IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 2, December 2023

Empowering Certificate Management with Blockchain Technology

Dr. Kapil Vhatkar[1], Yash Ambekar[2], Prathamesh Swami[3], Kartikey Singh[4], Yashovardhan Kaware[5]
Associate Professor, Department of Computer Engineering[1]
Student, Department of Computer Engineering[2,3,4,5]
Dr. D. Y. Patil Institute of Technology, Pune, Maharashtra, India
kapilnv@gmail.com, yashamb444@gmail.com, kartikey2k3@gmail.com
yashovardhankaware2002@gmail.com

Abstract*:* *The rise of online courses and certifications has created new opportunities for individuals to enhance their skills. However, this digital transformation has also given rise to coun- terfeit certificates. To address this multifaceted issue, we present a comprehensive certificate management system founded on blockchain technology and strengthened by smart contracts. Our innovative system comprises three pivotal components: certificate generation, authenticity verification, and a user-centric digital locker for certificate storage. Blockchain technology underpins the entire system, ensuring the immutability and integrity of each certificate. The inclusion of a cryptographic hash for each certificate is a fundamental aspect of our design. Any alteration in the certificate's data will yield a distinct hash, a powerful indicator of potential tampering. Furthermore, our system includes a secure digital locker based on cloud storage that empowers users to efficiently manage and access all their certificates in one place. Moreover, our project is committed to providing features for certificate revocation and updating, thereby enhancing the system's flexibility and security. Hence, the blockchain and smart contract-based certificate management system offers a robust and one-stop solution to the escalating problem of counterfeit certificates in the digital era*

Keywords: Blockchain technology, Smart contracts, Coun- terfeit certificates, Authenticity verification, Cryptographic hash, Digital locker

I. INTRODUCTION

In a bygone era, certificates were tangible, paper-based documents, requiring careful handling and posing challenges when shared with potential employers and recruiters. With the surge of Information Technology, the landscape of certification underwent a transformation. E-certificates became the new norm, offering individuals greater flexibility in sharing their qualifications. However, the authority to generate these e-certificates remained confined to select certification bodies, resulting in centralized data control. This centralization posed security concerns, as traditional storage and sharing methods grappled with a host of challenges.

Moreover, the verification of certificate authenticity could only be carried out through the specific portals designated by each certification authority, leading to fragmentation and inconsistency in the process.

The emergence of blockchain technology, exemplified by the inception of Bitcoin in 2009, introduced the world to a paradigm shift. It brought to the forefront immutable ledgers, consensus mechanisms, and tamper-proof data storage in chained blocks. While Bitcoin primarily revolutionized transactions, Ethereum, as a pioneering blockchain technology, expanded its applications by enabling data storage on blocks and harnessing the power of smart contracts—self-executing code. This monumental development unlocked a wide array of applications and possibilities.

This article embarks on a journey through the body of research on blockchain-based certificate management systems. It seeks to glean meaningful insights and draw significant con- clusions by evaluating the strengths and weaknesses of various systems. Our ultimate aim is to propose a comprehensive, user- friendly solution that simplifies certificate generation, storage, and verification—a one-stop platform for users to securely and conveniently manage their qualifications.

DOI: 10.48175/IJARSCT-14237

II. LITERATURE SURVEY

Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System[1]

This paper presents a system that leverages Ethereum blockchain and smart contracts to manage authorities, issue certificates, verify them, and handle revocation. The pros include a three-tier authority management system, certificate revocation, and the ability to display complete certificate information during verification. However, the system lacks a digital locker for issuers and individual users, as well as any mention of bulk certificate generation. An improvement can be done by storing the hash of the certificate itself for more robust verification, rather than just the certificate information.

