Grenze International Journal of Engineering and Technology, June Issue

CertiBlock: Decentralized Blockchain Framework for Tamper-Resistant Certificate Issuance and Real-Time Verification

Kavya D[1], Shruti Sharma[2], Samiksha[3] and Shabana Sultana[4]
[1-4]Dept. of Computer Science and Engineering, The National Institute of Engineering, Mysore-570008, India
Email: dkavya494@gmail.com, shrutisharmapatna22@gmail.com, samchand0211@gmail.com, shabana@nie.ac.in

***Abstract*—Many colleges and universities are facing problems in verifying the originality of certificates uploaded by students as tampering certificates and creating false certificates have become a common and serious issue. To solve this problem, we came up with a digital and centralized platform "CertiBlock". A blockchain based certificate verification platform is a digital platform which solves certificate forgery and tampering issues, data breaching issues, and helps to conduct verification processes efficiently.**

In the existing platform, admin and faculties must verify each certificate manually, which takes more time to complete the whole process. Whereas in this proposed platform we can store certificates protectly. We have used a decentralized network, where data is dispersed among multiple users, making this platform more robust, as there is no single point of failure. There is a database to store hashes of certificates using On-chain storage. We have Off-chain storage to store actual certificates, to reduce the size of the blockchain.

Benefits of using this platform:

- **Reduced verification time.**
- **Decentralized platform.**
- **Increase reliability and reliability among users.**

Keywords — Blockchain, Hash, Decentralized Network.

I. INTRODUCTION

Colleges and educational institutions deal with major problems in verifying certificates uploaded by students. Nowadays there are many sources using which students can generate or modify false certificates, and admins cannot identify mistakes or duplicity if checked manually. Still many institutions depend on manual checking, leading to mistakes, wrong outcomes, and increasing work for staff.

This paper shows the use of a blockchain based certificate verification platform that uses a decentralized network and On-chain storage to ensure security, integrity and authenticity of certificates. Blockchain technology provides us a platform where we can store certificates in a protected manner, unaudited way and in a tamper-resistant way.

Contribution: This paper makes following contributions:

- We propose a block-chain based certificate verification platform that uses On-chain storage and Off-chain storage to ensure protect and smooths verification of certificates

Grenze ID: 01.GIJET.12.2.648_26

- We have used decentralized network architecture to store data protectly and also auditable storage of hash of certificates generated by administrators. There is no single point of failure, making it a more reliable platform. It also avoids tampering and forgery of certificates.
- We checked the performance of our platform and discovered that verification time has reduced by 50% compared to the traditional platform. It also reduces human effort by automating the whole process. This shows that our platform has very potential to deploy for the real world.

Today this forgery and tampering of certificates are very common and an issue of concern. This proposed platform is a highly scalable and reliable solution for real world application.

Nowadays the certificates are issued by websites or applications for students. Few students complete their work properly, but all the other remaining students forged the certificate like name, roll number and submit to the faculty and then faculty or institution has to struggle to check whether those certificates are original or tampered. Organizations will get a decentralized platform where they can issue certificates to students. They can identify users who are attempting to bypass course requirements using fake certificates. This will help students to complete courses and improve their skills.

II. Related Work

TABLE I: COMPARISON OF PREVIOUS WORKS AND PROPOSED WORK

Papers	On-chain storage	Off-chain storage	Performance discussion	scalable
[1]	N/A	N/A	N/A	Limited
[2]	Yes	No	Missing	Limited
[3]	Yes	No	Missing	Limited
[4]	Yes	No	Missing	Limited
[5]	Yes	No	Missing	Limited
[6]	Yes	No	Missing	Limited
[7]	N/A	N/A	N/A	N/A
[8]	N/A	N/A	N/A	N/A
[9]	Yes	No	Missing	Limited
[10]	Yes	No	Missing	Limited
[11]	Yes	No	Missing	Limited
[12]	N/A	N/A	N/A	N/A
[13]	Yes	No	Missing	Limited
[14]	N/A	N/A	N/A	N/A
[15]	Yes	No	Yes	Yes
Proposed platform	Yes	Yes	Detailed Analysis	Highly Scalable

The whole concept of block-chain technology was first coined by S. Nakamoto in [1] , where it shows us the use of this blockchain technology for Bitcoin cryptocurrency. This paper shows us how reliable and auditable transactions are made.

