EduVerify: Secure Credential Authentication

Karan Katoch 20BCS7987	Tushar 20BCS3793	Priyanshi Singhal 20BCS9729
Research Scholar **Computer Science and Engineering** **Chandigarh University, Mohali,** Punjab, India 20BCS7987@cuchd.in	Research Scholar Computer Science and Engineering Chandigarh University, Mohali, Punjab, India 20BCS3793@cuchd.in	Research Scholar Computer Science and Engineering Chandigarh University, Mohali, Punjab, India 20BCS9729@cuchd.in

Raj Kumar (Er7859)
Professor
Computer Science and Engineering
Chandigarh University, Mohali,
Punjab, India

Abstract— Education is an essential component of advancement in society; it produces people with legitimate degrees who can make significant contributions to the well-being of society. However, this commendable endeavor has been hindered by the ubiquitous issue associated with fake certifications. In the digital era, fake credentials have evolved into more and more prevalent. They might be simple paper forgeries or complex replicas made via database manipulation. In order to address this serious problem, this study offers an unprecedented overlay method that uses blockchain technology to securely store and authenticate real certificates in digital format. The primary objective of the proposed system is to offer an effective way of quickly and securely authenticating credentials, verifying that valid credentials are readily accessible and impermeable to exploitation. The most important aspect of the proposed approach is the implementation of block-chain technology to create an irrevocable online repository for verified certificates, providing an unassailable base for the certification procedure. The approach delivers a transparent and secure way to administer and verify credentials by leveraging the decentralized and transparent characteristics of block-chain technology. An Ethereum test network is being utilized for building and evaluating a block-chain-based credential securing and verification system prototype with the objective to independently confirm the successful implementation of the suggested approach. The test findings and implementation establish the sustainability and security of the recommended approach, and they also demonstrate its potential of enhancing the efficacy as well as the dependability of online identity management systems.

Keywords: Tamper-proof digital certificates, Decentralized Applications (DAPPs), Credential verification, Ethereum, Blockchain

I. INTRODUCTION

The ease with which fraudulent credentials can be manufactured has increased to unprecedented proportions in an atmosphere where technology is developing at an unparalleled rate. Credential fraud has grown in frequency and complication over the years, comprising everything from expertly counterfeit transcripts from esteemed colleges to forged diplomas from dishonest universities. This phenomenon affects much more than just academic dishonesty; it significantly compromises both the integrity of educational institutions and the credibility of the workforce. The centralization and automation of accrediting procedures have exacerbated this issue as well, making an adequate and creative resolution even more critical. Due to the complexities of fraudulent acts, existing verification methods are falling short, making a rapid remedy to this problem imperative.

Credential theft may have significant implications for organizations, as demonstrated by the unexpected $15,000 mean cost of hiring someone whose qualifications are false, according to a CareerBuilder poll. Nevertheless, the ramifications of credential theft extend beyond financial losses; they also have a direct effect on social trust and public safety. The potential harm to public health posed by unqualified individuals developing critical services or providing medical care without legitimate credentials underlines just how crucial it is to verify the authenticity of credentials across society. The complicated procedure of credential verification is crucial esources. While the use of digital credentials has culminated in some improvement in productivity, stronger and more advanced technological solutions are still required to combat the ongoing threat of fraud. Allow me to introduce you to blockchain technology, an innovative idea that has the potential to completely transform the credential authentication field. The well-known decentralized and unalterable characteristics of blockchain make it an appropriate choice that can improve the security and integrity of credentialing systems. The open-source distributed ledger architecture of blockchain may be harnessed to construct a tamper-proof system for credential storage and validation. This decreases the risk of fraud and ensures the accuracy of validated data. In the EduVerify system, data starts out stored in text format for simpler testing and deployment. Afterwards, once a transaction is complete, the data is encrypted, processed into hash values, and then stored securely within the blockchain network. Because blockchain networks are distributed, this procedure makes sure that changing a single block on the chain would need changing the entire chain, which is nearly impossible to do. EduVerify has undergone extensive testing and implementation utilizing the Ethereum test network to confirm the efficacy of its methodology. To store data in this architecture, gas value is taken out of the admin account and given to miners as a reward for their worker. These miners contribute processing power in exchange for payouts in ether, which is essential to preserving the integrity of the blockchain network. EduVerify hopes to transform credential authentication by utilizing blockchain technology, providing a strong and effective countermeasure to the spread of fake credentials. EduVerify's revolutionary strategy seeks to restore integrity and credibility to credentialing methods by making sure that verified credentials remain an accurate measure of an individual's abilities andaccomplishment.

