JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain Based Credential Verification System

[1] Manish R. Umale, [2] Pratishtha Tiwari, [3] Mayank Singh, [4] Youbraj Singh, [5] Sahil Sunil

[1] Asst. Professor , [2] Student, [3] Student, [4] Student, [5] Student
[1]Department of Computer
Engineering,
[1]Lokmanya Tilak College of
Engineering, Navi Mumbai

Abstract : The Blockchain Based Credential Verification System uses the concept of blockchain technology to transform the process of credential checks through a reliable and tamper-evident method of digital certificate issuing and storing. Techniques of certification under the traditional process are often faced with forgery, unauthorized manipulation, and wastefulness during verification. This benefits from the irreversible nature of blockchain technology to ensure that every issued certificate is archived indefinitely and will not be tampered with, effectively reducing the probability of fraud substantially.

The system is designed to provide real-time validation, enabling institutions, employers, and individuals to validate credentials in real time without the need for manual procedures. Smart contracts provide assurance that the validation process is automated, whereby certificates can be accessed and validated securely via a decentralized system. The system's interface enables users with varying technical skills to manage credentials. Its decentralized system enhances transparency to the extent that all the records are verifiable by the stakeholders involved. As an innovative and efficient substitute for traditional certification systems, the Blockchain Based Credential Verification System is responding to the growing demand for a secure, fraud-free, and globally accessible credential validation system.

***IndexTerms* - Blockchain, Credential Verification, Digital Certificates, Smart Contracts, Ethereum, Web3.js**

I.INTRODUCTION

Credential validation is a necessary part of education, work, and professional licensure but is still beset with inefficiency, counterfeiting, and prohibitively expensive administrative burdens through traditional channels. Paper records are easily lost or modified, and centrally stored electronic systems can be subject to cyberattacks and unauthorized modification. These factors suggest the necessity of a more secure, transparent, and cost-effective credential management system.

Blockchain Based Credential Verification System solves these challenges by utilizing the blockchain technology in providing an immutable, tamper-evident, and decentralized platform for verifying and issuing digital certificates. Automatic verification is secured through smart contracts, eliminating third parties and processing time on checking credentials. Live verification is safer while making the credentials accessible and verifiable instantaneously.

With a user-friendly interface and QR code verification, Blockchain Based Credential Verification System streamlines the process of credential management for individuals, institutions, and employers. Its scalability and affordability make it an ideal candidate for mass market penetration in sectors such as education, healthcare, and corporate training. With a fraud-proof, globally accessible certification system.

1.1 Motivation

The growing need for a reliable, effective, and secure process of credential validation has acknowledged the shortcomings of current systems. Paper certificates may be lost, stolen, and destroyed and thus not useful for the long term. Even electronic records held in centralized databases are not secure since they can be hacked and altered. In the majority of situations, qualification validation through the employment of human intervention is done within weeks or days, leading to enormous delays in career development, university enrollment, and hiring into jobs. Such inefficiencies become a bottleneck for individuals and companies, slowing processes that involve real-time verification of qualifications.

Part of the problem lies in the issuance and verification of credentials at cost. Organizations will have to shell out huge expenses on certification processes, and users will have to pay astronomical charges when applying for verification for purposes of employment or study. It is not viable, and so access to authenticated credentials is cut off, making forgery likely. Therefore, traditional verification processes are not economically and conveniently efficient in credential management.

Blockchain Based Credential Verification System aims to address all these problems by utilizing blockchain technology for the development of a decentralized, tamper-free, and fraud-free verification platform. In contrast to conventional practice, it ensures that once the certificate is made available and placed on the blockchain, it can never be duplicated or altered. The platform also carries out the verification procedure using smart contracts such that real-time verification of the credentials is carried out without interference from humans. By eliminating the middlemen third-party verification providers, it reduces operational costs and hastens the verification process to be quicker, more secure, and in bulk supply. This innovative solution guarantees people, institutions, and employers rely on the credibility of credentials with an affordable and effective verification process.