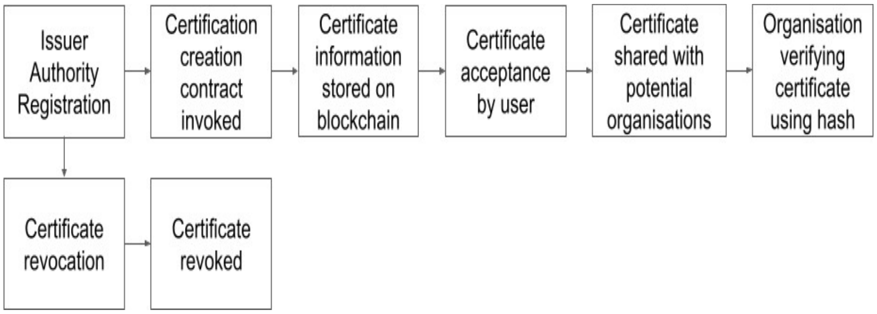
Issuer Authority Registration
Certification creation contract invoked
Certificate information stored on blockchain
Certificate acceptance by user
Certificate shared with potential organisations
Organisation verifying certificate using hash
Certificate revocation
Certificate revoked

Fig. 1. Combined system workflow

Blockchain Based Storage and Verification Scheme of Credible Degree Certificate[2]

This paper introduces a scheme for storing and verifying credible degree certificates using Hyperledger Fabric, with a particular emphasis on transaction speed. The advantages of this system include its use of a permissioned blockchain, maintaining a high system transaction throughput (ranging from 180 to 250 transactions per second), and the utilization of Kafka as a message queue for efficient transaction processing. However, it's worth noting that Hyperledger Fabric has certain inherent limitations that could impact the project's scope, hinting at a potential area for future research. Fig. 2. describes the system hierarchy of the system proposed in the paper.

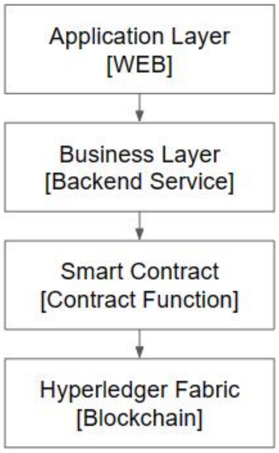
Application Layer [WEB]
Business Layer [Backend Service]
Smart Contract [Contract Function]
Hyperledger Fabric [Blockchain]

Fig. 2. System Hierarchy

DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts [3]

This research paper presents a system designed to streamline the issuance and verification of digital certificates. Its primary objective is to establish a process where issuing authorities share authenticated student lists with a distributed system for verification against student details uploaded via an application interface. The certificates are stored in the blockchain using smart contracts, ensuring their security. Students receive their certificates only after successful storage, which includes em- bedding data for security and QR codes for easy sharing and verification.

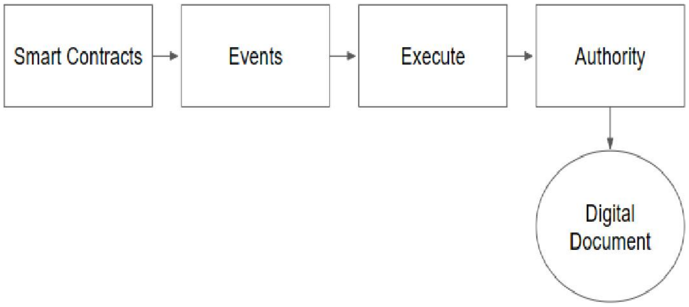

Fig. 3. System Structure

The advantages of this system include embedded watermarks on mark sheets for added security and one- time passwords for controlled certificate sharing with employers. However, the paper highlights two potential challenges: the management of a high volume of certificates, considering the large number of graduating students, and the use of a public Ethereum blockchain, suggesting that a private/permissioned network might offer a more suitable solution.

TrustCA: Achieving Certificate Transparency Through Smart Contract in Blockchain Platforms[4]

This paper presents a fresh way to improve traditional Cer- tificate Authorities (CAs). It leverages blockchain technology and introduces the idea of a ”CA proxy” to enhance security and transparency while reducing fraud risks. The approach involves a decentralized system and collaboration between the CA proxy, existing CAs, and identity verification parties, potentially transforming certificate issuance and management.

