Blockcertify - A Digital Certificate Verification System

Yash Pravin Karpe[1], Mayur Santosh Bhuran[2], Aditya Janardan Dere[3], Prof. Archana Mate [4]
[1 2 3]*Students, Department of Computer Engineering, Dilkap Research Institute of Engineering and Management Studies, Neral*
[4] *Professor Department of Computer Engineering, Dilkap Research Institute of Engineering and Management Studies, Neral*

***Abstract*—Digital certificate forgery and manipulation pose serious challenges in academic and professional verification systems. Traditional verification methods depend on centralized authorities, resulting in delays, high costs, and security risks. This paper proposes Block Certify, a block chain-based digital certificate verification system that ensures authenticity, immutability, and transparency. Certificate hashes are stored on a block chain ledger, enabling instant and trustworthy verification without third-party involvement. The system enhances trust, reduces verification time, and prevents document tampering.**

***Index Terms*— Blockchain, Certificate Verification, Digital Security, Smart Contracts.**

I. INTRODUCTION

Document verification is an essential process in education, recruitment, banking, and legal transactions. However, conventional systems often face challenges like delays, high costs, lack of transparency, and vulnerability to manipulation. Block chain technology offers decentralized, distributed, and immutable data storage, making it ideal for solving these issues. Block Certify aims to provide a block chain -based platform where documents can be securely issued, stored, and verified with cryptography proof of authenticity.

Currently, the process of generating certificates is handled educational institutions and government agencies. These certificates play a crucial role in admission procedures and job applications.

However, a major challenge arises from the fact that most educational institution certificates are in physical form, which creates difficulties in verifying their authenticity, sharing them with relevant agencies, storing them securely, and incurs high costs due to manual handling.

II. LITERATURE REVIEW & RESEARCH GAP

Block chain technology has emerged as a promising solution for secure and tamper-proof document verification due to its decentralized architecture, cryptography security, and immutable ledger properties. Researchers have extensively studied its application in academic credential verification to address challenges such as forgery, delayed validation, and centralized trust dependencies.

Satoshi Nakamoto (2008) introduced blockchain as a distributed ledger technology that ensures data integrity through cryptography hashing and consensus mechanisms. This foundational work established immutability and trustless verification, which are critical requirements for secure certificate validation systems.

Zibin Zheng et al. (2017) presented a detailed analysis of block chain architecture, including consensus algorithms, smart contracts, and decentralized applications. Their study highlighted block-chain's ability to eliminate centralized intermediaries while maintaining transparency and security, making it suitable for digital credential authentication.

Melanie Swan (2015) explored blockchain applications beyond cryptocurrency, emphasizing identity management and academic record verification. The research demonstrated how blockchain can provide self-sovereign identity control and verifiable credentials without reliance on third-party authorities.

Kim et al. (2020) proposed a blockchain-based university certificate authentication system that

stores cryptographic hashes of certificates on-chain while maintaining the actual documents off-chain. Their approach improved system efficiency and reduced storage overhead, but lacked scalability evaluation and real-world deployment analysis.

RESEARCH GAP

From the comparative analysis, it is evident that while block chain-based certificate verification systems ensure security and immutability, many lack practical deployment models, user-friendly verification interfaces, and integrated revocation mechanisms. Moreover, limited focus has been given to balancing on-chain security with off-chain scalability.

To overcome these challenges, the proposed Block Certify system integrates smart contracts, hash-based verification, and a web-based verification portal with off-chain storage, providing a scalable, secure, and user-concentric digital certificate verification solution.

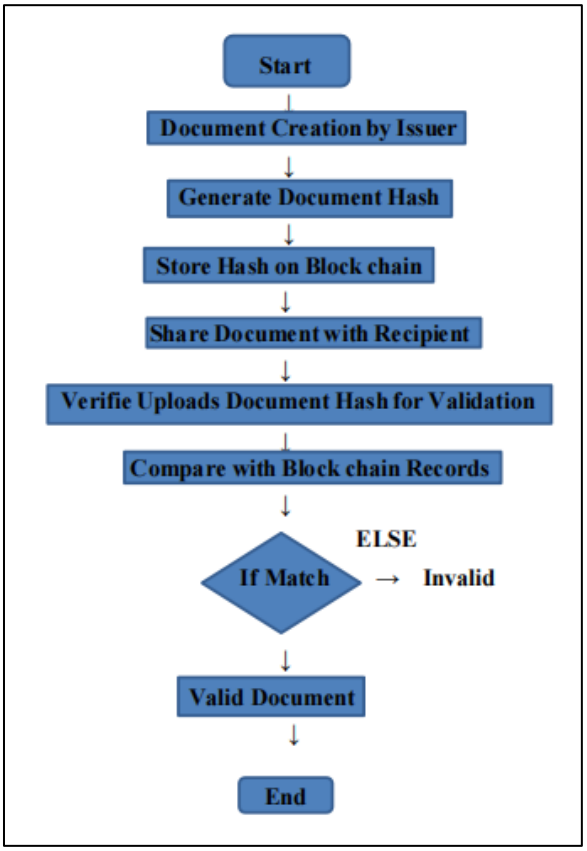
III. PROPOSED SYSTEM

The proposed Block Certify system is a decentralized digital certificate verification platform designed to eliminate forgery, unauthorized modification, and dependency on centralized verification authorities. The system leverages blockchain technology to store cryptographic proofs of certificates, ensuring immutability, transparency, and trust.