1.2 Key Features

Blockchain Based Credential Verification System offers a future-proof and secure method of managing credentials so that all certificates are securely stored, verifiable, and available at any moment. With the application of blockchain technology, the platform stores credentials on a decentralized ledger in such a manner that no individual is able to modify or alter in an unauthorized way. By implementing this decentralized methodology, issued certificates are assured to be permanent and available at any moment without loss or forgery.

One of the most powerful features of Blockchain Based Credential Verification System is that it can automate verification through smart contracts. These autonomous contracts authenticate credentials in real-time, saving time and effort otherwise spent on manual verification. Not only does this automation make the process more efficient, but it also does away with third-party intermediaries, making the whole process hassle-free and economical.

The website is built with functionality in mind and for application. It enables users to control their credentials via a user-friendly web-based and mobile-friendly interface, which makes it convenient for them to share their authenticated certificates with employers, learning institutions, and other concerned authorities. Maybe the most important innovation of Blockchain Based Credential Verification System is its QR code verification process, whereby every certificate that it issues contains a QR code that links to its blockchain record directly. This allows one to verify it in real time without necessarily having to communicate with the issuing body directly, and hence verification becomes much simpler. Because of its scalability and flexibility, BlockCred is capable of supporting numerous industries such as education, health, corporate training, and professional certification programs. With security, efficiency, and verifiability, the platform is going to revolutionize the digital credential management industry.

1.3 Research Objectives

The main goal of this research is to create a secure, efficient, and scalable blockchain-based credential verification system that surpasses the limitations of conventional approaches. Through the use of blockchain's immutability and transparency, the platform will eradicate fraud and unauthorized alterations, making all credentials forever verifiable and intact.

An interesting aspect of this study is embedding smart contracts into the verification system to enable real-time and instant automatic authentication of credentials. It would eliminate human intervention in manual verification and could shorten the verification time for academic, professional, and corporate credentials to a major extent.

Another central mandate is to establish a user-friendly and globally accessible credential management system. The research is aimed at developing a simple-to-use interface that allows individuals and institutions to issue, retrieve, and validate credentials without the need for technical savvy. Through removal of extra layers in certification, Blockchain Based Credential Verification System seeks to lower costs to institutions and individuals, lowering digital verification costs and making it easier to access.

Scalability is a core issue, where the ability of the platform to grow with growing users and credentials without degrading performance when it scales is taken into account. No less important is to be industry-agnostic by nature, such that corporate, university, healthcare organizations, and government organizations can implement Blockchain Based Credential Verification System with minimal hassle within established infrastructures.

Ultimately, the research hopes to establish a new standard for authenticating digital credentials through the integration of blockchain security and ease of use. In the pursuit of these goals, it is dedicated to transforming how issuing, storage, and authentication of credentials operate and establishing a secure, future-proofed platform for global utilization.

II. LITERATURE SURVEY

The increased need for a fraud-proof, effective, and safe credential verification system has driven large-scale research in industry and academia. The traditional certification methods have been researched extensively due to their limitations, including forgery, inefficiency, and high verification fees. To eliminate these pitfalls, researchers looked into blockchain technology as an alternative based on its decentralized, irreversible, and transparent nature.

The current credential verification systems are presented in this chapter and how blockchain is being utilized for digital certification. Through literature review, this research identifies past limitations and highlights how it aims to address them with a scalable, secure, and more reliable solution for credential management.

2.1 Survey of Existing Systems

Several studies have emerged to apply blockchain technology in digital credential management. Scholars aim to reveal how blockchain technology immutably holds credential data, verifiably checks it automatically, and objectively validates through no third-party entity. One such study by Zhang et al. (2023) considered the comparative aspects of decentralized certification systems. The research noted that blockchain offered a relatively secure alternative to traditional solutions, but existing laws and regulations could be obstacles to widespread adoption.