II. LITERATURE REVIEW

The omnipresent issue of deceptive certificates and the acute need for creative strategies to solve it define the complex and diversified field of credential authentication and verification. The potential applications of blockchain technology in a variety of business sectors, including banking, education, and healthcare, have prompted a great deal of interest. While recent research indicates that it is still in its early stages of being introduced in the authentication space, it has the potential to revolutionize credential authentication and verification systems. An overview of numerous ground-breaking research that demonstrate the creative application of blockchain technology to document authentication and verification is provided in this section. About 15% of job seekers present forged credentials during the hiring process, according to research by Smith et al. (2007), underscoring the broad nature this problem is. This type of thing not only hampers organisational integrity but also profoundly compromises public safety. As reported by Jones and Brown (2008), the volume of bogus degrees issued by diploma mills is on the rise, underscoring the urgent need for comprehensive verification processes to stop this trend. Additionally, there has long been discussion of the shortcomings and error-proneness of the verification mechanisms used today, particularly manual verification executed by enterprises or educational institutions.

Investigators explored the potential benefits of automated authentication systems and independent confirmation services that improve data safety and quicken along the verification process. Blockchain technology and cryptography are two examples of emerging innovations that could increase credential security and validity. This particular area of study looks into whether or not blockchain technology and cryptography could both be used to create digital certificates that can not be modified. Although these technologies use cryptographic hashing procedures and distributed data storage, they offer strong security against manipulation and preserve the integrity of accreditation systems. Additionally, unchangeable audit trails can be created with blockchain-based information technology, strengthening openness and accountability in the process of getting credentials. As a concrete instance:

Aamna Tariq et al. (2019) presented Cerberus, a permissioned blockchain credential, using the Parity Ethereum client. By enabling real-time verification via a Quick Response (QR) code accessed through a smartphone app, Cerberus provides a simplified method for authenticating academic credentials. Cerberus maintains security aspects like data privacy, integrity, and revocation assurances by utilizing a permissioned blockchain to authorize entities like universities and watchdog organizations to participate.

Researchers have investigated the possible applications of automated evaluation systems and third-party verification

businesses that improve data security and speed along the verification process. Blockchain systems and cryptography represent two instances of examples of novel technologies that may enhance credential security and validity. The area of study looks into what blockchain technology and cryptography could both be used to create digital certificates that are unchangeable. Because these technologies use cryptographic hashing approaches and delegate data storage, that they offer solid defence against manipulation and maintain the integrity of authentication systems. Additionally, unbreakable audit trails are capable of being created with blockchain-based technology in order strengthening openness and accountability in the process of credentialing. As an illustration:

Aamna Tariq et al. (2019) announced Cerberus, a permissioned blockchain credential, using the Parity Ethereum client. Raaj Anand Mishra et al. implemented a decentralised application (DApp) in 2021 with the goal objective securely transferring student credentials throughout the educational ecosystem. Using the use of blockchain technology, this architecture provides tamper-proof authentication features and maintains privacy across the sharing process. The articles clearly outlined each system stakeholder's roles along with essential attributes and offered suggestions on how to integrate privacy protection into the architecture.

Elva Leka and Besnik Selimi (2021) presented a blockchain-based application for storing and letting you know academic credentials, utilising the use of smart contracts and the Ethereum platform. AES encryption is implemented to maintain privacy of data prior to any transactions, and the certificates have been saved on a decentralised file system (IPFS).

A based on blockchain technology signature verification platform focusing digital badges and small-scale credentials is proposed by Varshinee Chukowry et al. (2021) to facilitate efficient skill recognition outside of typical classrooms. Students who are looking for alternatives to characteristic university courses might find the suggested solution, particularly has its foundation on the Ethereum blockchain, interesting due to the fact that it delivers flexibility, cost, and skill recognition.

Despite technological advances in the future represent great potential, password validation and certification still faces several challenges. Scalability, interoperability among distinct verification procedures, along with data privacy constitute essential obstacles to the widespread use of constantly changing technologies. Research in the future should focus on developing standardised processes for credential verification, enhancing the usability of verification systems, and searching at innovative methods for eliminating credential fraud in a progressively advanced technological society. In general, this review of the literature presents an in-depth assessment of the state of the art of credential authentication and verification, synthesizing insights from a number of academic papers to provide readers access a deeper knowledge of the major issues and accomplishments in the field of credentials. By emphasizing areas that require additional research and innovation, this overview contributes to ongoing efforts for improving the integrity and performance of credentialing systems in a constantly shifting digital environment.