Instead of storing complete certificate files on the blockchain, the system generates a cryptographic hash of each certificate using the SHA-256 algorithm. This hash acts as a unique digital fingerprint and is permanently recorded on the block chain along with issuer details and timestamps. Any alteration in the certificate content results in a different hash, making tampering immediately detectable.

The proposed system allows

- Issuer (e.g., universities, employers) to upload document metadata to blockchain.
- Blockchain Network to store document hash (unique digital fingerprint).
- Verify to check authenticity by comparing document hash with blockchain entry



IV. METHODOLOGY

The methodology defines the step-by-step technical process used to implement the Block Certify system.

Step 1: Certificate Generation

The issuing authority generates a digital certificate in PDF or JSON format containing recipient and credential details.

Step 2: Hash Computation

The certificate file is processed using the SHA-256 hashing algorithm to generate a fixed-length hash value. This ensures integrity and uniqueness.

Step 3: Blockchain Registration

A smart contract is invoked to store the generated hash, issuer ID, timestamp, and certificate type on the block chain.

Step 4: Off-Chain Storage

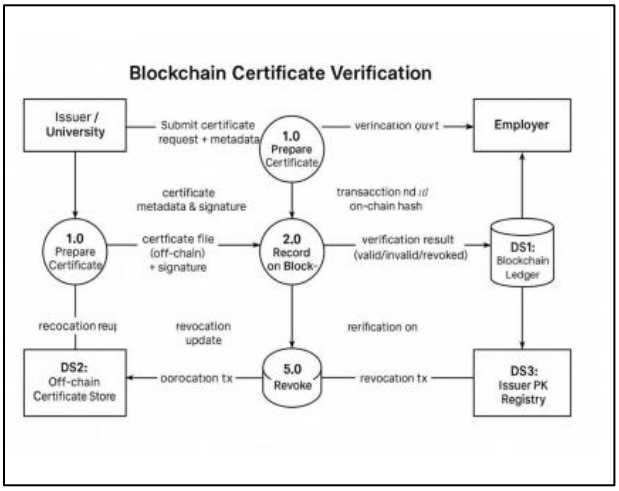
The actual certificate file is stored securely off-chain, while the blockchain maintains proof of authenticity.

Step 5: Verification Process

During verification, the uploaded certificate hash is recomputed and compared with the block chain record. A match confirms authenticity.

Step 6: Revocation Handling

Issuers can revoke certificates by updating revocation status on the block chain without deleting historical records



V. HARDWARE AND SOFTWARE REQUIREMENTS

Hardware Requirements:

Sr. No.	Component	Specification
1	Device	Laptop / Desktop Computer
2	Processor	Intel® Core™ i5 or Intel Pentium 3 / Core 2 Duo / Dual Core
3	RAM	Minimum 4 GB
4	Storage	At least 200 MB free disk space

Software Requirements :

Sr. No.	Software	Specification / Purpose
1	Operating System	Windows 7 or Windows 10
2	Programming Language	Python 3.10 (64-bit)
3	Development Environment	Visual Studio
4	Documentation Tools	Notepad, Google Chrome, Microsoft Word

VI. CONCLUSION

Block Certify simplifies the document verification workflow for both institutions and individuals. It reduces administrative delays, prevents fraudulent claims, and enhances trust between issuers and verifies. The solution is a step forward toward digital transformation and can be extended to various domains such as academic certificates, identity proofs, and legal records.

REFERENCES

[1] MIT Media Lab, Blockcerts – Open Standard for Blockchain Certificates, 2016.
[2] Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamoto, S. (2008).
[3] 3.An Overview of Blockchain Technology: Architecture, Consensus, and Applications. IEEE. Zheng, Z., et al. (2017).
[4] 4.Blockchain Technology: Beyond Bitcoin. Applied
[5] Innovation Review. Crosby, M., et al. (2016)
[6] 5.The history of OCR, optical character recognition.
[7] [Manchester Center, Vt.]: Recognition Technologies Users Association. ISBN. Schantz, Herbert F. (1982).
[8] 6. "On a Type-Reading Octophone" . Proceedings of

[9] the Royal Society A: Mathematical, Physical and Engineering Sciences .d'Albe, E. E. F. (July 1, 1914).
[10] 7. S. Kim, J. Kim, and H. Lee, “Blockchain-Based University Certificate
[11] Authentication System,” IEEE Access, vol. 8, pp. 139911–139920, 2020.
[12] IBM Block chain, “Block chain for Certificate Authentication,” IBM Developer Portal, 2023.
[13] S. Kim, J. Kim, and H. Lee, “Blockchain-Based University Certificate
[14] Authentication System,” IEEE Access, vol. 8, pp. 139911–139920, 2020.
[15] 10.Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[16] Zibin Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Applications,” IEEE Access, vol. 5, pp. 557–564, 2017.
[17] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain Technology: Beyond
[18] Bitcoin,” Applied Innovation Review, no. 2, pp. 6–10, 2016.
[19] Melanie Swan, Blockchain: Blueprint for a New Economy, O’Reilly Media, 2015.
[20] Garcia-Alfaro, G. Navarro-Arribas, and J. Herrera-Joancomartí, “Securing Documents Using Blockchain Technology,” Future Internet, vol. 10, no. 2, pp. 1–17, 2018.