Smith and Johnson (2022) considered the introduction of decentralized identity management in education. The study highlights the opportunity blockchain provides for students and professionals to achieve autonomous self-sovereignty identities. Additional challenges to mass implementation were listed including scalability and inter-operation between current institutional enclaves.

A case study by Lee and Kim (2021) examined blockchain-based data validation for academic credentials, illustrating how smart contracts could ensure verification is done automatically, requiring less time and effort. Yet, it emerged from this study that most accessible blockchain applications were not generalizable and more improvement in user adoption strategies is wanted to champion scalability.

Nakamoto (2021) talked about the positive and negative sides of the adoption of blockchain in digital credential management. While this study directly focused on the use of blockchain for a transparent, fraud-proof avenue to certification, it undertook to impart also the negative side, such as cost, energy usage, and usability.

2.2 Identified research gaps

Regardless of ongoing research witnessing the efficacy of blockchain in verifying digital credentials, numerous challenges abound. Legal and regulatory compliance rank as one of the largest issues due to differences across countries and sectors in having varying digital certification requirements, complicating global adoption. Aligning blockchain-based systems for credentialing with legal paradigms stands among the highest impediments to adoption.

Another serious limitation is scalability. Blockchain-based verification systems are extremely secure and automated, yet most of the solutions in place today cannot be scaled large-scale across institutions. The transaction processing speed, storage, and processing cost are the determining factors of blockchain's scalability.

Cost-effectiveness is an issue that casts a large shadow, especially when it comes to blockchain transaction charges (gas charges). The majority of credentialing frameworks are on top of public blockchains whose costs of transactions could be volatile and costly. Upcoming studies have to grapple with lowering such costs without compromising the integrity and security of the blockchain network.

By filling gaps in this research, Blockchain Based Credential Verification System seeks to create a scalable, affordable, and accessible blockchain-based credential verification system that improves upon current practice with security, transparency, and broad usability.

III. Proposed system

3.1 Problem Statement and Objectives

The conventional certification systems are plagued with a number of challenges by virtue of being based on outmoded systems. The increasing adoption of the internet makes such systems vulnerable to inefficiencies, high-cost operations, as well as counterfeiting. Paper-based certificates are simple to replicate and hence vulnerable to forgery, and verification procedures take considerable time by virtue of cross-verification manually. Also, most modern digital certification systems have cumbersome and uninformative user interfaces, so their use is questionable. These are the reasons why there is a need for a secure, efficient, and user-friendly credential authentication system.

BlockCred resolves these concerns through the application of blockchain technology to provide a tamper-proof and decentralized setting for digital certificates. The technology automates certification validation by adopting smart contracts within the system, eliminating latency and reducing third-party verification requirements. This renders the certificate secure, immutable, and verifiable in the time frame of a blink of an eye, giving everyone involved an ease-of-use experience.

The key objectives of BlockCred are to enhance certificate security by leveraging the immutability of blockchain so that issued credentials cannot be tampered with or replicated. The platform ensures verification through real-time authentication through smart contracts, which can grant instant access to credential verification. One of the priorities is to make it easier to use, so the system is user-friendly and simple to use, making it possible for users to have their certificates at minimal effort. In addition, the platform aims to reduce the cost of doing business by eliminating unnecessary intermediaries and automating verification, therefore reducing the process's cost to institutions and individuals. Lastly, BlockCred is highly scalable and adaptable and can be applied in multiple sectors such as education, corporate training, and government offices.

