IJARSCT
ISBN: 978-93-5833-924-6
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Research Paradigms in IT: From Theory to Implementation
Impact Factor: 6.252

Enhancing Academic Credentials Security and Verification using Blockchain

Prof. Bhakti Chaudhari and Govind Parab
Nirmala Memorial Foundation College of Commerce and Science, Mumbai, Maharashtra, India

Abstract: *In the realm of education and professional development, academic credentials are essential for verifying an individual's educational achievements and professional qualifications. However, the integrity of these credentials is often challenged by the limitations of traditional paper-based and digital formats. Paper-based credentials are vulnerable to forgery and manipulation, while digital credentials can be easily altered or deleted. This poses a significant challenge for employers, educational institutions, and other stakeholders who rely on these documents to make informed decisions. Blockchain technology, with its inherent properties of immutability, decentralization, and transparency, presents a compelling solution to address these shortcomings and enhance the security and verification of academic credentials. This paper proposes a blockchain-based solution to enhance the security of academic credentials. By leveraging blockchain's immutability, decentralization, and transparency, the system ensures tamper-proof storage. Academic credentials stored on the blockchain become resistant to forgery and unauthorized alterations. The decentralized storage mechanism eliminates reliance on a central authority, mitigating the risk of manipulation and unauthorized access, thus bolstering the overall security and verification process for academic credentials.*

Keywords: Blockchain, Academic Credentials, Security, Verification, Decentralized Storage

I. INTRODUCTION

Traditionally, the certification authority verifies diplomas or certificates because it is difficult to distinguish between genuine and fake certificates without specialized tools and knowledge that the certificate issuer can only provide [1]. Credential fraud in education, involving the falsification of credentials, poses challenges for institutions and employers. Common types include fake degrees, degree mills, transcript fraud, and credential misrepresentation. Fake degrees often use advanced printing techniques, requiring institutions to implement rigorous security measures. Degree mills grant degrees without academic requirements, necessitating awareness and background checks. Transcript fraud involves altering academic transcripts, mitigated by secure formats and blockchain technology. Credential misrepresentation extends to dishonesty in resumes and job applications, countered by thorough checks and promoting integrity. Vigilance is crucial to prevent consequences such as undermining academic integrity and eroding trust in educational institutions and the workforce. Cryptographic techniques used in Blockchain enhance the security and integrity of transactions recorded by a distributed ledger. Blockchain solves the problem of lack of trust by maintaining transaction records to each participating node. Transactions are recorded in a block which is added by a miner using a consensus algorithm. In addition, the Merkle tree generates a cryptographic fingerprint of the entire set of transactions for a block to ensure its integrity and inclusion. The chain is created by storing the cryptographic fingerprint of the previous block [2]. Blockchain technology's potential in enhancing academic credential security gained momentum in 2015, addressing challenges in traditional verification methods. The Blockcerts project by MIT in 2015 pioneered tamper-proof digital academic credentials, marking a significant advancement. Subsequent platforms in 2016 aimed at transparent issuance, storage, and verification of academic records. Pilot projects in 2017 showcased blockchain's feasibility for managing and verifying academic records, leading to increased adoption. In 2018, the focus shifted to interoperability and standardization, fostering a cohesive credentialing ecosystem. Recognition expanded beyond education in 2019, drawing interest from governments and industry players. The COVID-19 pandemic in 2020 accelerated the adoption of blockchain for secure and efficient virtual credentialing. In 2021, developments prioritized user-centricity, data privacy, and integration with educational platforms. The concept expanded in 2022 to include

IJARSCT
ISBN: 978-93-5833-924-6
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Research Paradigms in IT: From Theory to Implementation
Impact Factor: 6.252

various learning experiences, prompting research on blockchain's potential in admissions, student records, and lifelong learning pathways. Ongoing research aims to refine blockchain-based credentialing solutions, positioning blockchain to enhance the integrity, authenticity, and accessibility of academic credentialing.

II. LITERATURE REVIEW

The reviewed literature emphasizes blockchain technology's transformative potential in enhancing academic credential verification and security. Key findings highlight blockchain's capacity to revolutionize the verification process by addressing challenges like forged certificates, manual verification, and data sharing. Key components include distributed ledgers, cryptography, smart contracts, and decentralized storage, offering increased security, efficiency, and transparency. Widespread adoption of blockchain faces challenges such as scalability limitations, privacy concerns, regulatory gaps, automation issues, smart contract immutability, maintenance costs, and energy consumption. Despite these challenges, blockchain holds the promise to revolutionize academic certificate issuance and verification, enhancing overall security, efficiency, and trustworthiness. Numerous studies propose blockchain-based solutions, emphasizing benefits like immutability, traceability, and decentralization in academic certificate verification.

