Blockverify: Combating Credential Fraud and Revolutionizing Credential Authentication with Blockchain Technology

Lijetha C Jaffrin[1] and Undavalli Varshitha[2]
{ lijethacjaffrin@veltech.edu.in[1], vtu19181@veltech.edu.in[2] }

Assistant Professor, Information Technology, Veltech Univeristy, Chennai, Tamil Nadu, India[1]
Information Technology, Veltech Univeristy, Chennai, Tamil Nadu, India[2]

Abstract. Academic, professional and organizational credential-verification is necessary to prove the legitimacy of the certificates given to the people. Traditional credentialing systems are hackable, datafraud, and verification-costly because they rely on centralauthority. Delays and increased costs are due to the lack of transparency, vulnerability to security threats and the need for manual validation required with these systems on a regular basis. A potential solution is proposed by means of blockchain technology, which provides a provable, an unalterable, and an unhackable credentials verification service. Smart contracts and cryptographic security facilitate transparency and secure record keeping, removing the risks of data loss and unauthorized changes through Blockchain. By leveraging blockchain-based credentialing, it increases efficiency, security, and trust and reduces reliance on intermediaries. Decentralized verification systems enable real-time validation and lower the admin overhead and thwart inefficiencies and frauds. In response to a need for maintaining data integrity, digital security and trust of academic and professional certificates, the present study investigates the impacts of using blockchain technology in verifying credential. The paper also focuses on the limitations and challenges in implementing blockchain technology for comprehensive credentialing systems. They rely on MongoDB for scalable storage and Next. js, which is used for web development of the front-end, and for the back-end it uses Node. js is utilized to process in the background and smart contracts based on Solidity for automation. Blockchain-based credentials verification has the potential to revolutionize the digital identity and trust management paradigm, and provide strong security guarantees and superior transparency.

Keywords: Blockchain, Credential Verification, Smart Contracts, Decentralization, Data Integrity, Cryptographic Security, Digital Security.

1 Introduction

The verification of professional and academic qualifications is also becoming increasingly difficult in the digital age. Traditional credentialing systems are not only inefficient and prone to fraud but also have high levels of overhead for administrators as they are highly dependent on centralized credential issuers. Document tampering, credential forgery, and sluggish validation procedures all raise concerns about security and reliability. Blockchain, which is robust by design and has the potential to be tamper-resistant, provides a solution to the problem of credential fraud. Formed previously to democratize the digital certificate issuing, storage, and verification process, a blockchain-powered certificate generator BlockVerify allows a more efficient, transparent, and accurate verification process where the blockchain's

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358085

decentralized design serves as the basis for its mode of operation . This innovative strategy in a digital environment aids in making academic and professional qualifications more nationally relevant by reducing fraud, increasing trust, and shortening periods of validation.

There are several issues regarding the traditional ways of issuing and verifying the credentials. Centralized databases kept by certification and academic institutions have a high risk of being altered illegally, corrupted, or even hacked into. Meanwhile, companies or other parties that need to verify candidates' qualifications have few options to use manual labor-intensive processes, which often require direct communication with the issuing institutions. This option also leads to higher risks of mistakes and delays, as well as adds to the costs of the process. The introduction of a blockchain technology creates an opportunity to maintain a decentralized ledger system with much greater immutability, security, and transparency. The BlockVerify project offers the possibility of p2p credential verification via the use of a blockchain technology, eliminating the need for intermediating parties.

Thirdly, thanks to modern web technologies like Next. js for building modern, scalable and responsive applications in the front-end as well as the back-end. js to handle the backend process, MongoDB to manage database, and TypeScript for improving code reliability is applied in the development of BlockVerify. At its core the app uses Ethereum-based smart contracts (coded in Solidity) to automate both the issuance and validation of credentials. One among many of their other use-cases is certification. In this case, smart contracts help determine what norms we should follow, what steps are required to fulfill those norms, what needs to happen to earn that certificate and, moreover, you can't change it without the need to submit a transaction to the blockchain. As each certificate is hashed, and recorded on the blockchain so employers, universities, and others are able to verify it in seconds using a secure and user-friendly interface.