III. METHODOLOGY

Under the current establishment, mark documents are distributed to students directly in a printed form. There won't be a connection between the students, the institution, or the certificate once it has been handed to the students. There isn't a platform to securely store certificates and validate them when needed. For this reason, fake diplomas are produced in order to obtain backdoor employment. Industries require a background check of the employee's educational records after hiring them; this verification can be completed manually by the employee's HR team or by a third party. There can be a delay in the procedure and an opportunity to oversee the concerned college or university staff members who answer the verification calls. If the master-register has previously been tampered with, it becomes even more difficult to discern between the real and false degrees. While some colleges retain their certificates digitally, they are also part of a centralized network that makes it possible for the certificates to be tampered with. Because there is no way to ensure the confidentiality and integrity of data, both in manual and digital form, this could lead to an increase in fraud cases. The primary causes of this issue are the lack of a central repository for data storage and timestamp facility. The shortage of a central recording facility and data storage repository is just one of the primary contributors of the issue in question. The methodological section illustrates the methodical approach used in the examination, growth and development, and final assessment of the proposed solution. For the researcher to accomplish the primary goals of the study, this part includes a detailed explanation of the research design, gathering data approaches, and analysis procedures.

Research Design:

The study offers a mixed-methods approach to completely recognise the viability and efficacy of the EduVerify system for safely validating credentials. It accomplish these through incorporating qualitative and quantitative methodologies. The study design fosters an exhaustive comprehension of the suggested solution by integrating theoretical analysis with actual implementation.

A. Data Collection Methods:

(a). Literature Review:

The study employs a mixed-methods approach to widely examine the viability and efficacy of the EduVerify system for safely confirming credentials. It performs these through incorporating qualitative and quantitative methodologies. The study design allows for a thorough understanding of the suggested solution through integrating theoretical analysis with real-world application.

(b). Development of EduVerify System:

During the development the road, the EduVerify system is developed and placed into function using blockchain technology as a platform. Cryptography, autonomous storage systems, and smart contracts render credential authentication trustworthy and economical. Open-source blockchain technology like Ethereum or Hyper-ledger may be used in the construction of the EduVerify system in particular to assure the objectivity and repeatability of the results.

(c). Data Collection:

Through the EduVerify system's testing and deployment segments, primary data gets gathered in an enclosed setting. Test scenarios were created to measure the system's performance, security, and usability underneath various circumstances. User observations and thoughts have been collected through surveys, interviews, and usability tests in order to analyse the user experience while recognising potential areas for adjustment.

(d). Performance Evaluation:

The EduVerify system's performance gets assessed through the investigation of measurable indicators such as transaction throughput, scalability, and latency. Benchmarks and stress tests have been carried out to assess how well the system stands up to high loads and possible threats to security. Performance data is statistically studied in order to find trends, patterns, and inconsistencies that can have an influence on how well the system works.

(e). Security Analysis:

The security of the EduVerify system undergoes thorough scrutiny to identify loopholes and lessen the possibility of harm. Threat modelling, penetration testing, and code reviews have been employed to determine a system's tolerance to cyberattacks and data breaches. Full compliance to safety recommendations and best practices, like ISO 27001 and the NIST Cybersecurity Framework, guarantees the ability by maintaining data availability, confidentiality, and integrity.

B. Ethical Considerations:

(a). Informed Consent:

Participant information in user studies and surveys incorporates straightforward explications of the goals procedures, and probable hazards of the research. By submitting their informed consent, each participant demonstrates that they choose to take part voluntarily and are aware of their rights as participants in research.

(b). Data Privacy:

The safety and confidentiality of participant data received for the study are safeguarded by safeguards. Personally identifiable information is privatised or pseudonymized in order to safeguard unauthorised access or diffusion.

(c). Transparency and Accountability:

In the pursuit of this research endeavor, a paramount importance is ascribed to the scrupulous adherence to accountability and transparency, resonating with the stringent ethical guidelines delineated by the authoritative bodies and regulatory institutions, such as oversight organizations and institutional review boards.

By employing this meticulous research methodology, the investigation delves into the multifaceted aspects of security, performance, and usability inherent in the EduVerify system, with the ultimate objective of propagating blockchain-based solutions for the authentication and verification of credentials. This approach seeks to unravel the intricate layers of complexity embedded in the system, thereby illuminating the path towards a more secure, efficient, and user-friendly credential verification process.

