Ms. Pradnya Patil, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Verifying Digital Academic Credential Using Blockchain

Ms. Pradnya Patil[1], Omkar Karade[2] , Soham Vare[3]
[1,2,3]Department of computer engineering

Abstract- In today's increasingly digital and global environment, traditional methods of issuing and verifying certificates are prone to fraud, loss, delays. This solution introduces a blockchain-based system for storing and protecting academic credentials, where educational institutions issue digital certificates directly onto a blockchain network based webapp, Blockchain network mean's Polygon Amoy. In which, the user will be able to have all the control related to it's credentials and not the institution, as sometimes personal information of users can get leaked by institutions which is a breach of smart contract, so this webapp will ensure full control to the users. Through the use of smart contracts, the system automates the verification process, which will be directly issued to the intended user and also will adapt paperless system which will be environment friendly. This approach not only reduces the dependency on educational institutions it will also help to save paper which is the major factor for such credentials/certificates.

Keywords: Blockchain Technology, Polygon Amoy Network, Metamask Wallet, Academic Credential, Smart Contract, Ngrok, Certificate Record, Digital Record.

I. INTRODUCTION

Digital revolution had made the process of credential verification more easy and accurate as proper logs were maintained virtually without any physical form or shape . Previously certificates were printed and authenticated using signatures or stamps which were much easy to forge or replicate , but there was no medium for verifying authenticity of credentials . But now digitization has made easy to maintain records. First step was to control or have a responsible person for certificate issuing purpose . Next was to store all the data into centralize database and then use it for verification purpose. But it had its own limitation like centralized server can be easily taken down with cyber attacks [1]. To overcome this decentralized storage systems like blockchain was implemented , it solved all problems like privacy , security and ease of access but it increased the overall computational requirement . It was advantageous to use it in small institution with overall less data . Hence a new prototype was developed which used POS (Proof of Stake), where only specific data regarding the credential is stored on the blockchain network effectively reducing gas fee , storage cost [5]. Another method was using different type of blockchain consortium model which has mixed properties of public and private blockchain which has potential more upsides and less downsides . To narrow down even more private blockchain is implemented which has more restriction , but allows more control over network and storage capacity [7]. In real world scenario blockchain has been found more reliable and accurate than the traditional approach , hence implementation ofour system will lead to effectively eliminate all the potential downsides like complexity , large storge , high computational demands with effective and selective use of blockchain for storage and administrative rights for uploading certificates and using unique code for seamless verification .

II. LITERATURE REVIEW

Cardenas-Quispe A Blockchain ensuring academic integrity with a degree verification prototype[1]

This research develops the functional prototype using the python to secure the academic credentials through hybrid blockchain ,mainly it focuses on the technical registration of the data,node

synchronization ,and use of the associative signatures, this that ensures that the Generated creadentials are authentic.There is a significant gap in the actual technical implementation of such systems.most of the existing literature focuses on theoretical frameworks rather than practical ,code execution. Hence addressing issues we have demonstrates the better efficiency with low latency for record signing and block replication,this system has admin panel where certificates are secured and it records unique code on the blockchain to ensure trust and reduce academic frauds.

Moya, J. A. B, Blockchain-Based Academic Record Verification System[2] This system utilizes zero knowledge proofs to allow students to prove the status of certification without revealing underlying sensitive personal data. It has dual blockchain architecture to make the balance between the transparency of public chain with the privacy of a private one. While it provides strong privacy ,they involve high computational cost and more financial overhead that makes it difficult to sustain for long-term.

Many digital certificate method are vulnerable to tampering during the sharing phase. To overcome it proposed system solves this privacy concern by not giving any student login feature which removes the third party exploitation of vulnerabilities,instead of high-compute proofs,we use the system-generated QR code that will prove authenticity of certificate.

