Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024: Vol 13: Issue 3
Open Access

Implementing Blockchain Based Credentials In Education Sector In India

Rima Shelat[1], Dr. Sanjay M Shah[2]
[1]Research Scholar,KSV University, Gandhinagar
rimashelatphd@gmail.com// https://orcid.org/0000-0003-4801-5001
[2]Director ,S.V. Institute of Computer Studies, KSV University, Kadi
prrof_smshah@yahoo.com

Cite this paper as: Rima Shelat, Sanjay M Shah (2024) Implementing Blockchain Based Credentials In Education Sector In India. *Frontiers in Health Informatics, 13* (3), 1338-1348.

Abstract

In today's digital era securing and managing and issuing digital credentials plays a crucial role in the education sector, but the old solutions are prone to data breaches, forgery, data alteration, manipulation and other centralized database weaknesses. In such scenarios Blockchain technology proved to be a life saver, Originally it was developed for Bitcoin but now it provides a various alternative including storing, issuing and managing Immutable credentials. Its decentralization mitigates the risk of attacks, threats while its immutability assures unaltered or unchanged credentials boosts the trust and integrity of them. This Research investigates the paradigm of immutable credentials on the blockchain,using cryptographic functions to securely link academic degrees , professional certificates to individual identities . Benefiting by providing improved security standards, eliminating single point failures, better accountability and transactions through verifiable and simplified validation procedures. This technique aligns with the self-sovereign identity movement, providing people not only to control over their credentials but also to provide selective access to their digital identities. By looking at the technological basis and real-world implementation , this study highlights the transformation of centralized databases to blockchain in Indian scenarios in the Indian Education sector.

Keywords:*Blockchain Technology, Immutability, Secure Transaction, Credentials, Decentralization, Cryptographic Credentials.*

INTRODUCTION

In today's digital era, it is very much important that our credentials remain safe, secure & intact. Old systems which were centralized for storing and managing the certificates and credentials faced many difficulties for managing and issuing them. They also faced data breaches, forgery of the certificates and credentials and the failure of a single point centralized system. They also face the shortage of the necessity of serving digital access and identity needs as well. For providing a tabula rasa that provides the necessary security and usability in the types of and volumes of digital communication that defined us today, Blockchain technology revolutionized as a prime candidate to deliver it.

Blockchain Technology which was originally planned for Bitcoin transactions, has grown tremendously for the variety of operations, including secure credential management as well. Blockchains' main feature of decentralization grants that no single party manages the entire system, mitigating the risk of hostile attacks and data manipulation or forgery. Furthermore, the immutability of Blockchain records ensures that once they are generated an credential can not be altered, deleted or manipulated which ensures a very high level of security and trust.

Immutable Credentials on the blockchain refers to the creation and management of digital credentials that are securely stored on the blockchain ledger. Degrees and professional certificates, as well as personal identification documents are the examples of such credentials. Using cryptographic means, each credential is safely and securely encoded and attached to an individual's identity ensuring privacy, security and validity.

This technology provides a number of benefits. First it will improvise security through mitigation of the risk of a single point failure, which makes it very much extraneous for the attackers to break into the system. Secondly, it induces accountability and transparency by sorting all the transactions and modifications on the blockchain, which can be sustained individually . Thirdly, it will ease the credentials' validation process by allowing stakeholders to willingly confirm legitimacy of a credential using Blockchain without any third party interference.

The Need of immutable Credentials on blockchain is also in accord with the larger drive towards self-dominant identification, in which individuals have complete authority over their digital identities.

This drastic change will enable individuals to maintain their credentials securely and share with selectively trustworthy partners, abolishing the need of centralized authority.

In this research article, we look at the technical implementation of storing immutable credentials on blockchain. We look at the concept of blockchain Technology, cryptographic algorithms and consensus processes that will qualify secure credential issuance and verification in the education sector. Furthermore we have deliberate pilot projects and case studies that promote the efficiency of the techniques. This study plans to provide a full knowledge of how blockchain based credential management can change the way we maintain digital credentials in the modern era.