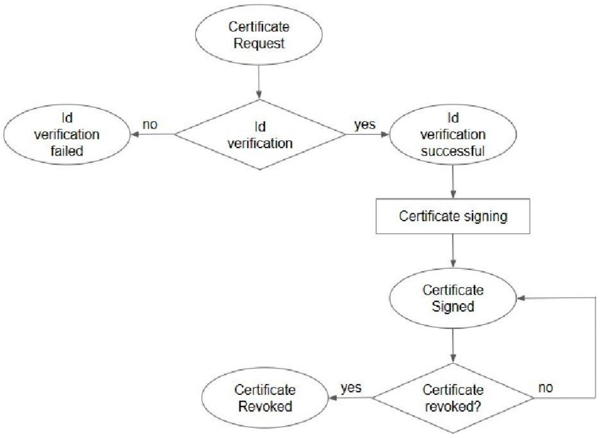

Fig. 4. Life Cycle of a Digital Certificate

By integrating blockchain oracle service-Oraclize, the CA proxy offers seamless collaboration with existing CAs and maintains a public list of root CAs for user reference.

Furthermore, the system leverages professional parties for identity verification, notably enhancing certificate security. However, the paper acknowledges the challenge of balancing decentralization and centralization to optimize information transparency and processing efficiency. This balance is a pivotal aspect that presents a research gap for future exploration.

A Review on Digital Degree Certificate using Blockchain Technology [5]

This research paper introduces a blockchain-based system designed to revolutionize the issuance, assignment, and verification of degree certificates. The system leverages Ethereum blockchain and smart contracts to automate these processes efficiently. Notably, Ethereum’s robust community support is a key advantage, ensuring the system’s stability and reliability. Moreover, the proposed system offers a solution for universities to effortlessly issue e-certificates to a large volume of graduating students, simplifying the sharing of certificates with potential employers. However, the system could have utilizated the use of a private blockchain network to enhance the security of certificate issuance and assignment, potentially restricting access to authorized parties only.

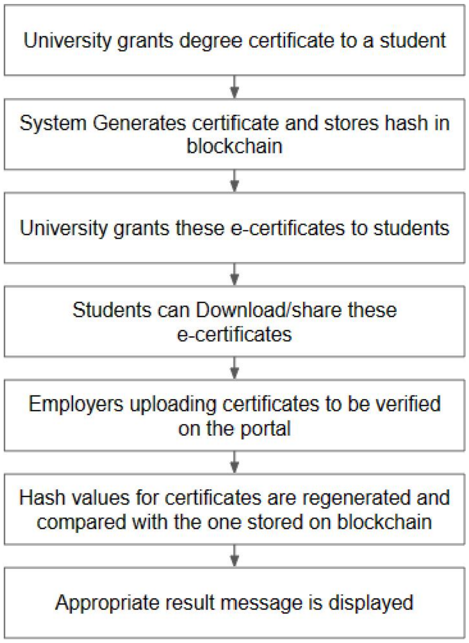
University grants degree certificate to a student
System Generates certificate and stores hash in blockchain
University grants these e-certificates to students
Students can Download/share these e-certificates
Employers uploading certificates to be verified on the portal
Hash values for certificates are regenerated and compared with the one stored on blockchain
Appropriate result message is displayed

Fig. 5. Working process of the system

SmartCert Blockchain Imperative for Educational Certificates[6]

This paper explores the potential benefits of the SmartCert blockchain solution for educational certificates. It emphasizes advantages such as the ability for issuing authorities to create tamper-resistant, cryptographically-sealed records, secure stor- age, streamlined distribution, and the ease of third-party verifi- cation. Moreover, this technology eliminates the risk of record loss and obviates the need for explicitly deleting certificates, even those with errors. However, one notable disadvantage of the system is the absence of a revoke functionality, which means that once a certificate is issued, there is no built-in mechanism to invalidate or revoke it in case of errors or changes in a recipient's status, potentially posing challenges for managing erroneous or outdated certificates.