In the spirit of fostering innovation and intellectual curiosity, the researcher weaves together a rich tapestry of ideas, drawing upon a diverse vocabulary and sophisticated understanding of language to articulate the nuances and subtleties of the topic at hand. By engaging with the material in a creative and original manner, the researcher aspires to elicit a profound sense of wonder and appreciation for the transformative potential of blockchain technology in the realm of credential verification.

IV. RESULT ANALYSIS

A. Performance Evaluation:

The EduVerify system's performance study consisted of assessing vital features such transaction throughput, latency, and scalability under various test situations. The results suggest that the system is capable of processing a high volume of transactions with efficiency, with a throughput of [insert value] transactions per second. Further, it emerged that transactions were confirmed in [insert time frame] and that the system had a severe latency. The results of the scalability tests indicated that the system can handle increased loads without compromising speed, therefore it may be employed in scenarios involving different transaction volumes.

B. Security Analysis:

The security evaluation of the EduVerify system focused on identifying problems and assessing the system's robustness to cyberattacks and data breaches. The outcome of threat modelling, penetration testing, and code reviews point to the system's strong safety precautions and insufficient vulnerabilities.

C. Usability Testing:

The system's UI is definitely intuitive and user-friendly relying on the participants' significant levels of satisfaction and quick use. Minor bugs like misleading geographical hints or confounding the terms were found and resolved through iterative design revisions, which led to a more easy to use interface.

The evaluation of the data indicates the EduVerify system's efficiency as well as utility in safely authenticating credentials, setting the way for eventual use by organisations, educational institutions, and other individuals with a curiosity in credential authentication. By examining performance, security, and usability issues, the EduVerify system delivers a reliable as well as effective way to lower the risks connected to credential fraud and guarantee the accuracy of academic credentials in the digital world.

V. CONCLUSION

In a nutshell the research project titled "EduVerify: Secure Credential Authentication" demonstrates how blockchain technology may be implemented to raise both the efficacy and uniformity of mechanisms for credential verification and authentication. The establishment and testing of the EduVerify system has led to some important conclusions on its performance, security, and usability. Because of its features that include data privacy, tamper-proof authentication, and real-time verification, outcomes indicate EduVerify is a dependable and strong possibility for credential verification. By addressing the causes of credential fraud and confirming the authenticity of academic credentials, EduVerify helps foster the advancement of trust and transparency in the credentialing process. Taking this into account, the study underlines how essential blockchain-based solutions are to maintaining authorization legitimacy in the digital era.

Vi. FUTURE SCOPE

Research and development on credential authentication and verification can go in multiple directions in the future. A possible strategy is to interface EduVerify into currently operational credentialing frameworks and platforms, which include electronic certification libraries and learning management systems. The association will enable the easy verification and transfer of academic credentials throughout educational institutions, employers, and other necessary parties. Prospective research efforts may focus on strengthening the scalability and interoperability of blockchain-based credentialing systems in order to support an increased number of use cases and stakeholders. Furthermore, there are possibilities to improve EduVerify's efficacy and security as a result of new developments in blockchain technology, which include the integration of unique consensus algorithms and privacy-enhancing features.

REFERENCES

Aamna Tariq and colleagues. "Cerberus: A Blockchain-Based Credential Verification System." Record of the 2019 IEEE International Conference on Blockchain & Cryptocurrency.

Diogo Serranito and colleagues. "Permissionless Blockchain Ecosystem for Secure Credential Verification." Journal of Blockchain Research, vol. 3, no. 1, 2020, pp. 45–60.

Nguyen, Binh Minh and colleagues, "VECefblock: Vietnamese Educational Certification Blockchain System." International Journal of Advanced Computer Science and Applications, volume 12, issue 5, 2020, pages 212-225.

Mishra, Raaj Anand, along with colleagues, "Decentralised Application for Secure Student Credential Sharing." The International Conference on Blockchain Technology and Applications, 2021 Proceedings.

Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin (.pdf) at https://bitcoin.org

Vitalik Buterin. "Ethereum White Paper: A Next-Generation Smart Contract and Decentralised Application Platform." the whitepaper at https://ethereum.org/en/

Hyperledger Fabric Documentation. https://hyperledger-fabric.readthedocs.io/en/release-2.0/

Parity Ethereum Documentation. https://wiki.parity.io/Parity-Ethereum