Oluwaseyi, Blockchain Technology for University Certificate Verification System, [3] In this system they study on Ethereum-based system where issued certificate and metadata stored on the blockchain while the actual certificate or file are kept in decentralized storage.In this system it send 5 word mnemonic password sent to student,this password are required for verification process. While traditional paper-based systems are follow that can easily forged and digital mnemonicsystems have a disadvantage like if mnemonic is generated by known algorithm that can easily be predicted or duplicates once the algorithm was compromised.In our system, to avoid the predictability of algorithm-generated codes our system are allows to free to choosing unique code. This code was shared between institution(admin) and studentand they also insuring not easily predicted by any third parties while remain simple for student to remember unique code compare to 16-character hashes Abdelmagid.

R. A Blockchain Framework for Academic Certificates Authentication [4]

This system work on a permissioned Hyperledger fabric network are manage student data like information and certificate issuance . This is private channels and smart contract like chaincode to reach higher transaction per second(TPS) and lower latency compare to public network like bitcoin and Ethereum. But system follow traditional institutional databases are highly unsafe to external attacks and also internal issues.In this system public blockchain are required high gas fees when try to storage huge amounts of certificate data on the ledger. Our system are gives a database vulnerabilities by storing the unique certificate codes on imitate in blockchain. To resolve the high costs associated with public ledger , we can not store whole contain on blockchain, the admin store the certificate in database and certificate information and records like encrypted hash or code store on the blockchain to reduce transaction costs.

Rahman, Verifi-Chain[5]

Verifi-chain system is based on decentralized system that can integrated blockchain with the Interplanetary File System(IPFS).Certificate are store in IPFS and Then system are generate hash code and This particular Hash code are stored in blockchain an they make sure to provide a non repudiable and tamper proof electronic record.In this system storing full document contain in blockchain is requires huge amount of storage capacity. Centralized verification also remains a hold up then often relies on third party intermediaries which can be a single point of failure. We also follow similar logic, In our system implements Database for storage to certificate to reduce load on blockchain.The admin are issue the certificate and issues a unique code to student,store this code on blockchain and create excel sheet for simple and seamless future authentication and eliminates the any centralized third party verification.

Rustemi, A Blockchain-Based Systems for Academic Certificate Verification[6]

In this system they analyzes studies on blockchain's role in education. It highlights how decentralized ledgers eliminate reliance on intermediaries and create a record of ownership that is resistant to unauthorized changes.In previous system common problem identified in previous methods is the use long hashing process for verification, which are difficult for users to remember and understanding ,they can lead to high level of input error during certificate verification process. In our system simplifies the verification work by using a secret or unique code and system are generated QR and shear link of certificate. This process make trouble free for student and verifier. As the QR can be scanned to show certificate directly on mobile phone without the need for enter hash manually or link will send on mobile or any device directly and they do not need complex login process.

Serranito, Blockchain Ecosystem for Verifiable Qualifications[7]

This system are proposes an ecosystem using Ethereum based and smart contract that allows higher education institution to register for issuing certificate.it allows recruiters to authentic verification directly against the blockchain records without contacting the university or institution. Historicallay, physical stamps and signatures were used for certificate verification process, But now in digital world , these process sassily manipulated by using image editing software or tools. Even digital signature and watermark also potential drawback regarding manipulation and case to certificate verification. In our system avoid the risk of digital image manipulation by using a logical control over the issuing certificate authentically . If admin attempts to claim a forged certificate is real,then unique code stored on blockchain then source of truth that anyone can to verified certificate's as true status.

Fartitchou, BlockMEDC[8]

In this paper introduce BlockMEDC,A sysyem are based on Ethereum smart contracts and IPFS to provide secure and manage certificate process.This system Aim to decentralize certificate storage to ensure transparency and security in system. Public blockchain network like Ethereum can face significant issuance problem and required high transaction cost mean's gas fees when large volume of certificates are issued and managed on blockchain. Our system optimizes storage by utilize mogoDB database for off chain storage of the file.We only keeping cryptographic hashes in blockchain . our project follow this logic by storing certificate in an encrypted format , they can reduce the transaction costs like gas fees storage demands compared to traditional methods.

Ifeyemi, Blockchain-Based Digital Educational Certificate Verification System[9]

In this system develops a verification system using the celo blockchain, they ca gives mobile first access. It allows institution to issue digital certificates that can store permanently in decentralized ledgers. making them easily verification process. In previous system they are depends on algorithm generated process, Identifier that can be predicted once the generation logic is known and also long verification hash is difficult for verifier to manage manually. In our system we are providing free choose to issuer to select unique code for certificate by issuer they can shared privately with the student,which eliminates predictability. Also system generate QR and link of certificate for making verification process seamless and problem free.