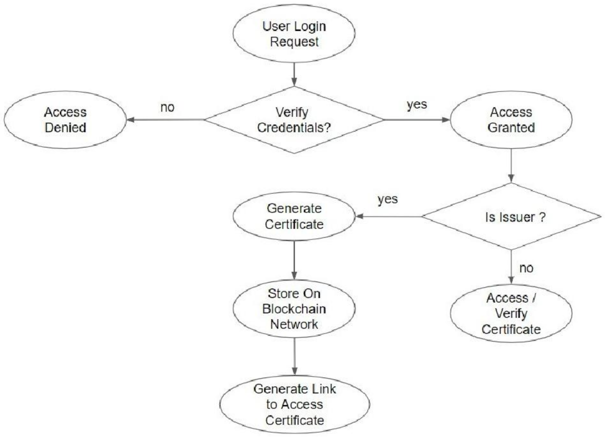

Fig. 6. System workflow of the proposed system

Blockchain and Smart Contract for Digital Certificate[7]

In this paper, the authors tackle the issue of counterfeit certificates by introducing a blockchain-based digital certificate system. Recognizing the significance of academic and professional certificates as reference materials for schools and employers, the paper underscores the need for an effective anti-forgery mechanism. Leveraging blockchain's immutability, the proposed system is designed to provide digital certificates that are both tamper-resistant and verifiable. The process involves generating electronic files for certificates, calculating their hash values, and storing these values in the blockchain. QR-codes and inquiry string codes are affixed to paper certificates, allowing individuals to easily verify their authenticity through mobile scanning or website queries.

DistB-CVS: A Distributed Secure Blockchain based Online Certificate Verification System from Bangladesh Perspective[8]

In this paper, the authors address the issue of academic certificate issuance and verification, particularly in the context of a country where cryptocurrencies are banned. They propose a blockchain-based certificate verification system hosted on the cloud, emphasizing its potential to provide a secure and efficient solution to this problem. The system, referred to as ”DistB-CVS,” leverages blockchain technology to create immutable and publicly verifiable academic credentials. DistB- CVS showcases the adaptability of blockchain in countries with cryptocurrency restrictions, meeting the requirements for a modern academic certificate verification system and address- ing existing challenges in certificate authenticity verification.

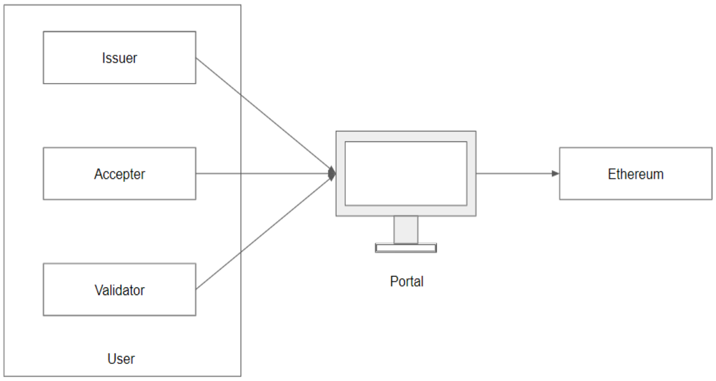

Fig. 7. Configuration of blockchain based system

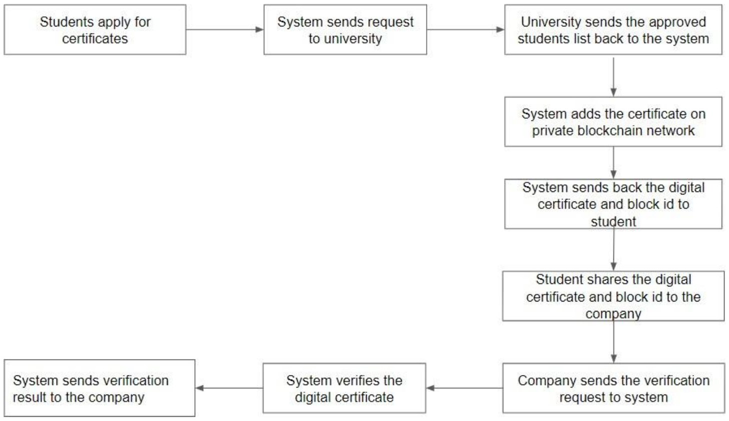
Students apply for certificates
System sends request to university
University sends the approved students list back to the system
System adds the certificate on private blockchain network
System sends back the digital certificate and block id to student
Student shares the digital certificate and block id to the company
Company sends the verification request to system
System verifies the digital certificate
System sends verification result to the company

Fig. 8. Certificate verification process

Proof of Blockchain Work on The Security of Academic Certificates[9]

In this paper, the authors introduce a quantitative framework for assessing the security and performance implications of the Proof of Work (PoW) consensus mechanism in the context of academic certificates. They explore the use of PoW and the SHA-256 cryptographic hash function to create secure and tamper-resistant certificates on a blockchain. The paper also addresses the importance of PoW in preventing cyber-attacks, specifically Distributed Denial of Service (DDoS) attacks.