3.2 Scope of the Work

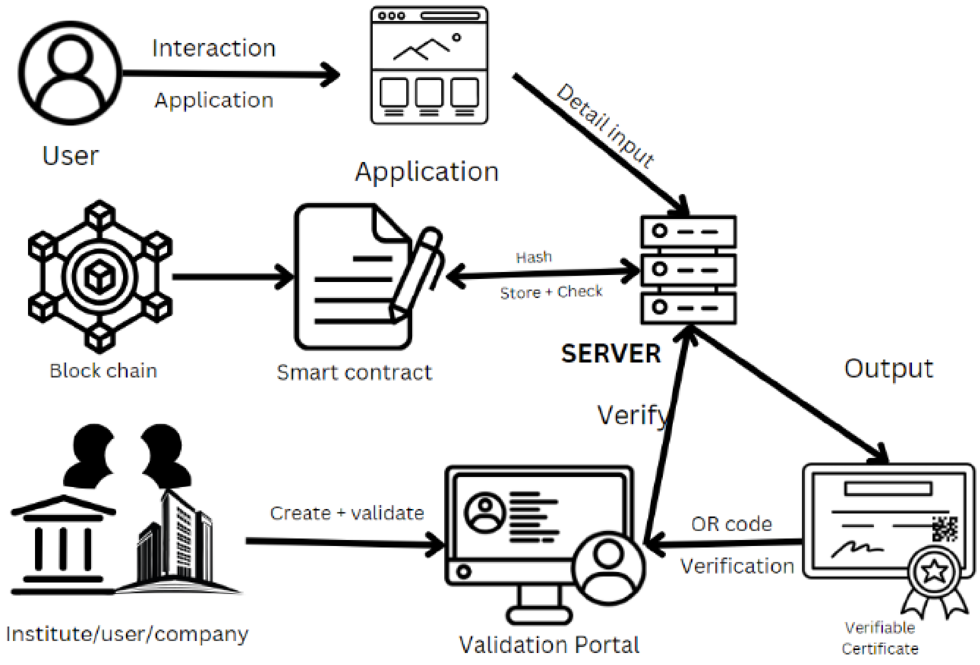
BlockCred is a distributed, scalable, and automated credential verification process that enables institutions to grant digital certificates and individuals to safely store and retrieve credentials. The system makes on-the-spot verification possible without human intervention and significantly lessens authentication delays. With the use of blockchain technology, the site ensures all credentials are tamper-proof, accessible, and stored forever, raising certificate security and transparency.

The platform targets education institutions, corporate organizations, and government agencies with a one-stop solution to issuing and managing digital credentials. The platform empowers universities to securely issue academic certificates, companies to confirm employee credentials, and regulatory bodies to authenticate professional licenses. The introduction of artificial intelligence (AI) fraud detection further enhances the security of the platform with the identification and prevention of fraudulent use of counterfeit or manipulated credentials.

Blockchain Based Credential Verification System is created to be able to support increasing numbers of users, and as such, it is scalable and can handle big demand as online credential verification keeps on increasing. The platform has a versatile system that can make it possible for different industries to tailor the platform to fit their own requirements. For degrees for school, certifications for the workforce, or licenses for the government, it offers an adaptable and secure platform that maximizes overall efficiency in handling credentials.

IV. System Framework and Architecture

Blockchain Based Credential Verification System is formulated to provide enhanced security, transparency, and efficiency in the credential authentication by making use of blockchain technology to give an immutable, decentralized, and tamper-resistant platform. The architecture comprises various elements, such as users, applications, smart contracts, servers, and validation portals, that help to issue, store, and validate digital certificates seamlessly. The subsequent paragraphs describe how every part of the system communicates to provide a secure, real-time, and cost-effective credential verification process.



4.1 User Interaction and Data Submission

The users start off by accessing the Blockchain Based Credential Verification System application through a web-based or mobile user interface. This is the main interface used by those who want to issue, store, or verify credentials. Users may input information such as personal identification, education qualifications, and professional certification, which are needed to generate a valid digital certificate.

After the data is submitted, it goes through preliminary verification checks within the application. The system ensures that the data entered is complete, accurate, and in accordance with institutional or industry standards. After this is done, the data is now ready for further processing and encryption before being securely stored on the blockchain.

4.2 Data Processing and Secure Storage

Upon submission, the system encrypts the credential information and transforms it into a secure cryptographic hash with the aid of advanced encryption techniques. The cryptographic hash is subsequently a digital fingerprint of the certificate, maintaining data confidentiality and integrity.

