPFS.

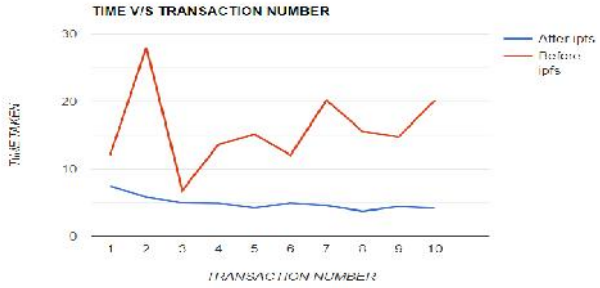

Fig. 12. Time vs Transaction number

E-certificates generated by the proposed methodology reduces the administration time, consume less space, and reduce the cost, improving efficiency and being more secure.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 5- Issue 2, Paper 37 August 2022

VI. CONCLUSION

Using a proposed blockchain-based system reduces the chances of certificates being forged.The certificate application and automatic certification process are open and transparent in the system. Many industries and organizations can check the certification within the system. The proposed methodology improves the reliability of e-certificates. It reduces the chances of certificate fraud and makes the entire process transparent. E-certificates can be viewed at any point of time by giving an alternative serial number as an input. The IPFS in the proposed methodology saved space and time, hence improving the scalability.The whole system ensures the accuracy and security of the information.

Further, the system can be extended for the wider network (presently done only for one institution), and an extra feature like scanning QR can be added.

REFERENCES

[1] Hu, Yining & Liyanage, Madhusanka & Manzoor, Ahsan & Thilakarathna, Kanchana & Jourjon, Guillaume & Seneviratne, Aruna. (2019). Blockchain-based Smart Contracts - Applications and Challenges.

[2] Said, A.G. & Ashtaputre, R.P. & Bisht, Bivas & Bandal, S.S. & Dhamale, P.N.. (2019). E-Certificate Authentication System Using Blockchain. International Journal of Computer Sciences and Engineering. 7. 191-195. 10.26438/ijcse/v7i4.191195.

[3] thin zar ko ko, “certificate verification system based on blockchain technology” 2020..

[4] Priya, Shanmuga. “Online Certificate Validation Using Blockchain.” (2019).

[5] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 10.1109/BigDataCongress.2017.85.

[6] Ebin Mathew, Maria Paulson, Reshma Joy, Prof. Jisha P Abraham *"E-Certificate Generation using Blockchain"* International Journal of Computer Trends and Technology 68.3 (2020):70-73.

[7] marco baldi , franco chiaraluce, emanuele frontoni , giuseppe gottardi, daniele sciarroni , and luca spalazzi ,“certificate validation through public ledgers and blockchains”,2017

[8] mr. Saber nasir take1 , prof. Monika d. Rokade , “customized e-certification generation using blockchain technology for distributed framework”,2021

[9] kumari, S. & Dhandapani, Saveetha. (2018). Blockchain and Smart Contract for Digital Document Verification. International Journal of Engineering & Technology. 7. 394. 10.14419/ijet.v7i4.6.28449.

[10] Gopal, Neethu V. and Vani V Prakash. “Survey on Blockchain Based Digital Certificate System.” (2018).

[11] Pawar M.K., Patil P., Hiremath P.S. (2021) A Study on Blockchain Scalability. In: Tuba M., Akashe S., Joshi A. (eds) ICT Systems and Sustainability. Advances in Intelligent Systems and Computing, vol 1270. Springer, Singapore.

[12] Pawar M.K., Patil P., Hiremath P.S., Hegde V.S., Agarwal S., Naveenkumar P.B. (2021) “Scalable Blockchain Framework for a Food Supply Chain”. In: Thampi S.M., Gelenbe E., Atiquzzaman M., Chaudhary V., Li KC. (eds) Advances in Computing and Network Communications. Lecture Notes in Electrical Engineering, vol 735. Springer, Singapore. https://doi.org/10.1007/978-981-33-6977-1_35.

[13] M. K. Pawar, P. Patil, M. Sharma and M. Chalageri, "Secure and Scalable Decentralized Supply Chain Management Using Ethereum and IPFS Platform," 2021 International Conference on Intelligent Technologies (CONIT), 2021, pp. 1-5, doi: 10.1109/CONIT51480.2021.9498537.

[14] R. Kumar and R. Tripathi, ”Implementation of Distributed File Storage and AccesFramework using IPFS and Blockchain,” 2019 Fifth International Conference on Image Information Processing (ICIIP), 2019, pp. 246251, doi: 10.1109/ICIIP47207.2019.8985677.

[15] Q. Zheng, Y. Li, P. Chen and X. Dong, "An Innovative IPFS-Based Storage Model for Blockchain," 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), 2018, pp. 704-708, doi: 10.1109/WI.2018.000-8.

[16] D. Malhotra, S. Srivastava, P. Saini and A. K. Singh, "Blockchain based audit trailing of XAI decisions: Storing on IPFS and Ethereum Blockchain," 2021 International Conference on COMmunication Systems NETworkS (COMSNETS),2021,pp.1-5,doi:10.1109/COMSNETS51098.2021.9352908.

[17] M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State, "Blockchain-Based, Decentralized Access Control for IPFS," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1499-1506, doi: 10.1109/Cybermatics2018.2018.00253.

[18] R. Kumar, N. Marchang and R. Tripathi, "Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain," 2020 International Conference on COMmunication Systems NETworkS (COMSNETS), 2020, pp. 1-5, doi: 10.1109/COMSNETS48256.2020.9027313.

s