DOI: 10.48175/IJARSCT-14237

Analysis of Blockchain Technology for Higher Education [10]

The proposed system offers a blockchain-based solution for issuing and verifying digital diplomas in higher education (focusing on University Fernando Pessoa (UFP) in Portugal). It adheres to Blockcerts standards, ensuring compatibility with any blockchain, and provides open-source software for academic record management. This system consists of four key components: cert-tools, cert-issuer, cert-viewer, and the Blockcerts wallet, each serving specific functions related to configuration, publication, visualization, and verification of diplomas.

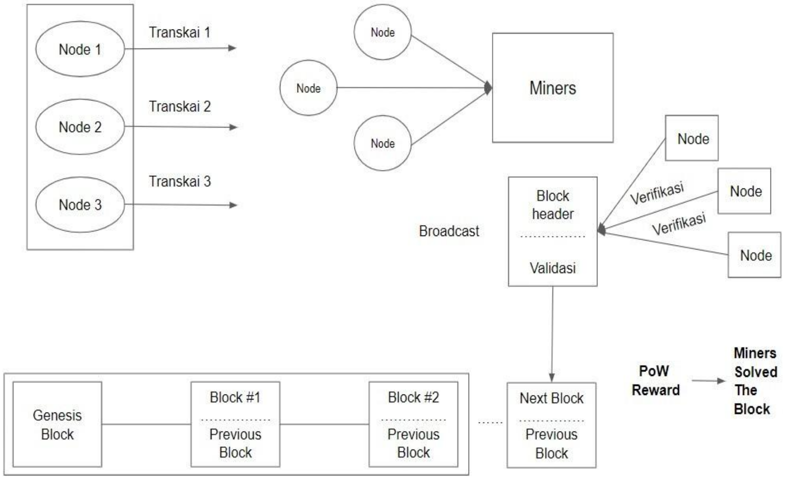

Fig. 9. Proof of work consensus mechanism

Furthermore, it has been successfully tested on Bitcoin and Ethereum networks and offers the advantage of bulk diploma issuance, which can significantly reduce operational costs. However, the proposed blockchain solution for higher education faces several challenges. Diploma revocation is complex due to the immutable nature of blockchain, and solutions like smart contracts or revocation lists have their own limitations. Fig. 10. describes how different stalkeholders interact with each other using the proposed system.

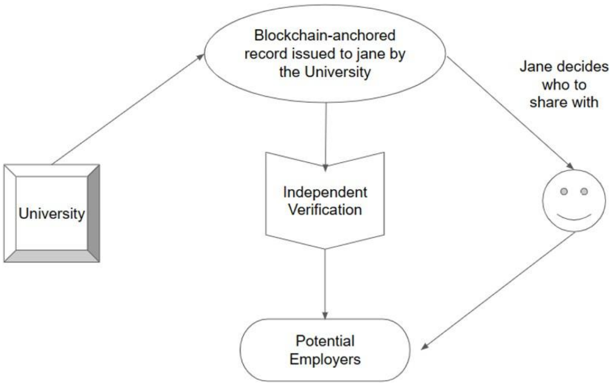
Blockchain-anchored record issued to jane by the University
Jane decides who to share with
University
Independent Verification
Potential Employers

Fig. 10. Interaction between potential stalkeholders

Issuing And Verifying Digital Certificates With Blockchain[11]

The system utilizes Blockcert, which uses the Bitcoin network for certificate data storage, providing transparency and availability. However, Blockcert has drawbacks, such as dependence on Bitcoin's fluctuating rates and rising network costs. In response to these challenges, the authors propose UniCert, a model based on UniCoin, a blockchain-based digital currency, which could address various issues, including anti-counterfeiting and copyright protection. Blockchain technology is seen as a promising solution to counterfeit certification problems, offering transparency, security, and privacy. Other blockchain-based applications like 0xcert, Open Certificates, and CertChain, which aim to solve similar issues in the education and certification domain. The UniCert system utilizes metadata in transaction structures to store hashed certificates using the Merkle tree hash algorithm. UniCert validation process involves comparing various components of certificates to ensure their authenticity, address generation, block querying, and transaction details.