2. EXISTING CASE STUDIES

There are many pilot projects and case studies current available that prominently shows the usage of blockchain technology in securing the immutable credentials, such as

- **Blockcert:** Blockcerts is an open standard for creating, issuing, viewing, and verifying blockchain-based certificates. Developed by MIT Media Lab, it enables academic institutions, professional organizations, and other entities to issue tamper-proof credentials.[1]
- **Learning Machine :** Learning Machine partners with institutions to issue official records that are instantly verifiable anywhere in the world. It leverages Blockcerts for blockchain-based credentialing.[2]
- **Sony Global Education :** Sony Global Education has developed a blockchain-based platform for securely sharing and verifying academic achievements. This system allows for the tamper-proof sharing of learning achievements and career histories.[3]
- **Credly :** Credly offers digital credentialing solutions that leverage blockchain technology for secure and verifiable digital badges. These badges represent skills and achievements, providing a trusted way for individuals to present their qualifications.[4]
- **DiplomaSafe :** DiplomaSafe provides blockchain-based verification for educational certificates and diplomas. It ensures the authenticity of issued credentials and simplifies the verification process for employers and institutions.[5]
- **ODEM (On Demand Education Marketplace) :** ODEM uses blockchain to verify and share educational records and achievements. The platform allows students to manage and control their educational credentials in a secure, decentralized manner.[6]

3. RESEARCH DEFINITION

This study recommends implementing an Ethereum-based prototyping system for decentralized data management in India's education sector. The suggested system intends to improve the security and integrity of academic credentials by adding strong access controls and encryption methods such as keccak-256 and ECDSA, as well as decentralizing storage using the **InterPlanetary** File System (IPFS). Specific goals are to:

- Use decentralized data storage and modern encryption techniques to reduce the risk of data breaches and unauthorized access.
- Use blockchain technology to ensure that academic credentials are immutable and tamper-proof.
- Make verification processes more safe and transparent, enhancing stakeholder trust.

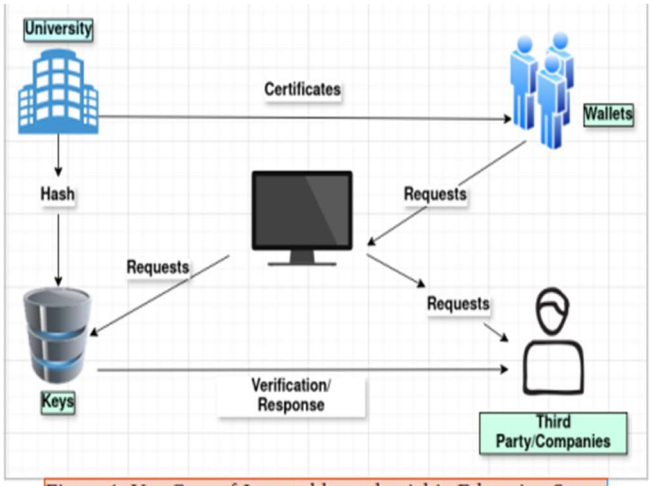

Figure 1: Use Case of Immutable credential in Education Sector

4. LITERATURE REVIEW

The traditional method of managing student certificates and academic records in universities is fraught with challenges, including the risk of data breaches, unauthorized access, and the time-consuming process of manual verification. These issues compromise the security and integrity of academic credentials while creating inefficiencies and increasing operational costs for educational institutions (Zheng et al., 2017).

This research aims to develop a private, permissioned blockchain repository for student certificates using Ethereum technology. The proposed system will verify the issuance of certificates manually only once, after which the process of re-issuing and verifying certificates will be automated. Additionally, third-party verification will be streamlined, allowing universities to generate revenue by offering certificate verification services (Sharples & Domingue, 2016). Based on our scope of literature review and functional requirements, we have determined that the Ethereum blockchain, implemented as a private permissioned blockchain, is an optimal solution for our use case. This approach involves a fixed or limited number of nodes and validators (miners) to create records on the ledger, ensuring security, control, and efficiency (Buterin, 2014).