The hashed data are then saved on the Blockchain Based Credential Verification System server in a manner that the records are saved in a retrievable and orderly way. Unlike decentralized storage systems with a centralized structure where data can be deleted or altered, the hashed record saved on the server is merely a point of reference, and the verification actually happens at the blockchain network.

This two-layer solution secures credential records safely but accessibly without unauthorized alteration. This crypto-hashing solution also ensures the elimination of storage of personally identifiable information (PII) in any express form on the blockchain to ensure compliance with data governance and privacy regulations.

4.3 Blockchain Interoperability and Immutability

The app serves as a middleman between the users and the blockchain in order to ensure that all credentials that are being stored are securely stored in an immutable ledger. The moment a credential is issued and saved on the blockchain, it is tamper-proof and irreversible, thus ensuring that any forgery, unauthorized modification, or false presentation is prevented.

As blockchain is a distributed network, the lack of centralized management makes the system extremely hacker- and data-compromise-proof. This keeps the credentials effectively verifiable and auditable, at any time, without the issuer's involvement.
By using distributed ledger technology (DLT), it reduces the necessity to depend on third-party verification platforms such that the certifying process is accelerated, made more efficient and more reliable.

4.4 Smart Contract Execution

As soon as a request for a certificate is made, built-in smart contracts within the blockchain are self-activated. They are programmed and pre-authored contracts that do authenticity checks for verification of posted credential details with regards to predefined validating rules established during setup.

Precision and authenticity using smart contracts happen without interference. They do extensive checks that comprise .The establishment of legitimacy and authenticity of the issuing agency. Verification of whether the information given is consistent with the records being kept. Upon successful verification, the problem of issuing the credential is completed by the smart contract by creating a unique blockchain record for the certificate. Such operations being carried out through an open and automated process drastically cuts down verification time and eliminates the possibility of human error.

4.5 Server Communication and Data Management

BlockCred server is an active participant in processing communication between blockchain, application, and validation portal. It performs an intermediary role and is in charge of processing requests, deflecting data, and ensuring the whole process runs smoothly and trouble-free.

4.6 Validating Credentials using Validation Portal

After issuing a credential, institutions, employers, and other verification parties can verify a credential through the BlockCred Validation Portal. Validation must be fast, efficient, and highly automated.

4.7 Instant Verification Output

As soon as the system performs a verification check, it delivers a real-time authentication verdict. If the credential information matches the blockchain record, then the system verifies that the certificate is authentic and valid. If discrepancies are identified, then the system marks the credential as tampered or invalid so that only the original certificates are identified.

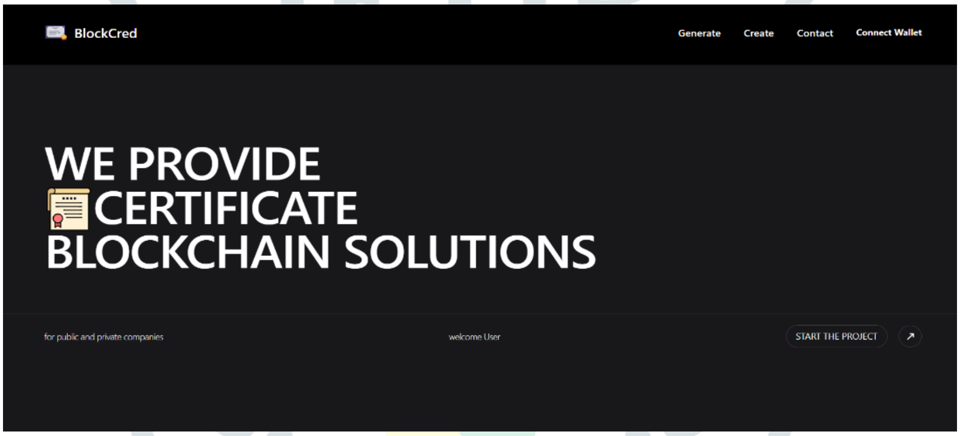
By doing it automatically, Blockchain Based Credential Verification System does not face any delays in verifications and can enable the employers and institutions to verify the credentials in mere seconds. It is of utmost benefit in the fields of education, healthcare, corporate recruitment, and professional licensure, where real-time as well as accurate verification is vital.