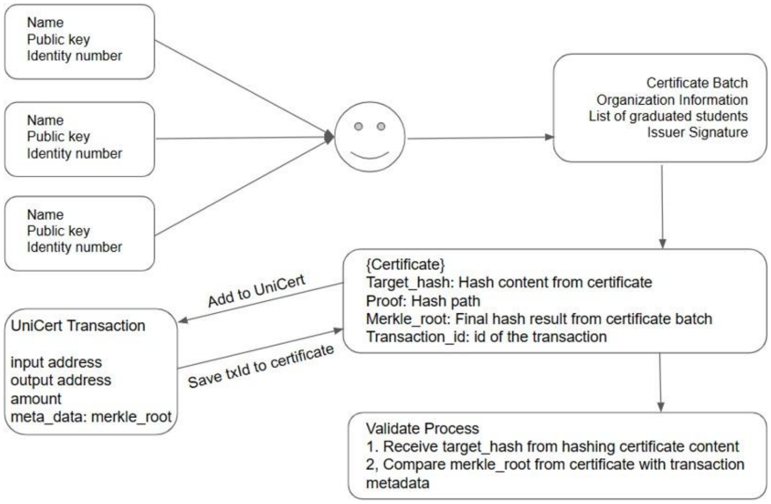

Fig. 11. UniCert Blockchain Mechanism

Issuing And Verifying Digital Certificate Using Blockchain[12]

The system utilizes the InterPlanetary File System (IPFS) for secure certificate storage. Each certificate is assigned a unique hash, acting as a digital fingerprint. Students receive this hash via email for easy download and verification. Verifiers can search for certificates using the hash, streamlining the verification process, however we cannot simply upload a certificate file to check it's authenticity, we need to use the hash for verification and download, which adds an extra step to the process. While IPFS and certificate hashes enhance security and accessibility, the system lacks a built-in revocation mechanism for certificates, potentially posing challenges with errors or updates in a recipient's status.

Towards A Framework Of A Secure E-Qualification Certificate System[13]

The proposed secure e-qualification certificate system rep- resents a significant advancement in certificate management, aiming to replace traditional paper-based certificates with easily managed, verified, and distributed electronic versions. It offers several advantages, such as utilizing digital signatures, timestamps, access tokens, and content extraction signatures to ensure the authenticity, integrity, and privacy of e-certificates.

Notably, it minimizes the need for storing sensitive data within the system, enhancing security and saving storage space. Additionally, the system adopts a service-oriented architecture and interoperable XML schemas, facilitating seamless integration with various applications, including e-portfolios, and offers a centralized platform for issuing, managing, and verifying e-certificates nationwide. However, there are certain challenges to overcome. These include addressing the legal aspects of recognizing digitally signed documents as valid replacements for paper certificates, establishing trust among stakeholders and ensuring broad acceptance of e-certificates by universities and employers, and managing compatibility issues that may affect the accessibility and validity of e-certificates.

Cloud Based Graduation Certificate Verification Model[14]

The research paper proposes a cloud-based model for certificate verification. The system uses a secret key and a serial number for each certificate, which are generated by the university and given to the graduate. Verifiers can access the online system on the university's website and enter the secret key and the serial number to validate the certificate. This reduces the time and cost of manual verification and ensures the security, validity, and confidentiality of the certificate. However, the system requires the graduate to share the secret key with the verifier, which may compromise its secrecy. The system also does not provide a way to revoke or update certificates in case of errors or changes in the graduate's status. This paper has clarified our ideas regarding implementing our product as a cloud-based or blockchain-based application. The various challenges and privacy factors that can be affected while using the cloud as a base can be easily addressed when implementing the application using blockchain.