The paper by M. Sharples and J.Domingue [2] shows how this blockchain technology is based on decentralized network architecture. This paper proposes a decentralized platform for storing and managing the information of millions of students, course certificates, rewards using smart contracts.

Maintaining authentication in this platform is taken from paper by N.Chalaemwongwan and W.Kurutach [3] , which proposes a block-chain based platform that protectly stores all information of students. The problem we face while considering this paper is that it does not support off-chain storage, making this platform less scalable.

Maintaining authentication of digital certificates as in paper

[4][5] shows application of on-chain storage for authentication. It shows how hashes of certificates are stored on blockchain. Concept of decentralized certificate verification platform in paper[6], by A.Tapas, S.Patil focuses on using decentralized architecture using blockchain technology. This paper lacks detailed analysis of the platform's efficiency.

Utilizing blockchain for IoT devices has been learnt from paper[7], by X.Liang, J.Zhao, S.Shetty which proposes a blockchain based reliability model for these devices, aims to create reliability and relation between devices. To gain complete knowledge about blockchain technology we referred to paper[8], by Z.Zheng, S.Xie, X.Chen, and H.Wang that provides us a complete overview of blockchain technology such as its architecture and all other mechanisms.

For verifying digital certificates in more protect and auditable way we referred paper[9] by R.Malik, A.Khanna and N.Kaur and paper [10], by Y.Zhang, Y.Chen, and J.Peng which gives us detailed understanding of how to verify certificates correctly and more efficiently.

Researchers have also explored some digitalized education platforms such as in paper [11] and [13], that propose blockchain based learning platforms. We also referred to some surveys and reviews such as [12] and [14], that show interest in applying blockchain technology in various fields such as education and healthcare.
Paper[15] by Y.Chen, S.Ding, Z.Xu, H.Zheng and S.Yang proposes a blockchain inspired framework for protected storage and maintaining of medical records and data, also enabling protected sharing of these data and restricted access of these records.
The comparison of distinct blockchain based verification platforms are given in Table 1. This table demonstrates different features of each platform and their disadvantages and failures and also advantages of various papers referred to.

III. METHODOLOGY

The methodology for the Protect Certificate Management and Verification platform was built by giving priority to security, scalability, and smooth running of the program during verification. Rather than blindly relying on a purely conceptual blockchain model, our platform tries to focus on how effectively we can store and manage the certificates in a simpler way while minimizing cost and performance overhead.
Storing complete certificate files directly on the blockchain is not the best method, since it is neither cost-effective nor scalable due to high transaction fees and limitations in storage. To avoid this, our platform comes up with another hybrid approach where we only store the cryptographic hash of each certificate on the blockchain, while the actual certificate file is protectly maintained off chain. By this method, any changes made to the certificate will also change the hash, making the tampering detectable at the very moment, while keeping the load on blockchain storage low.
Ethereum was selected as the best option for the underlying blockchain platform because of its stability, wide adoption, and strong support for the execution of smart contracts. To avoid financial stress due to costs during development and testing, we implemented the platform on the network Ethereum test.

IV. IMPLEMENTATION

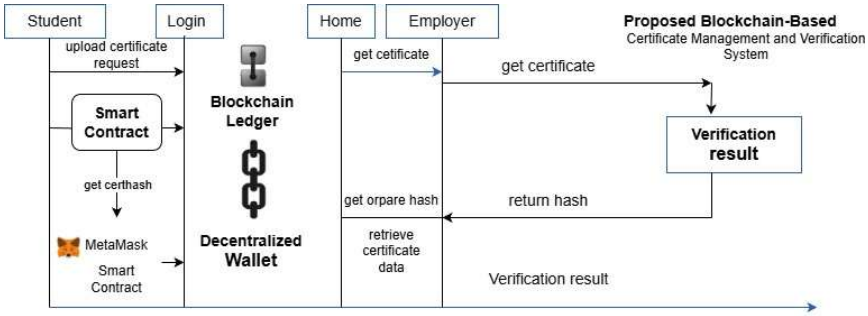

Fig 1. Illustrates the Proposed Blockchain-Based Certificate Management and Verification platform. It provides the complete workflow of certificate issuance storage and verification using blockchain technology in a structured and protected manner