The specific goals of this research are to enhance security and integrity by using blockchain technology to create an immutable and tamper-proof repository for student certificates, reducing the risk of data breaches and unauthorized access (Swan, 2015). Additionally, the system aims to automate the re-issuance of certificates, saving time and resources, and streamline the process of third-party verification by providing easy access to a secure, blockchain-based repository (Tapscott & Tapscott, 2016). Furthermore, the research explores the potential for universities to generate additional revenue by offering certificate verification services to third parties (Underwood, 2016).

This study will address the technical and practical challenges of implementing such a system, including the setup of a private permissioned blockchain, integration with existing university systems, and ensuring scalability and compliance with regulatory standards (Yli-Huumo et al., 2016). By focusing on the unique

requirements of academic record keeping, this research aims to demonstrate how blockchain technology can revolutionize the management of student certificates, providing a secure, efficient, and revenue-generating solution for universities (Puthal et al., 2018).

5.IMPLEMENTATION METHODOLOGY

This research paper investigates the development of a blockchain-based system for the management and verification of university degree certificates. In this system, each department within the university functions as a node, while the University and the Administrator serve as validators. These validators are responsible for mining data over the ledgers and validating it using Proof of Work (PoW). By restricting the number of validators to two, the system aims to enhance chain latency, reduce mining time, and improve chain finality.

The system ensures that each ledger entry has valid ownership, which can be transferred to rightful owners. Certificates are treated as assets embedded with tokens, allowing for their validation and verification when challenged by third parties. Degree certificate images are stored in the InterPlanetary File System (IPFS), which generates a unique hash for each certificate. These IPFS hashes are referenced in an Ethereum smart contract, which also generates a key held by two stakeholders in wallets, such as MetaMask. The smart contracts, written in Solidity, manage verification requests for the degree certificates.

The implementation of this system involves several key steps. Initially, departments are configured as nodes, and the University and Administrator are established as validators. Degree certificate images are stored in IPFS, and the generated hashes are retrieved. A Solidity smart contract is developed to manage certificate data, referencing IPFS hashes and managing keys. Wallet integration ensures that stakeholders can securely store and control keys. The verification mechanism within the smart contract allows third parties to challenge and verify the authenticity of certificates.

This system offers several advantages, including enhanced security through decentralized storage and verification, increased transparency in certificate authenticity, and improved efficiency with faster consensus and reduced latency. However, challenges remain, such as the resource-intensive nature of PoW, secure key management, and the need to handle large amounts of data efficiently. Overall, this blockchain-based system presents a promising approach to modernizing and securing the management and verification of university degree certificates.

6.TOOL & TECHNOLOGY

Ethereum Server	Go(Language Binding)
Smart Contract	Solidity(language)
API JS	Web3JS (Library Tool)
Wallet Creation	Metamask (OS Wallet)
Decentralized Database	IPFS Protocol(File System)
UI Components(DApps)	React(UI Library)
File System	IPFS
Local Storage	Fly.io

Technology	Ethereum
Language	Solidity(Version 0.8.17)
Smart Contract	Ethereum
Tool	Hardhat
IDE	VS Code
Runtime	Node.js

Table 1: Tools & Technology for Implementation

7.SYSTEM COMPONENTS & HARDWARE

API Server • Developed using Node.js, capable of handling RESTful requests. • Connects to Redis, IPFS, and Ethereum nodes to process and retrieve data.
IPFS Nodes • Set up on multiple instances (using Fly.io) to ensure redundancy and high data availability. • Each record is stored as a file on IPFS, with a maximum size limit of 2MB per record
Redis Cache • Configured for high availability and partitioned to handle 10 million records (10% of 100M). • Uses eviction policies like LRU to manage memory efficiently.
Ethereum Nodes • Deployed within the private network to facilitate fast transaction processing. • Smart contracts deployed to manage the authentication and verification of records.
Load Balancer • Configured to handle up to 16,000 concurrent connections, ensuring efficient distribution of network and application load across server