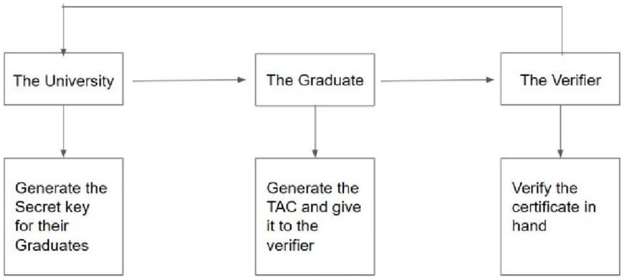
The University
The Graduate
The Verifier
Generate the Secret key for their Graduates
Generate the TAC and give it to the verifier
Verify the certificate in hand

Fig. 12. Cloud based System Workflow

Analysis Of Revocation Mechanisms For Blockchain Applications And A Proposed Model Based In Self-Sovereign Identity[15]

The paper outlines a novel model for revoking blockchain transactions, and it stands out for several key features. The proposed model leverages self-sovereign identity standards, such as Verifiable Credentials (VC) and Decentralized Identifiers (DID), to enable the revocation of both old and new records while maintaining the integrity of the original blockchain structure and data. This revocation model is achieved through the use of a reverse link and a data revocation scheme, which references the revoked transactions and provides additional complementary information. Importantly, the model is characterized by its flexibility, decentralization, and compatibility with a variety of blockchain applications, with a particular emphasis on its suitability for academic settings.

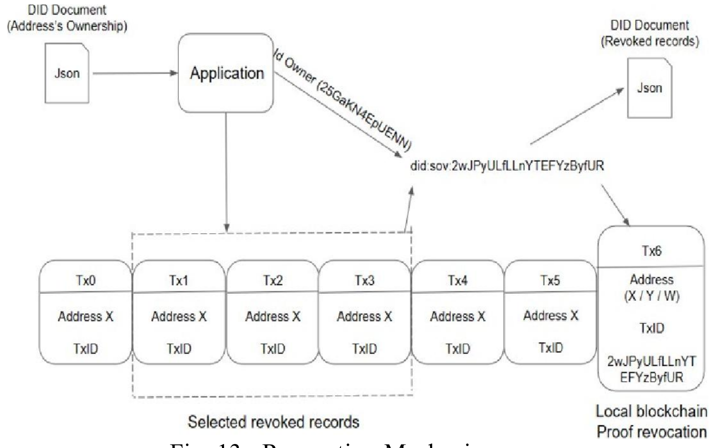

Fig. 13. Revocation Mechanism

III. FINDINGS AND DISCUSSION

Based on our extensive literature review, we have identified several critical findings that shape the landscape of blockchain-based certificate generation, storage, and validation systems:

- The choice of blockchain technology is pivotal and de- pends on the specific applications and use cases of the proposed system.
- The nature of the certificates to be generated dictates the choice between public and private blockchains, with implications for privacy and control.
- Systems designed for mass-scale deployment must offer the capability to generate certificates in bulk efficiently.

DOI: 10.48175/IJARSCT-14237

- Certificate validation remains a central application of blockchain technology and demands careful implementation. The method of verifying certificate authenticity can involve generating the hash of certificate information or the hash of the entire certificate, offering different levels of security.
- Revoking and updating records or certificates on the blockchain network pose ongoing challenges and remain areas of active research.
- The core aim of these systems is to decrease dependency on certification authorities and third-party verification services, concurrently leading to a reduction in the over-all cost associated with both certificate generation and validation processes.
- Striking a balance between system centralization and decentralization is essential to optimize transaction processing efficiency.
- Ethereum is versatile and suitable for public or open- access certificate systems, thanks to its wide developer community and smart contract capabilities. In contrast, Hyperledger Fabric is ideal for scenarios requiring a permissioned blockchain, offering fine-grained access control and privacy features, making it a practical choice for more controlled and centralized environments.