III. METHODOLOGY

Here is a proposed highly effective methodology for your project .Synthesizing the best practices from the research papers you provided. This architecture balances security, cost-efficiency and user-friendliness.

The system begins with a secure entry point where institutional issuers mean's admin must go with strict authentication process. Admin access the Student Credential DApp platform by using email and password login process. After login Admin enter credential details , To facilitate operation on the decentralize network the admin account utilize MATIC Tokens. These tokens are critical for covering the computational cost like gas fees required to

interact with smart contract and process transaction on the blockchain network mean's polygon amoy network and ensuring that only authorize funded accounts can initiate the certificate issuing process. Once we complete securely authentication, then admin is gather the necessary information to issue digital certificate on the platform or portal. During this process, the system processes the specific information like metadata and student information enter by the admin to issuing the digital certificate. A core security feature of this stage is the unique code identification to each individual certificate. This unique code acts as the primary cryptographic identifier and linking student's academic achievement to a verification record.

In this system, the system executes a dual-storage operation to handle both security and platform efficiency. In first phase, the actual digital certificate file encrypted to protect sensitive data or information and hosted on a regular or reliable storage platform to avoid the huge amount of costs of storing certificate or large file directly on a distributed ledger. During this phase simultaneously, a blockchain transaction is initiated to record the certificates unique code and associated cryptographic proof on the polygon amoy testnet network. Polygon amoy testnet ensures an immutable, tamper proof record of the certificate. They also maintain high transaction throughput and low network fees. In this transaction they use MATIC tokens for gas fees.

In the final phase they are focuses on maximizing utility and gives access for third party mean's verifier, such as potential employes or student and other educational institutions. To avoid complexity, verifiers are accessible without any registration or login requirement. They navigate directly to a public certification validation portal and input or enter certificate's unique code. The system are queries the blockchain to validate code or not. If done successful authentication, then system are generates a shareable QR and link that can direct verification of certificate on mobile. This also allows verifier to view certificate and download instantly certificate. They create a seamless and trouble-free verification exprerince.

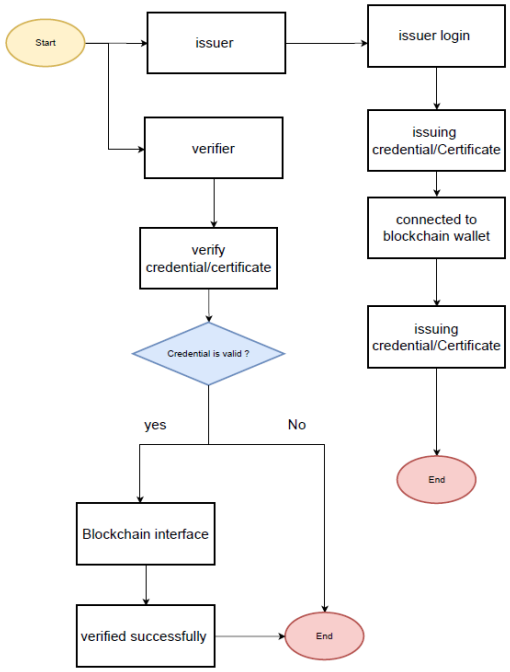

Figure 1. System Architecture

This is the system architecture which has been implemented into the project it has three main stages which are as follows :

In the first step a admin form a respect institute will have rights to issues a valid certificate and generate a unique code which can be use for future verification and it will be stored on blockchain network with a secure transaction using meta mask wallet and stored on polygon amoy blockchain network . Here only admin can post certificates on the system so to stop forged documents from getting Authenticated .

Once the certificate is verified and issued the transaction will be initiated and confirmed through meta mask wallet using cryptocurrency named matic which is free use for development and testing purposes . After it is confirmed and gas fee is under limit transaction takes place and certificate is stored Now the certificate is issued and can be verified through the system using unique code or shared QR code . Once the code is entered the certificate is displayed and can be shared with other authority.