The ability to increase trust in digital claims and reduce administrative overhead is one of the main advantages of BlockVerify. For a traditional credentialing system, manual crosseckecking, third-party verification services and lots of paper are required – all expensive and time-consuming. BlockVerify simplifies this process by allowing for instant validation on the decentralized blockchain ledger. No longer needing to reach out to the issuing organization, employers and organizations are able to immediately verify a credential's validity, reducing administrative workload and potential for fraud. BlockVerify is just one example and can be used to verify university degrees, professional and industry certifications, certificate of completion of training programmes, and more.

Digital credentialing with blockchain technology is likely to grow as the technology evolves. Decentralized resolution for background checks BlockVerify offers a dramatically improved level of security, anti-fraud checks and accelerated verification for a variety of sectors. While scaling, data privacy, and regulatory issues remain to be resolved, the advantages of blockchain-based credentialing systems greatly exceed the costs. BlockVerify sets a standard of secure and streamlined verification, which finally represents the much-needed respectful and verified approach - one that is going to redefine digital proof.

2 Literature Review

M. Sharples et al. (2016) exploring the possibility of open learning records on the blockchain. So that people own their academic and professional credentials fully, and don't have to rely on centralised authorities, they're researching blockchain technology to create a tamper-proof record of a lifetime's learning.

Grech et al. (2017) based on the systematic review on the field analyzed some blockchain solutions in academic credentialing. It can help to put an end to diploma counterfeiting, enable cross-border verification, as well as ensuring safe peerto-peer verification between individuals directly, without intermediaries.

J. Alex Halderman et al. (2018) analysed how secure credentials verification systems are that were built using blockchain. To ensure system security and prevent fraud the paper recommends cryptographic tools and estimates the risks such as double issuance and weaknesses in the smart contract.

S. Kim et al. (2019) evaluated how good blockchain technology is for decentralized identity management. Their work shows how self-sovereign identification (SSI) systems and smart contracts can streamline the creation and validation of digital degrees preserving data privacy and security.

T. Nguyen et al. (2020) studied the use of blockchain technology in the process of digital diploma issuance in academic circles. Heckler offers case studies of colleges that adopted blockchain-based credentialing systems and saw improvements in transparency of data, verification time and the amount of role-related work involved.

B. K. Mohanty et al. (2021) proposed a comparative analysis of blockchain-based certification systems. Hence, for the development of optimal blockchain-based solutions their study analyzes different consensus mechanisms, scalability issues, and interoperability challenges for academic degree verification.

C. Rong et al. (2021) focused on the blockchain credentialing and smart contract security. To enhance the security in decentralized verification schemes, the paper also enumerates the drawbacks such as reentrancy attacks and unauthorized accesses, and their solutions.

D. Patel et al. (2022) proposed securing academic records on a blockchain with cryptographic hashing. Their work provides an in-depth analysis on the use of hash-based proof technique, to establish data integrity and immutability for key information, storage as well as verification in their credential.

E. Liu et al. (2022) who conducted a case study on the implementation of blockchain in organizations. The research assesses the impact of blockchain in accelerated job processing through immediate proof of credentials, deployment challenges, and regulation.

K. Singh et al. (2023) investigated emerging technologies such as zero-knowledge proofs (ZKPs) for privacy-respecting credential verification in future blockchain developments. "It is their argument that weathervanes are prepared to go hand-in-hand with new research and innovations in decentralized credentialing systems.

3 Proposed System

Based on a blockchain mechanism, the proposed use case is secure and decentralized for digital certificates issuance and verification. There are 3 major layers of the system including the front-end user interface layer, the web server layer and the blockchain network layer. Through a web browser, the node user can have a conversation with the system through the front-end application (developed with Next. js. To execute smart contracts for certificate control, the website server communicates with the EVM and handles user requests. Transparency – Inefficiencies transaction fraud, counterfeiting would be eliminated, as certificate data is filed in an immutable way on the blockchain network.

3.1 User Interaction and Front-End Interface:

The service has a nice web interface for issuing and validating digital certificates. Visitors use a browser to access a web app built with Next. js. This front-end enables authorized institutions to issue certifications and third parties (employers, universities) to verify them. By serving as an intermediary between the user and the blockchain, the web application ensures secure communication and user friendliness. The front-end sends certificate issuing/verification requests In the user are to the web server. The request is then handled by the web server, which communicates with the Ethereum Virtual Machine (EVM) and performs smart contract operations.