Table 2 : System Components and Hardware

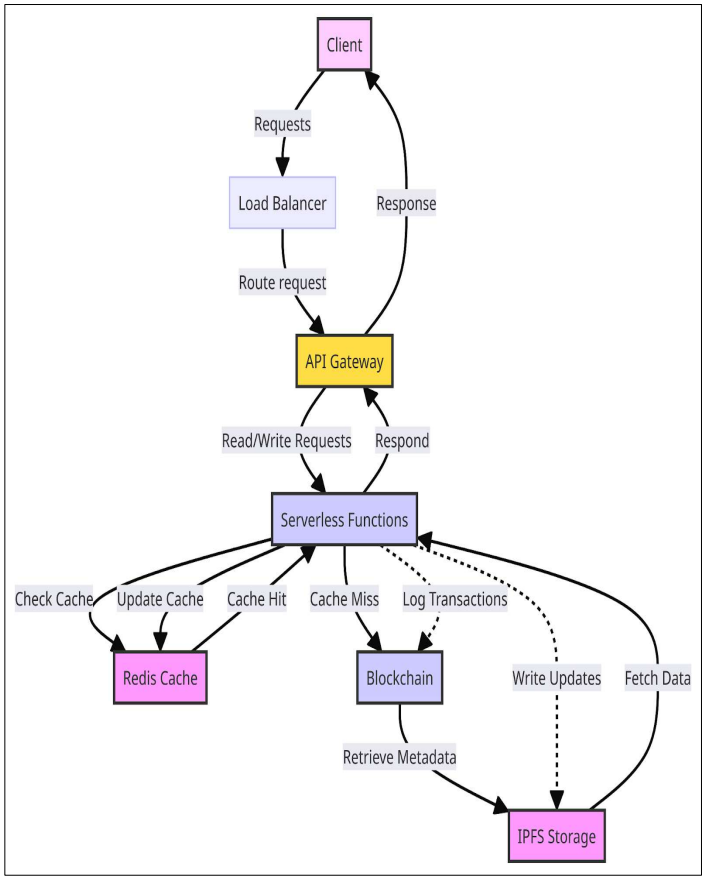

Figure 2: System Components and Hardware

8. TECHNOLOGY FOR TEMPER PROOFING AND SECURITY

Login	SSO(Single Sign On)
JWT (Jason Web Token)	Header, Payload, Signature
2FA	Two Factor Authentication using OTP.
Refresh Token	Expiration
RBAC	Role Based Access Control
Ethereum Address	ECDSA Algorithm
Private Key Generation Formula	**y2 = x3+ax+b**
Asset Sorting	IPFS Protocol (Decentralised Storage)
Content Hashing: Keccak-256 hashes the block content using IPFS Hash	

Table 3: Tamper Proofing

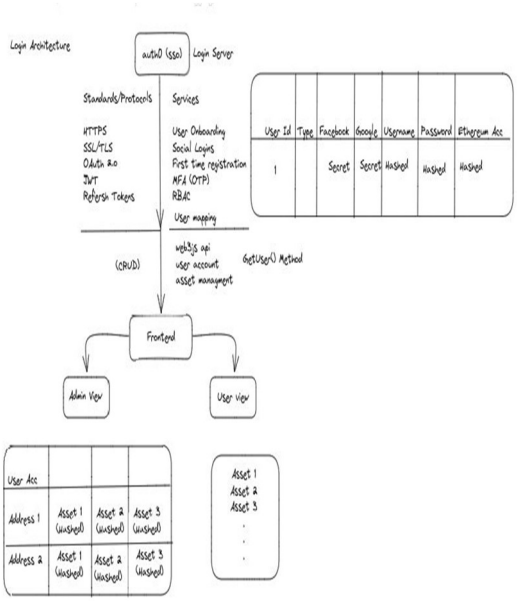

Figure 3: Tamper Proofing Methodology

9.METHODOLOGY & ALGORITHM

Methodology – ECDSA

Elliptic curve Digital Signature Algorithm

Certificate Issue: Generates a digital signature for the certificate issued by the Certificate Authority. The private key of the certificate is issued by the Issuer, this key is unique to each certificate generated using ECDSA.