Cerberus is a blockchain-based credential verification system that is designed to be more efficient, user-friendly, and capable of addressing various forms of fraud [3]. **BCert** is a decentralized academic certificate system that utilizes Ethereum smart contracts and IPFS for decentralized file storage [4]. **HEDU-Ledger** is a hyperledger fabric-based system that aims to digitize and secure the degree attestation process, ensuring traceability, validation, and privacy [5]. **UniverCert** is a platform that creates a unified digital register of students educational achievements [6]. **Verifi-Chain** is a system that uses blockchain technology and the Interplanetary File System (IPFS) to create a secure and tamper-proof system for verifying academic credentials [7]. **SmartCert** is another blockchain based digital credentials verification platform. SmartCert is developed to establish the authenticity of academic credentials on a blockchain and to overcome the problem of fake certificates. SmartCert makes use of cryptographic signing of educational certificates to provide transparency in the case of recruitment [8]. **Records Keeper** is another blockchain based solution to verify academic certificates. With RecordsKeeper, educational institutes can issue certificates and provide a receipt to the user which can be shared with a third party to prove the certificate is authentic [8]**.** There are a number of different blockchain-based solutions for verifying academic certificates in development. These solutions are still in their early stages, but they have the potential to make a significant impact on the education sector.

III. RESEARCH METHODOLOGY

Objective Of The Study

The primary objective of this research is to investigate the potential of blockchain technology to enhance the verification and security of academic credentials. Specific research objectives include:

- To identify the key challenges associated with the current academic credential verification process.
- To explore the theoretical underpinnings of blockchain technology and its potential applications in the education sector.
- To design and develop a blockchain-based academic credential verification system.
- To evaluate the effectiveness and efficiency of the proposed blockchain-based system in terms of security, scalability, and usability.
- To analyze the potential impact of blockchain technology on the education sector, including its implications for student privacy and data protection.

Proposed System: The fundamental mechanism of our proposed system revolves around the use of blockchain, a decentralized and immutable ledger.

At foundation level following data will be collected for the system

Credential Information:

- Type: Diploma, certificate, or transcript.
- Identifier: Unique credential ID.

IJARSCT
ISBN: 978-93-5833-924-6
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Research Paradigms in IT: From Theory to Implementation
Impact Factor: 6.252

- Issuer: Institution name and contact.
- Issue Date: Date of issuance.
- Recipient: Student's name and contact.
- Credential Metadata: Program, major, graduation date.
- Credential Hash: Cryptographic hash ensuring the credential's integrity.

Issuing Institution Information:

- Name, ID, address, accreditation status.
- Authorized Representatives: Contact for verification.

Student or Credential Holder Information:

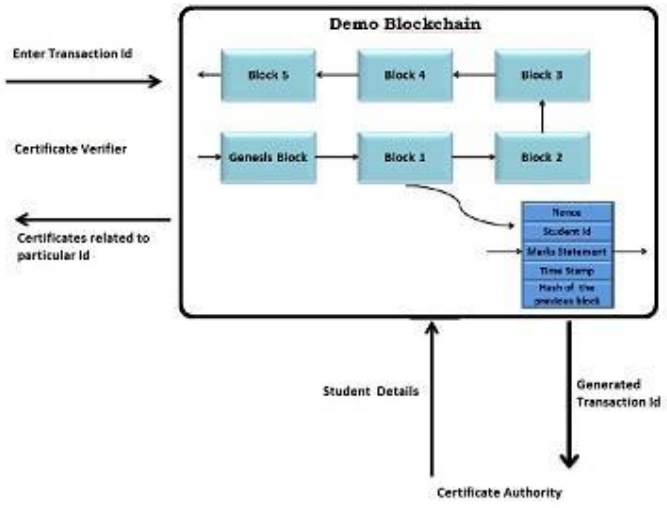
- Name, ID, contact, academic history.

Steps in credential issuance

- Educational institutions issue digital credentials to students upon completion of their studies. These credentials include the student's name, degree, date of graduation, and other relevant information.
- The digital credentials are then hashed and stored on the blockchain. The hash is a unique fingerprint of the credential that cannot be altered.
- The educational institution signs the digital credential with its private key. This signature serves as proof of authenticity and ensures that the credential has not been tampered with.
- The student receives a copy of the digital credential and the hash.