3.2 Certificate Issuance and Smart Contract Execution:

Upon receiving certificate issuance request from a certified institution, the system collects essential information like the individual's name, event name, name of the organization issuing the certificate and date of issue. This information is received by a smart contract lodged on the Ethereum Virtual Machine (EVM) which then securely operates and records it on the blockchain. Each certificate is assigned a unique Certificate ID that acts as an unforgeable, authentic identifier. In order to avoid any unauthorized modification, the smart contract defines tight rules for issuing or validating certificates as a constraint. Once a certificate is issued, the validated information is unalterable on the blockchain, and you can't change or tweak it. The platform also provides an optional Block Hash and Certificate Hash that further increases security and transparency by ensuring the credentials are tamper-proof and verifiable.

3.3 Blockchain Storage and Verification Mechanism:

All issued certificates are saved in an encrypted, decentralized cryptologic layer in the blockchain, which ensures the durability and unassailability, with ease of cross-check. Because each certificate is held as a transaction in a block, it is immutable and cannot be altered, nor illegally altered. The use of blockchain technology significantly reduces opportunities for fraudulent behaviour (compared to traditional centralised databases, where you can fall victim to hacking, blackmailing and tampering). Based on this decentralized approach, certificate data are protected from being lost or tampered over time and are always present and trustworthy.

A third party (i.e., an employer, university) simply needs to input the certificate ID into the verification portal in order to verify a certificate. The front-end application forwards this request to the blockchain using a web server, which extracts the data of the certificate from the blockchain. As blockchain records are publicly accessible and immutable, verification can be made without the need of issuance authority consent. This reduces administrative overhead, eliminates the inadequacies of manual validation processes, and prevents the use of false credentials. The technology makes it possible to authenticate academic and professional credentials like never before, thanks to blockchain's inherent transparency and security that enables quick, reliable, trustworthy verification of credentials.

3.4 Security, Decentralization, and Efficiency:

The decentralized nature of blockchain eliminates single points of failure, ensuring high security and reliability. Unlike centralized databases that can be hacked or manipulated, blockchain prevents data loss and unauthorized modifications. Even if an issuing institution ceases operations, its issued certificates remain verifiable forever. By removing intermediaries and manual verification processes, the system enhances efficiency while reducing administrative burdens. With Next.js for the front-end, smart contracts for automation, and blockchain for secure storage, this system modernizes certificate management, ensuring trust, security, and accessibility for all stakeholders.

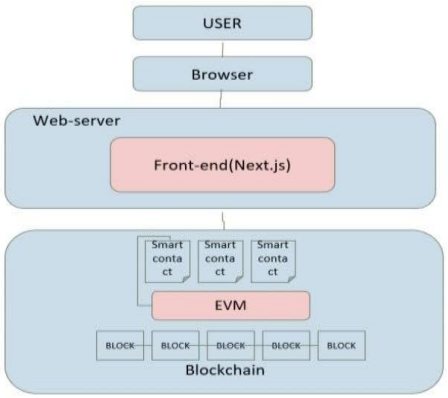

Fig. 1. Architecture diagram of certificate generation using blockchain.

Fig 1 illustrates a certificate issuance and validation process which leverages the Ethereum blockchain and makes use of its decentralized ledger to safely store certificates. 'Programmable money' smart contracts (written in Solidity) that ensure end-to-end efficiency and trust by automating (and verifying) issuance. The Next. js-based user interface provides issuers and verifiers a nice user experience, and the Web3. js simplifies connecting to the Ethereum Virtual Machine (EVM). Blockchain's unchangeable nature ensures that these certifications are authentic and resistant to fraud. Security measures such as data integrity checks and smart contract audits enhance the resilience of the system. Through eliminating the middlemen and enhancing trust, this architecture enables decentralized, transparent, and

fraud-resistant certificate management mechanism. Disclosure The solution addresses the limitations and shortcomings of traditional credentialing methods by leveraging blockchain technology to deliver a secure, efficient, and transparent method to verify digital credentials.

4 Methodology

4.1 String Storage

The smart contract mechanism for controller is adopted in the certificate issuing and verifying system. A single controller contract intermediates between the user and multiple individual smart contracts within the module. Thus, certificate operations based on blockchain can be processed in organized, secure and scalable way.