If a student want to share his credentials but do not want to share his private information like unique code then he can simply generate a qr code and then can send it to respective receiver and then he can view it with scanning the qr code or sharing the link so he can directly view it on mobile phone.

IV. RESULT AND ANALYSIS

Issuer Or Admin Login Page:

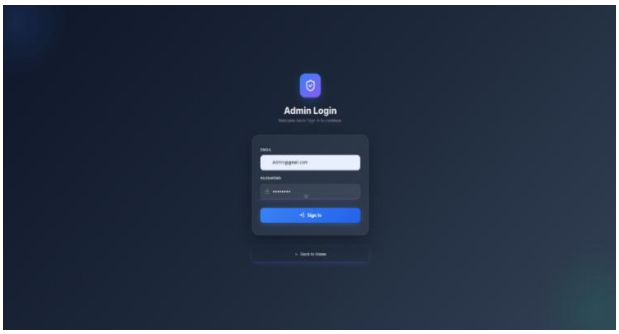

Figure 2 : Admin login page

This image displays a clean, modern user interface (UI) designed specifically for an Administrator Login page. Its purpose is to securely authenticate a user before granting them access to the backend or administrative controls of a system.

Issuer interface:

Figure 3 : Admin Dashboard

This image shows the main dashboard or landing page for a web application called the Student Credential DApp (Decentralized Application). Based on the text and layout, this platform uses blockchain technology to securely handle educational records.

Certificate uploading and issuing:

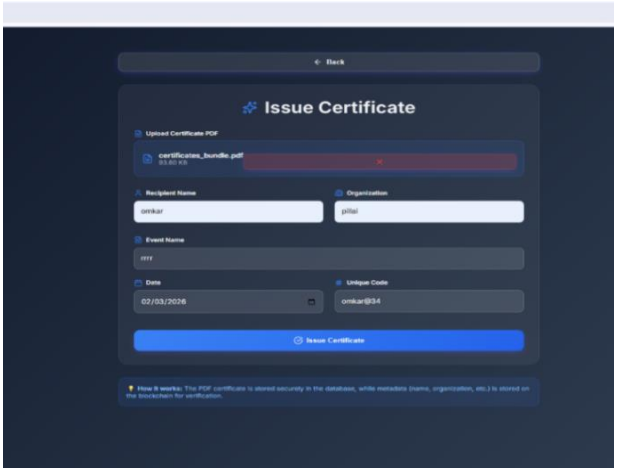

Figure 4 : Issuer page

This Issue Certificate screen is a form where administrators create tamper-proof credentials. They simply upload the certificate file (which goes to a database) and enter the student's details (which are locked securely on the blockchain).

User and verifier interface:

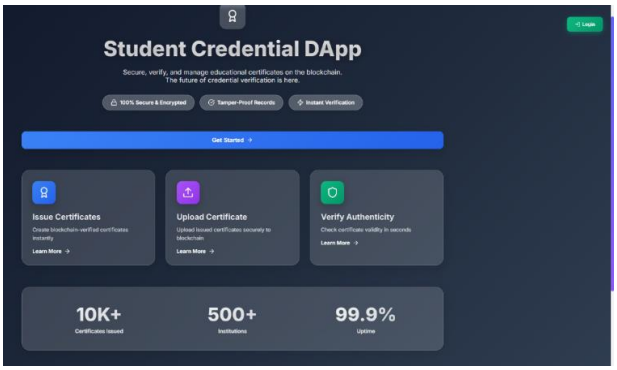

Figure 5: Verifier Dashboard

It's basically user or verifier dashboard , they can use for only verifying credential or certificate purpose.