Steps in credential verification

- A potential employer or other stakeholder wants to verify the authenticity of a student's academic credentials.
- The student provides the employer with the hash of their credential.
- The employer can then search the blockchain for the hash and retrieve the corresponding credential.
- The employer can verify the authenticity of the credential by comparing the hash of the credential on the blockchain to the hash provided by the student.
- If the hashes match, then the employer can be confident that the credential is authentic.
- Each student's academic credentials are stored in a block, generating a unique Hash number, serving as the primary key. This pioneering approach facilitates seamless certificate verification for students and empowers employers to validate the authenticity of provided certificates.



To enhance the verification process, every student is assigned a unique Hash Id. This identifier provides a consolidated view of all associated certificates, streamlining the verification process and offering verifiers a comprehensive perspective. Upon the addition of a certificate, a nominal Ethereum gas fee is incurred, debited from the certificate

authority's account. This fee is crucial for compensating miners, essential contributors responsible for adding blocks to the blockchain. In return, miners are rewarded with Ethereum coins, ensuring the sustainability and integrity of the blockchain network. The distributed nature of the blockchain establishes a formidable defense against tampering. While acknowledging that absolute immunity is unattainable, the increasing length of the blockchain significantly elevates the difficulty of unauthorized data modification, providing a robust foundation for secure data storage. The proposed system serves as a pivotal link between educational institutions and industries. Institutions can securely store candidates' academic credentials, and industries can effortlessly verify these credentials using Hash number. The proposed system also serves as a pivotal link between educational institutions and industries. Academic institutions can securely store student credentials on this platform, and industries can effortlessly verify them using Hash numbers.

IV. CONCLUSION

The proposed system is a consortium blockchain designed for collaboration among universities, affiliated and autonomous colleges, and companies to bolster the security and authenticity of student certificates. Operating on a transparent and decentralized ledger, it prevents tampering and unauthorized additions. Universities initiate the process by adding certificates to the blockchain, establishing secure and immutable academic records. Each transaction generates a unique identifier for subsequent verification. Companies verify certificates using the student's Hash Number, adding an extra layer of security. The consortium blockchain's collaborative nature enables multiple institutions to participate, fostering a standardized and universally accepted approach to certificate validation. Blockchain technology ensures data protection and resilience by eliminating single points of failure. The system not only safeguards certificate integrity but also protects students' sensitive data. Leveraging Hash number makes the verification process efficient and reliable, reducing the risk of fraud.

REFERENCES

[1]. Rustemi, Avni, Fisnik Dalipi, Vladimir Atanasovski, and Aleksandar Risteski. "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification." IEEE Access (2023).

[2]. Kaneriya, Jayana, and Hiren Patel. "A Secure and Privacy-Preserving Student Credential Verification System Using Blockchain Technology." International Journal of Information and Education Technology 13, no. 8 (2023).

[3]. Tariq, Aamna & Binte Haq, Hina & Ali, Syed. (2019). Cerberus: A Blockchain-Based Accreditation and Degree Verification System.

[4]. Leka, Elva & Selimi, Besnik. (2020). BCERT - A Decentralized Academic Certificate System Distribution Using Blockchain Technology. 12. 103-118.

[5]. Ayub Khan, Abdullah, Asif Ali Laghari, Aftab Ahmed Shaikh, Sami Bourouis, Amir Madany Mamlouk, and Hammam Alshazly. 2021. "Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission" Applied Sciences 11, no. 22: 10917. https://doi.org/10.3390/app112210917

[6]. Kistaubayev, Yerlan, Galimkair Mutanov, Madina Mansurova, Zhanna Saxenbayeva, and Yassynzhan Shakan. 2023. "Ethereum-Based Information System for Digital Higher Education Registry and Verification of Student Achievement Documents" Future Internet 15, no. 1: 3. https://doi.org/10.3390/fi15010003

[7]. Rahman, Tasfia, Sumaiya Islam Mouno, Arunangshu Mojumder Raatul, Abul Kalam Al Azad, and Nafees Mansoor. "Verifi-chain: A credentials verifier using blockchain and IPFS." In International Conference on Information, Communication and Computing Technology, pp. 361-371. Singapore: Springer Nature Singapore, 2023.

[8]. Saleh, Omar & Ghazali, Osman & Rana, Muhammad Ehsan. (2020). Blockchain Based Framework for Educational Certificates Verification. Journal of Critical Reviews. 7. 79-84. 10.31838/jcr.07.03.13.