A. Methodology

The functionalities of the administrators include:

- Login Interface : The administrators get permitted access to the page where they can check the valid certificates by entering their details, that is email, password or other credentials.
- Addition of Certificate : Administrators checks student details for certificate generation. Once a cryptographic hash of the certificate is stored on the blockchain, the student itself receives their login details via their email id.
- View All Certificates : The details of students will be shown with the availability of edit options, the admin can edit the record of a particular student.
- Verify Certificates : This core section where the uniqueness of each digital certificate is validated using blockchain technology. When a certificate is put for verification, the platform evaluates its cryptographic hash and compares it with the actual hash or key stored on the blockchain. If both hashes match, the certificate is confirmed as authenticated; otherwise, it is marked as fake or forged. The results after verifying certificates are displayed on the interface, and it shows details of valid and invalid certificates in the given verification dataset.

- Profile Updating : The Admin can update the details or change the password for security reasons. This ensures that only authentic users can upload and verify the certificates on the platform.
- Queries : The queries asked by students or recruiters regarding certificate issues (such as access errors or verification failures) are written under the Pending Queries section in the Administrator portal. After reviewing, the admin checks the issues and answers to the problems listed under the pending Queries section after getting answered the issues moves to the list of answered queries section.
- Solution : The administrator will check the problems and provide the solution in cases like if the certificate contains the wrong information about the student, it can re-issue the certificate.

The functionalities of the student include:

- Update Profile ; Student can change his/her password and see their certificates. Students can check if their details are entered correctly. If any field is wrong then can again issue the certificate or ask the admin to edit the certificate or resolve the issue.
- Login module ; Students can login to the certificate verification portal using the user id and password that they get after registering to the portal. They have a specific role on the portal as student so first they register their details as a student then they get that user id and password for su
- View Certificate Module ; Students can view all their blockchain-verified certificates issued by the institution.
- Every certificate consists of details or fields such as course name,duration of course, issue date, issuing authority, principal signature, unique blockchain transaction id or certificates that share them directly with recruiters for verification purposes.

The functionalities of the recruiter include:

- Login module : Recruiters can log in to the blockchain certificate verification portal after entering the user id and password through which they were registered to the portal. Once authorized, they gain protected access to the verification dashboard where they can check the certificate that is stored on the blockchain network.
- Recruiters verify the legitimacy of a student's certificate by uploading the certificate file or entering its unique transaction ID. The platform evaluates the crypto hash of the certificate with the hash stored on the blockchain. If both hashes match, the certificate is acknowledged as

valid and tamper proof, otherwise it is marked as invalid or altered. The verification results are displayed as soon as the certificate is validated, ensuring reliability in the recruitment process.

B. The platform Model

The Fig2 illustrates the overall platform architecture of the proposed blockchain-based certificate management and certification platform.