ECDSA Key Generation

1: Randomly compute an integer d in the interval [1,n - 1]

2: Calculate Q = dG

***3:** The public key computed is Q and the private key is d*

Verification of Signature:

ECDSA is employed to verify digital signatures associated with the certificates. The Public key corresponding to the CA's Private key is used to validate the signature. By comparing the generated signature with the verified signature, The receipt or verifier can ensure that the certificate is genuine and altered.

Signature Verification – ECDSA

1. *Verify that r and s are integers in the interval [1, n - 1]*
2. *Compute H(m) and convert this bit string to an integer e*
3. Compute w = s −1 mod n

4. *Compute u1 = ew mod n and u2 = rw mod n*
5. *Compute X = u1G + u2Q*
6. *If X = O(the point at infinity), reject the signature. Otherwise, convert x1 of X to an integer x¯1 and compute v = x¯1 mod n*
7. *Accept the signature if and only if v = r*

10. HASH FUNCTION

Keccak-256 (Hash Function)

- Certificate Content Hashing :Keccak-256 is applied to create a unique hash value for each Digital Certificate: The certificate's content is secured through the Keccak-256 algorithm, resulting in the condescending representation of the certificate known as hash.
- IPFS Storage & Retrieval: The Digital Certificates with its respective hash are stored in IPFS, which is distributed and decentralized file systems. The IPFS uses the Hash value to address the corresponding certificate.
- Verification of Certificate Integrity: When the certificate is verified, The recipient or the verifier retrieves the certificate from the IPFS using its hash value,The verifier then recalculates the hash value of the certificate using Keccak 256 , By comparing the recalculated hash with the stored hash value, the verifier can ensure the integrity of the Certificate.

11. RECORDS & RESULTS

- Record Size: 2MB
- Internet Speed: 100 Mbps (12.5 MBps)
- Number of IPFS Nodes: 4
- Number of Ethereum Nodes: 4
- Verification: Instantaneous
- Hardware: S3 bucket and EC2 instances

Results - Efficiency (Uploading Data)

- Record Size: 2MB
- Internet Speed: 100 Mbps (12.5 MBps)
- Number of IPFS Nodes: 4
- Number of Ethereum Nodes: 4
- Approver: 1
- Hardware: S3 bucket and EC2 instances

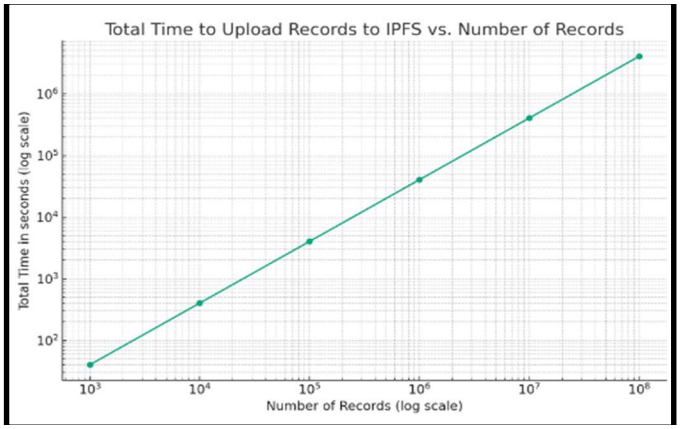

Figure 4:Uploading Record Efficiency

12. CONCLUSION

The implementation of blockchain-based systems for managing academic credentials marks a significant advancement in addressing the longstanding challenges faced by traditional, centralized systems. By leveraging blockchain's decentralized nature, cryptographic security, and immutable record-keeping, educational institutions can ensure the authenticity, integrity, and security of academic records. This not only mitigates the risks of data breaches and unauthorized access but also streamlines the verification process, empowering both students and institutions with greater control over their digital identities. As demonstrated by various pilot projects and case studies, the adoption of such technology is not just feasible but also essential in modernizing and securing the management of academic credentials. The proposed Ethereum-based prototype, with its integration of IPFS and robust encryption methods, represents a forward-looking solution that aligns with the broader global trend towards decentralized digital identity management. Ultimately, this research underscores the transformative potential of blockchain technology in the education sector, paving the way for a more secure, transparent, and efficient future in academic credential management

REFRENCES

[1] "Blockcerts: Open Standard for Blockchain Certificates." MIT Media Lab, 2016, www.blockcerts.org/.