4.8 Decentralization and Trust

The decentralized structure of blockchain removes the third-party verification services, therefore the process is timely, cheap, and highly reliable. In contrast to a centralized database which could be hacked, blockchain-based verification guarantees that only verifiable and authentic credentials are accepted.

V. Results

Homepage: The homepage welcomes the blockchain-based certificate solution, by which users can access functionality like certificate issuance, verification, and wallet integration. It presents a seamless entry point for the secure credential handling process to be initiated.

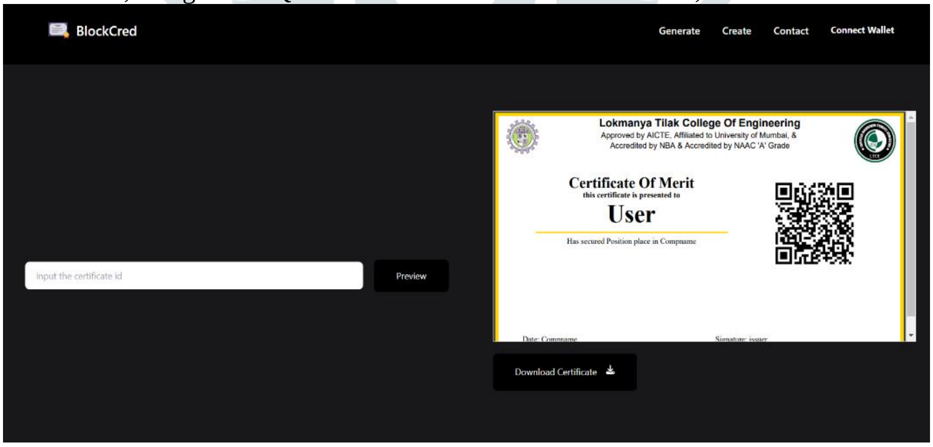

WE PROVIDE
CERTIFICATE
BLOCKCHAIN SOLUTIONS

for public and private companies

welcome User

Figure 5.1

Certificate Verification Page: Users can enter a certificate ID to instantly verify its validity, providing secure and tamper-proof verification. The verified certificate, along with a QR code associated with the blockchain, is shown for convenience and download.

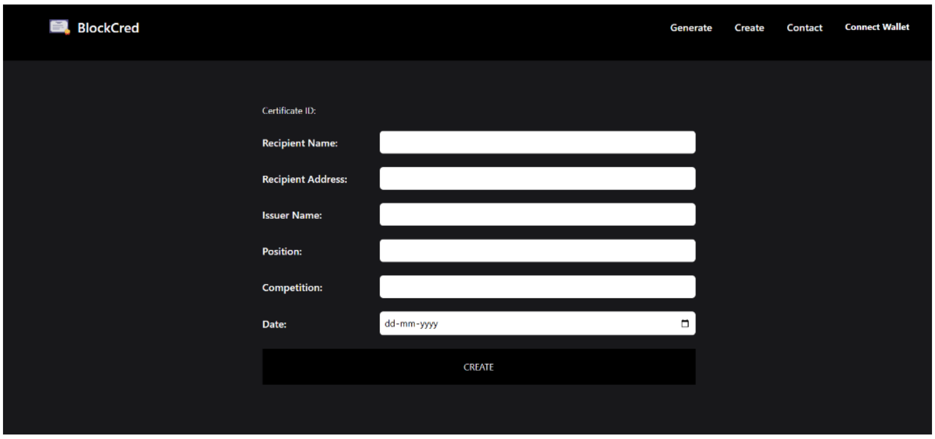

Lokmanya Tilak College Of Engineering
Approved by AICTE, Affiliated to University of Mumbai, &
Accredited by NBA & Accredited by NAAC 'A' Grade

Certificate Of Merit
this certificate is presented to
User
Has secured Position place in Compname

Date: Compname
Signature: issuer

Figure 5.2

Certificate Generation Page: The digital certificates are provided by the organization in charge by filling recipient information, issuer information, and additional required details. After submission, the system provides a distinct, blockchain-encrypted certificate for immutable storage and authentication.