IV. CONCLUSION

The possibilities within blockchain technology offer a promising avenue to enhance the efficiency, security, and accessibility of certificate management. In addition to the key findings derived from the reviewed papers, several important conclusions have been drawn:

- Private blockchains, particularly Hyperledger, exhibit sig- nificantly higher transaction throughput compared to pub- lic blockchains, making them ideal for systems prioritiz- ing transaction speed.
- If the objective is to restrict certificate issuance and revocation to authorized entities, private blockchains, such as Hyperledger, offer an excellent choice.
- Ethereum, with its extensive community and rich feature set, is a suitable option when certificates are intended to be made public.
- Blockchain technology inherently provides integrity, transparency, security, and privacy for the certificate hashes stored on the blockchain.
- Cloud storage can serve as a digital locker, providing a centralized repository for individual certificates or those issued by organizations, aligning with our vision of a unified platform for all certificate-related operations

REFERENCES

[1]. Rui Xie, Yuhui Wang, Mingzhou Tan, Wei Zhu, Zhongjie Yang, Jiaji Wu, and Gwanggil Jeon, “Ethereum-blockchain-based technology of decentralized smart contract certificate system,” IEEE Internet of Things Magazine, June 2020.

[2]. Dongwei Liu, Xiaojin Guo, “Blockchain based storage and verification scheme of credible degree certificate,” 2019 2nd International Confer- ence on Safety Produce Informatization (IICSPI).

[3]. Ms. R.Poorni, Mr. M.Lakshmanan, Ms. S. Bhuvaneswari, “DIGICERT: A secured digital certificate application using blockchain through smart contracts,” Proceedings of the Fourth International Conference on Com- munication and Electronics Systems (ICCES 2019).

[4]. Jian Zhao, Zexuan Lin, Xiaoxiao Huang, Yiwei Zhang, Shaohua Xiang, “TrustCA: Achieving certificate transparency through smart contract in blockchain platforms,” 2020 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS).

[5]. Roshani S. Bele, Jayant P. Mehare, “A review on digital degree certificate using blockchain technology,” Volume 9, Issue 2 February 2021.

[6]. Tarek Kanan, Ahamd Turki Obaidat, Majduleen Al-Lahham, “SmartCert blockChain imperative for educational certificates,” 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Informa- tion Technology (JEEIT).

DOI: 10.48175/IJARSCT-14237

[7]. Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen, "Blockchain and smart contract for digital certificate ," Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE ICASI 2018- Meen, Prior & Lam (Eds).

[8]. Mahmudul Hasan, Anichur Rahman, Md. Jahidul Islam, "DistB-CVS: A distributed secure blockchain based online certificate verification system from bangladesh perspective," 2nd Int'l Conference on Advanced Information & Communication Technology (ICAICT 2020), 28-29 November 2020, Dhaka, Bangladesh..

[9]. Indri Handayani, Ruli Supriati, Euis Siti Nur Aisyah, Sulistiawati, "Proof of blockchain work on the security of academic certificates," The 8th International Conference on Cyber and IT Service Management (CITSM 2020).

[10]. Fernando Richter Vidal, Feliz Gouveia, Christophe Soares, "Analysis of blockchain technology for higher education," 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC).

[11]. Trong Thua Huynh, Trung, Tru Huynh, Dang Khoa Pham, Anh Khoa Ngo, "Issuing and verifying digital certificates with blockchain," 2018 International Conference on advanced technologies for communications.

[12]. Ms Sneha A. Khaire, Divesh Jadhav, Navnath Ugale, Vaishnavi De- ore, Ankita Pawar, "Issuing and verifying digital certificate using blockchain," Volume 05, Issue 05, May 2023, International Research Journal of Modernization in Engineering Technology and Science.

[13]. Lisha Chen-Wilson, Dr David Argles, "Towards a framework of A Secure E-Qualification Certificate System," 2010, Second International Conference on Computer Modeling and Simulation.

[14]. Osman Ghazali, Omar S. Saleh, "Cloud based graduation certificate verification model," International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-5, Issue-2, Feb.-2017.

[15]. Fernando Richter Vidal, Feliz Gouveia, Christophe Soares, "Analysis of revocation mechanisms for blockchain applications and a proposed model based in self-sovereign identity," Journal of information Technology Management, 2022, Special Issue, pp. 192-210. Published by University of Tehran, Faculty of Management.