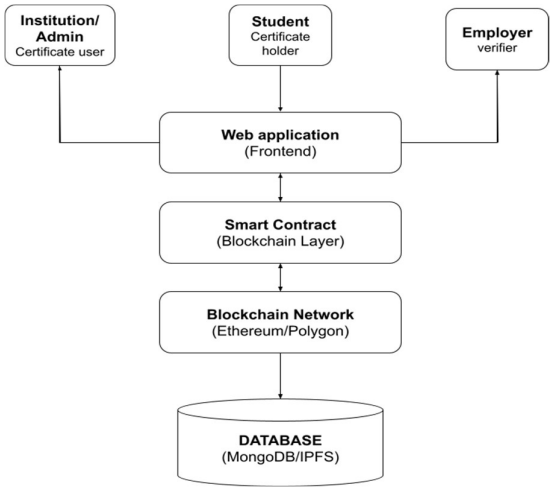

Fig. 2. Architecture of Blockchain-Based Certificate Verification platform

The platform architecture of the Blockchain-Based Certificate Management and Verification platform is made in such a way that provides authenticity, transparency. The architecture is made in a way that combines backend, frontend, blockchain and database layers, providing a seamless and safe workflow for students, institutions, and employees. The architecture is built to ensure a reliable, protected and decentralized framework.

The platform comprises three main entities:
Certificate Issuer (Institution/Admin) : Responsible for generating and issuing certificates.
Certificate Holder (Student) : Receives, stores, and shares certificates protectly.
Verifier (Employer) Responsible for verification of certificates using the blockchain data.
Communication among these entities is established through a web application that interacts with a smart contract deployed on the blockchain network (Ethereum or Polygon). The MongoDB database is used to store off-chain data such as user profiles and non-sensitive metadata.

C. The Threat Model

The development of the Blockchain-based Certificate Management faces certain risks like fake or forged certificates or someone trying to change the grade or details of the certificate.
Also someone prints the certificate that was never really issued or someone successfully changes the details on a real certificate.

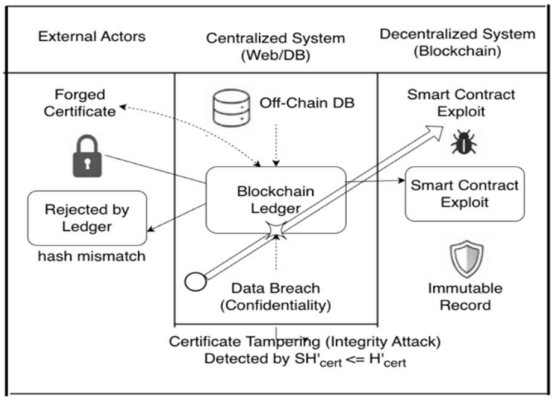

Fig. 3. Threat Model

Threat Model can be thought of as a security inspection for a certificate platform before it's built. Our main objective is to identify unauthorized entities and analyze capabilities to overcome all threats and malicious activities.
Fig3. tells us about the primary threats to the Blockchain- Based Certificate Management and Verification platform and it explains how different components are designed to find the solution of those threats.
The core security challenges in this platform are Certificate tampering that is the integrity attack , Forged PDF certificate that is the authenticity attack.
These threats are decisively solved by the Decentralized platform (Blockchain). When a certificate is generated, this platform generates a unique hash (Hcert) on the blockchain ledger; Now if an attacked tries to tamper with the details of certificate, the verification process recalculates the Hash (H'cert) and now if there is mismatch, it's obvious that the certificate was tampered. While the centralized platform (Web/DB) faces risks like data breach , these are contained as the blockchain provides critical integrity , demonstrating that the platform's architecture effectively separates non-critical, scalable data from security-critical proofs.

D. The Smart Contract

The Smart Contract is the core technical component deployed on the decentralized network that is Ethereum. Its purpose is to act as an immutable, reliabilityless ledger that enforces the rules for certificate issuances and enables verification without relying on any Centralized server.
It's a way to reduce complexity, lower costs and to lessen the surface area for code exploits. Here the structure is key because it ensures that only the intended, verified information is permanently recorded. Our design mainly focuses on two functions: adding certificates and retrieving all details of the issuer. The addCertificate function is restricted only to authenticated users, which ensure the integrity of stored data.
While recruiters don't interact directly with smart contracts, their role is crucial, it serves as the important verification source. Recruiters depend on smart contracts for tamper-proof certificates.
Fig.4 illustrates a streamlined system that eases the management of academic and course certificates. Admins create academic certificates and students can upload their course certificates. When verification is done, the certificate hash is matched against the blockchain record, this way authenticity of certificates are maintained.