Certificate ID:

Recipient Name:

Recipient Address:

Issuer Name:

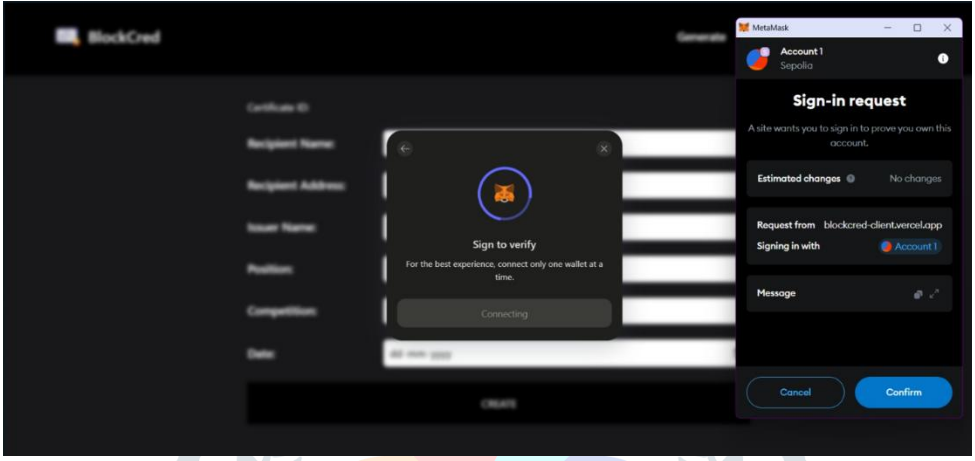
Position:

Competition:

Date: dd-mm-yyyy

Figure 5.3

Wallet Connection Page: A blockchain wallet like MetaMask needs to be linked by users to support transaction authentication and issuing of certificates. The integration increases security, decentralization, and access control of the system.



Sign to verify

For the best experience, connect only one wallet at a time.

Account 1

Sepolia

Sign-in request

A site wants you to sign in to prove you own this account.

Estimated changes: No changes

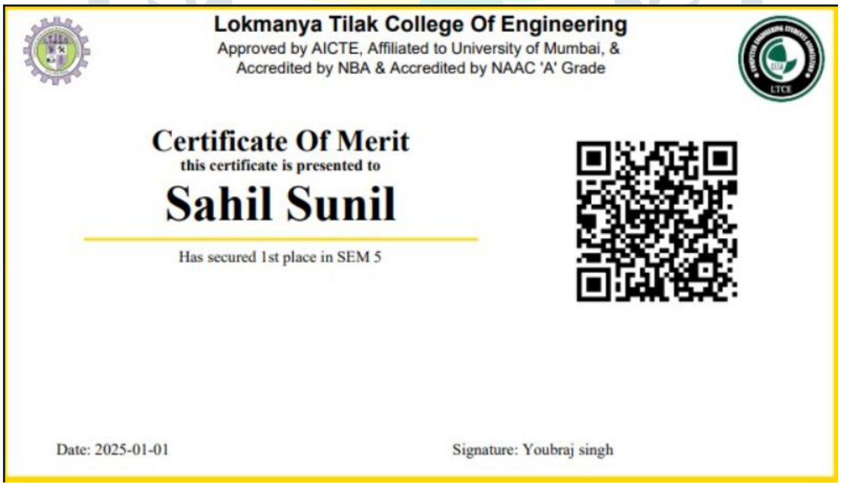
Request from: blockcred-client.vercel.app

Signing in with: Account 1

Message

Figure 5.4

Certificate Generated: User can be downloaded, shared, or printed while maintaining its authenticity through blockchain verification. This ensures secure and tamper-proof proof of achievement, accessible anytime for validation.