[2] "Learning Machine Issuing Digital Credentials on Blockchain." Learning Machine, 2018, www.learningmachine.com/.

[3] "Sony Develops Technology Using Blockchain for Open Sharing of Academic Proficiency and Progress Records." Sony, 2017, www.sony.net/SonyInfo/News/Press/201708/17-072E/.

[4] "Credly: Digital Credentials and Open Badges." Credly, 2021, info.credly.com/.

[5] "DiplomaSafe:Secure and Verifiable Diplomas." DiplomaSafe, 2019, diplomasafe.com/.

[6] "ODEM:Blockchain Education Marketplace." ODEM, 2020, odem.io/.

[7] Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved from https://ethereum.org/en/whitepaper/

[8] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The Blockchain as a Decentralized Security Framework [Future Directions]. IEEE Consumer Electronics Magazine, 7(2), 18-21.

[9] Sharples, M., & Domingue, J. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In the European Conference on Technology Enhanced Learning (pp. 490-496). Springer, Cham.

[10] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

[11] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

[12] Underwood, S. (2016). Blockchain Beyond Bitcoin. Communications of the ACM, 59(11), 15-17.

[13] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PloS One, 11(10), e0163477.

[14] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.

[15] Osterwalder, A., & Pigneur, Y. (2010). Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers. John Wiley & Sons.

[16] Swanson, T. (2015). Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management. Self-published.

[17] Elmasri, R., Navathe, S. B., & Navathe, S. B. (2020). Fundamentals of Database Systems (8th Edition). Pearson.

[18] Gollmann, D. (2011). Computer Security (3rd Edition). Wiley.

[19] Reinsel, D., Gantz, J., & Rydning, J. (2018). Data Age 2025: The Evolution of Data to Life-Critical Don't Trust, Verify: A Guide to Blockchain and Smart Contracts. Wiley.

[20] Computing: A Survey". International Journal of Advanced Research in Computer Science, 8(6), 269-272.

[21] Gupta, A., & Garg, A. (2019). "Blockchain Technology: A Review Hellerstein, J. M., & Stonebraker, M. (Eds.). (2008). Readings in Database Systems (3rd Edition). MIT Press.

[22] Nakamoto,S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[23] Singh, R., & Sharma, S. (2019). "Data Security and Privacy Issues in Cloud Computing: A Review". International Journal of Computer Applications, 182(40), 16-22.

[24] Gupta, R., & Chaudhary, P. (2018). "A Review on Data Security Issues in Cloud Computing". International Journal of Computer Applications, 180(26), 20-24.

[25] Patel, H., & Patel, D. (2020). "A Review on Data Security and Privacy Issues in Cloud Computing". International Journal of Computer Applications, 167(6), 17-20.

[26] Sharma, N., & Mittal, N. (2017). "Data Security Issues and Solutions in Cloud n Its Challenges and Opportunities". International Journal of Computer Applications, 181(37), 30-34.

[27] Khan, S. A., & Khan, S. A. (2018). "Blockchain Technology: A Literature Review". International Journal of Advanced Engineering, Management and Science, 4(6), 493-498.

[28] Singh, A., & Sharma, S. (2019). "Blockchain Technology: A Comprehensive Survey". International Journal of Advanced Research in Computer Science, 10(2), 123-128.

[29] Sharma, A., & Yadav, P. (2018). "A Survey of Blockchain Technology and Its Applications". International Journal of Computer Applications, 181(8), 42-47.