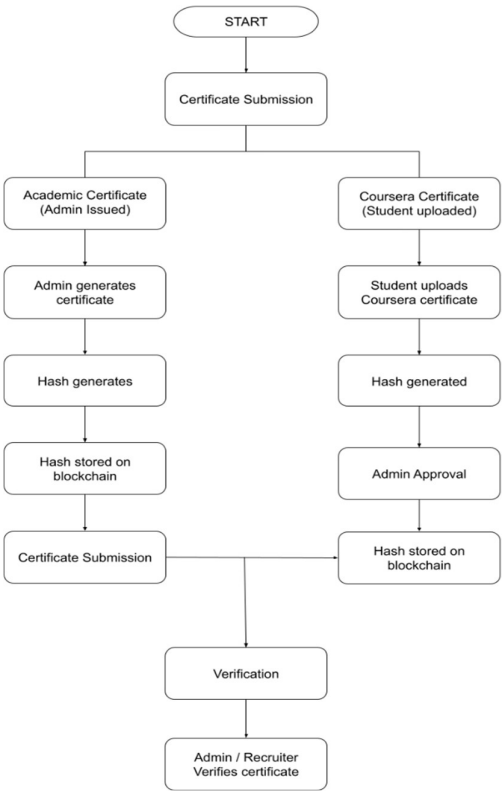

Fig. 4. Smart Contract Workflow for Certificate Verification

V. Evaluation and Results

We built and tested a certificate management and verification platform using Ethereum blockchain, integrated with smart contracts to securely store the certificate's details on the blockchain- where these certificates are tamper-proof and preserved. The hashed data make verification easy, which ensures authenticity of certificates. And we have also included verification of Coursera certificates, which have widened our application of our platform.

A. Performance Evaluation

To enhance our platform's performance, we limit the time for certificate issuance and verification. During development , we started with Ganache which is a local blockchain simulator which is used to test smart contracts and uploading certificates.

Table II: Performance Evaluation Results

Operation	Average Time	Gas Cost
Certificate Issuance	6.2	42,000
Certificate Verification	2.1	18,000
Certificate Revocation	4.5	30,000

Table II illustrates the time and cost difference between verification and issuance of certificates. Since we are just comparing hash on the blockchain, this comparison is valid. Gas usage can be reduced by storing only meta data on-chain and not full certificates.

B. Security and Robustness Analysis

Our platform solves common certificate threats like tampering of certificates, modification of data and many more. When users change the certificates, it matches the hash, if it does not match, it is marked as fake. Only approved issuers get access to create certificates. These observations show the platform's resistance to tampering, fake data and many other threats.

C. Comparison with Existing Approaches

TABLE III: COMPARISON WITH TRADITIONAL VERIFICATION METHODS

platform	Verification Speed	Security Level	Tampering Risk
Manual Verification	Slow	Low	High
Centralized Database	Medium	Medium	Medium
Proposed Blockchain	Fast	High	Very low

Table III illustrates the verification speed varies on different platforms, strength of security provided on each platform, and also shows the risk of tampering in different data storing platforms. This table concludes that blockchain is a highly secure and transparent platform with high verification speed. These factors make this platform more efficient, scalable and reliable.

D. Sample Output Screens

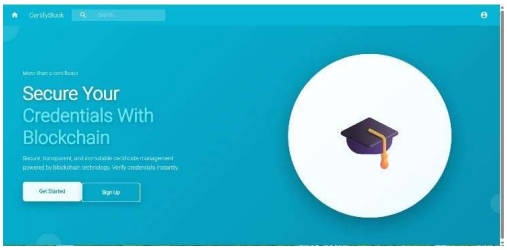

Fig.5 Login or Sign-up Page

Fig.6 Coursera Certificate Verification Dashboard

Overall, The goal is to protect Certificates for Management and Verification using Blockchain. It prevents duplicate academic certificates and makes it trust worthy and it solves issues of fake certificates

VI. CONCLUSION AND FUTURE WORK

In the present scenario in the educational and employment area, fake certificates have become a big problem. Academic Credentials has become very important. To solve this problem, a protected clear platform to verify all the real or fake certificates. This platform stores certificates in a secured digital system called Blockchain It cannot be changed to tampered by anyone. Hence it ensures integrity, reliability, honesty, trustworthy and transparent.