Lokmanya Tilak College Of Engineering

Approved by AICTE, Affiliated to University of Mumbai, &
Accredited by NBA & Accredited by NAAC 'A' Grade

Certificate Of Merit

this certificate is presented to

Sahil Sunil

Has secured 1st place in SEM 5

Date: 2025-01-01

Signature: Youbraj singh

Figure 5.5

VI. Methodology

Planning and system development have been done with utmost care to ascertain security, reliability, and effectiveness in authenticating credentials. Planning started by looking at the limitations of conventional certification processes such as fraud, inefficiency in the Mandragora pathway, extreme cost, and time-consuming verification processes. This study established the scope and intent of the platform to ensure it addressed the limitations adequately. After determining the minimum requirements, the architecture of the system was established, including how each of the different components would interact with each other. This included establishing data flow, security elements, and integration protocols for storing and verifying blockchain credentials. While creating, the system was made sure to be decentralized, immutable, and automatic so that institutions and end-users could have a smooth experience.

Development process consisted of coding the smart contracts using Solidity, the main programming language for Ethereum applications. The contracts were then run on the Ethereum blockchain via Remix IDE to allow for automatic, tamper-proof verifications of the credentials. To cater to the front-end, React.js was used in developing simple and light-weighted interface to facilitate ease of issuing, retrieving, and authenticating credentials. For the back-end, Node.js and Express.js were used in developing functionality that would facilitate provision for uncontrolled interactions between the users, the blockchain, and the authenticator system. To enable end-to-end real-time connectivity between frontend and blockchain network, Web3.js was used. This supported instant issuing, revocation, and verification of credentials without the need for human intervention and latency.

VII. Conclusion

Use of blockchain technology in credential authentication has revolutionized certificate storage, issuance, and verification. Those traditional systems have been plagued with fraud, verification lag, and operational cost and hence not feasible for large scales. With a tamper-evident, open, and decentralized mechanism, such a system ensures that the credentials are secure, verifiable at any time, and free from fraud.

One of the most robust features of this process is smart contracts, which authenticate automatically and eliminate the third-party verification procedure, thereby enhancing security, minimizing mistakes, and speeding up the verification process, enabling users and institutions to verify credentials in good time.

The system is extremely flexible, and therefore it is possible to apply it to various industries. Academic to corporate education, health care, and government licensure are some of the areas in which the system gives credentials in an accessible, trusted, and readily managed way.

From security, scalability, and accessibility principles, the system gives the foundation for an enhanced transparent and secure credential verification process. The future development will involve deployment of new cryptographic techniques for privacy protection, increased system interoperability with existing databases, and mobility integration to perform verifications on the move. By offering a fraud-free, low-cost, and universally available solution, this process establishes a new standard for digital certificate authentication, enabling individuals and companies to authenticate qualifications with complete confidence and security.

VI. REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin.org, 2008.

[2] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Whitepaper, 2014.

[3] G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," Ethereum Yellow Paper, 2014.

[4] K. Croman, et al., "On Scaling Decentralized Blockchains," Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, pp. 106-113, 2016.

[5] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World, Penguin, 2016.

[6] J. Bonneau, et al., "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," Proceedings of the IEEE Symposium on Security and Privacy, 2015, pp. 104-121.

[7] L. Guo and M. Xiao, "A Survey on Blockchain Applications in IoT," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4467-4477, 2019.

[8] A. Narayanan, et al., Bitcoin and Cryptocurrency Technologies, Princeton University Press, 2016.

[9] C. Catalini and J. Gans, "Some Simple Economics of the Blockchain," MIT Sloan Research Paper, no. 5191-16, 2016.

[10] A. K. B. So, "Blockchain and Cryptocurrency Technology: A Survey," IEEE Access, vol. 8, pp. 167798-167812, 2020.