Verifying Certificate Page:

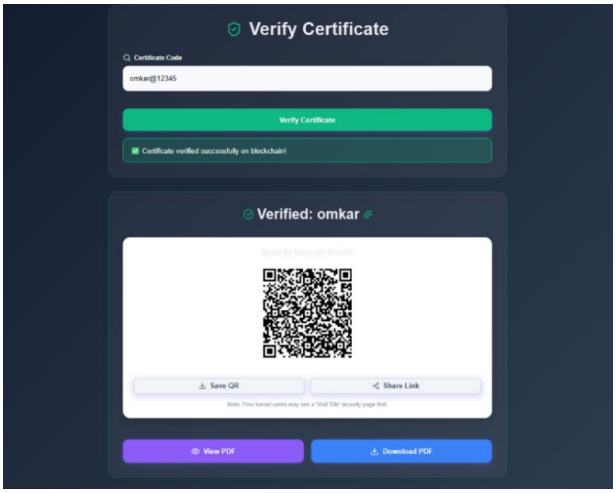

Figure 6 : Certificate Verifying page

In this dashboard show , Securely managing educational records. Logged-in admins use the platform to issue tamper-proof certificates by saving the document to a database and locking the student's details on the blockchain. They can use QR or link for easy access Meanwhile, a public interface allows anyone like potential employers to instantly verify those certificates without needing an account.

V. CONCLUSION

Hence ability of individual can be predicted using certifications as proof of skill . But validating credentials has become a major task due to not knowing authenticity of certificates . Physical certificates were easy to forged and also digital but verification is much more accurate and reliable then physical authentication . In digital world all logs are stored and maintaining logs is crucial task hence block chain plays a crucial role in maintaining these logs .Then only it can be used to verify the authenticity of certification. By integrating instant QR code verification, the framework bridges the physical and digital divide, empowering employers and institutions to authenticate academic records in real-time without relying on costly, time-consuming third-party intermediaries. Ultimately, this tamper-proof infrastructure establishes a new standard for academic integrity, fostering a trusted ecosystem where educational achievements are immutable, transparent, and effortlessly verifiable also has reliable and seamless operations.

REFERENCES

1. Cardenas-Quispe, M. A., & Pacheco, A. (2025). Blockchain ensuring academic integrity with a degree verification prototype. Scientific Reports.

2. Moya, J. A. B., Ayoade, J., & Uddin, M. A. (2025). A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System. Sensors, 25(11), 3450.

3. Oluwaseyi, O. S. (2024). Utilizing Blockchain Technology for University Certificate Verification System. International Journal of Applied Information Systems (IJAIS), 12(45).

4. Abdelmagid, R., Abdelsalam, M., & Alsheref, F. K. (2024). A Blockchain Framework for Academic Certificates Authentication. International Journal of Advanced Computer Science and Applications (IJACSA), 15(7).

5. Rahman, T., Mouno, S. I., Raatul, A. M., Azad, A. K. A., & Mansoor, N. (2023). Verifi-Chain: A Credentials Verifier using Blockchain and IPFS. arXiv preprint arXiv:2307.05797.

6. Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2023). A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification. IEEE Access, 11, 64684-64696.

7. Serranito, D., Vasconcelos, A., Guerreiro, S., & Correia, M. (2020). Blockchain Ecosystem for Verifiable Qualifications. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS).

8. Fartitchou, M., Lamaakal, I., El Makkaoui, K., El Allali, Z., & Maleh, Y. (2024). BlockMEDC: Blockchain Smart Contracts for Securing Moroccan Higher Education Digital Certificates. IEEE Access.

9. Ifeyemi, T., Oyedeji, A., & Adebiyi, F. (2024). A Blockchain-Based Digital Educational Certificate Verification System. Journal of Engineering and Technology for Industrial Applications (ITEGAM-JETIA), 10(49), 35-41.

10. Sultana, S. A., Rupa, C., Malleswari, R. P., & Gadekallu, T. R. (2023). IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field. Information, 14(8), 446.

Author's Details

1. Ms. Pradnya patil, Department of Computer Engineering , Pillai HOC College of Engineering and Technology, Maharashtra,India,pcavarka@mes.ac.in
2. Omkar karade, Student , Department of Computer Engineering , Pillai HOC College of Engineering and Technology, Maharashtra , India , omkarrk22hcompe@student.mes.ac.in
3. Soham Vare, Student , Department of Computer Engineering , Pillai HOC College of Engineering and Technology, Maharashtra, India, sohamdv22hcompe@student.mes.ac.in