The platform will allow students to upload the course certificates and store them permanently in blockchain. Since blockchain records are not changeable and certificates will remain original and safe. Students can see their certificates at any time anywhere. Recruiters can also see and verify those Student certificates through blockchain. This system uses an approach to improve data security, reduces verification time, improves accuracy and removes manual verification and it is more protected.

The clear platform of blockchain CertiBlock will show that it can solve the problems of centralized verification systems. Storing data at one place instead of that blockchain stores it in a secure manner and it gives tamper-resistent certificates. This blockchain technology overcomes the weakness in traditional systems effectively and keeps data always available. It builds trust among Recruiters, Students and Colleges.

Testing will show that the proposed system reduces certificate verification time by around 50% and reduces administrative work and Recruiters work using automation. It decreases human effort using blockchain technology.

Decentralized Identity (DID) frameworks allow users to manage, control and ownership of their personal information.

These Certificates can be issued in digital form. It gives each student a very unique identity. Each NFTs make a unique hash id or certificate. AI will detect fake or fraudulent activities by default/automatically. A mobile user can be developed to allow users to verify certificates quickly from anywhere and anytime.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[2] M. Sharples and J. Domingue, “The Blockchain and Kudos: A Distributed System for Educational Record, Reputation, and Reward,” in Proc. 11th European Conf. on Technology Enhanced Learning, Lyon, France, 2016.

[3] N. Chalaemwongwan and W. Kurutach, “Blockchain-Based Transcript Authentication System,” in Proc. IEEE 3rd Int. Conf. on Computer and Communication Systems, 2018, pp. 186–190.
[4] P. Raj and G. Deka, Blockchain Technology: Platforms, Tools, and Use Cases. Academic Press, 2018.
[5] U. Rahardja, A. N. Hidayanto, P. O. H. Putra, and M. Hardini,“Immutable Ubiquitous Digital Certificate Authentication Using Blockchain Protocol,” J. Appl. Res. Technol., vol. 19, no. 4, pp. 308–321, 2021.
[6] A. Tapas, S. Patil, and D. Gujarathi, “Decentralized Education Certificates Verification System Using Blockchain,” in Proc. IEEE Int. Conf. on Smart Technologies for Smart Nation, 2019.
[7] X. Liang, J. Zhao, S. Shetty, and D. Li, “Towards a Blockchain-Based Trust Model for the Internet of Things,” in Proc. IEEE Int. Conf. on Services Computing, 2017.
[8] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in Proc. IEEE Int. Congress on Big Data, 2017, pp. 557–564. S
[9] R. Malik, A. Khanna, and N. Kaur, “Blockchain for Education: Secure and Transparent Credential Verification System,” Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 5, 2021.
[10] Y. Zhang, Y. Chen, and J. Peng, “Blockchain-Based Digital Certificate Verification System Design and Implementation,” IEEE Access, vol. 9, pp. 24456–24464, 2021.
[11] A. Gräther, A. Kolvenbach, S. Ruland, C. Schütte, and F. Wendland, “Blockchain for Education: Lifelong Learning Passport,” in Proc. 1st ERCIM Blockchain Workshop, Barcelona, Spain, 2018.
[12] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, “Blockchain-Based Applications in Education: A Systematic Review,” Appl. Sci., vol. 9, no. 12, p. 2400, 2019.
[13] N. 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.
[14] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, “Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends,” IEEE Trans. Syst., Man, Cybern.: Syst., vol. 49, no. 11, pp. 2266–2277, Nov. 2019.
[15] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, “Blockchain-Based Medical Records Secure Storage and Medical Service Framework,” J. Med. Syst., vol. 43, no. 1, pp. 1–9, 2019.