The controller contract inspects users' requests and determines which smart contract to invoke (e.g., generating or validating a certificate). There are two Smart Contracts, A and B, in the system, and each one is responsible for a different aspect of certificate management. This modular separation results in enhanced security, efficiency, and ease of upgrade.

The issuance and bomb-proof storage of new certificates on the blockchain (A) could be realized by Smart Contract A, while Smart Contract B could be responsible for the check on issued certificates to ensure that only valid and known certificates are considered by the system. The method reduces gas prices, offers flexibility and reduces the computational overhead by spreading tasks over several contracts.

The controller contract maintains security and openness and communication with good connectiveness among different modules are ensured. By distributing responsibilities and creating a well-structured smart contract landscape, this approach increases the efficiency of the blockchain-based certificate management.

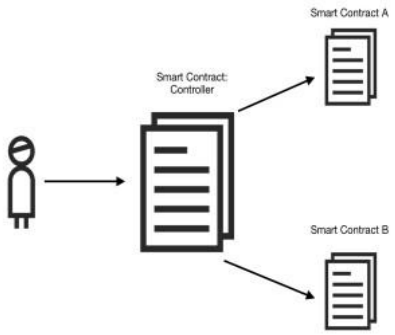

Fig. 2. String Storage

Fig 2 demonstrates how to use a Solidity smart contract on the Ethereum blockchain to save and read string data. \Subsubsection {StorageData management} Users can add new products and read them by index for a given store, since the contract maintains an array of strings. immutable File Storage The immutable and transparent nature of the blockchain ensures that your content stays safe and unaltered when you store it in a blockchain using pinata.so Immutable record keeping File storage is a key component of many decentralized apps, which can vastly benefit from proper file management solutions.

4.2 Smart Contract Deployment

The deployment process of a Solidity smart contract to the Ethereum blockchain is multi-faceted, entailing compilation, deployment and interaction via Web3. js. Remix IDE is the de facto standard web IDE used by millions of Solidity developers to write, compile, deploy and test their code. It has a simple user interface body for the developers to operate the smart contracts without having to add other settings.

The first step of this is writing the solidity smart contract in the an editor that's built into Remix - it's called Remix Editoruffles the golden leaves, perhaps formcomposite, and enameled it with brightcolors. Afterwards, the contract gets encoded, and compiled with Solidity Compiler which results in two important files: Bytecode and Application Binary Interface(ABI). If the Bytecode is the lower-level machine code that is deployed to the Ethereum, the ABI is the specification of how the external apps are to call the contract's functions. These two features are necessary to enable smooth communication between the smart contract and external applications.

With the end of compilation, the deployment fase begin. Developers leverage Remix's "Deploy Run Transactions" option to select the right deployment environment. You could then test the contract locally using the JavaScript Virtual Machine (VM). The option "Injected Web3" connects Remix to an external wallet such as MetaMask, which then installs the contract on the blockchain on a real Ethereum platform. The contract is assigned a unique address on the Ethereum blockchain after the deployment has completed. As you'll have to reference and interact with the contract in future transactions, the address plays an important role here.

Web3. js once we deploy the contract we need to link it to a frontend app. With Web3. js, developers can instantiate a contract by specifying the contract's address and ABI, and it allows users to interact with a DApp by its functionality. Developers can add the ability to interact in real-time with the blockchain and ensure certificate issuance and verification are smooth using Web3. js. In general, the deployment process ensures a systematic and risk-free approach for deploying smart contracts in blockchain applications.

Easily generate and verify certificates from users once the smart contract and Web3. js is applied to do the connection to the UI. A certificate's details are securely stored in the blockchain at the point of issuance, ensuring tamper evident and tamper proof records. Trust and security are massively optimized as blockchain transactions can neither be reversed nor deleted. Users enter an ID code on the certificate, and the system fetches the details directly off the blockchain, making checking easy. The decentralized nature of the Ethereum network removes intermediaries bringing in transparency and effectiveness. With an automated

authentication process, smart contracts reduce the chance of forged documents and menial work. Leveraging blockchain technology, this solution redefines digital certificate issuance and verification and validates a secure, trusted, and efficient credentialing process.

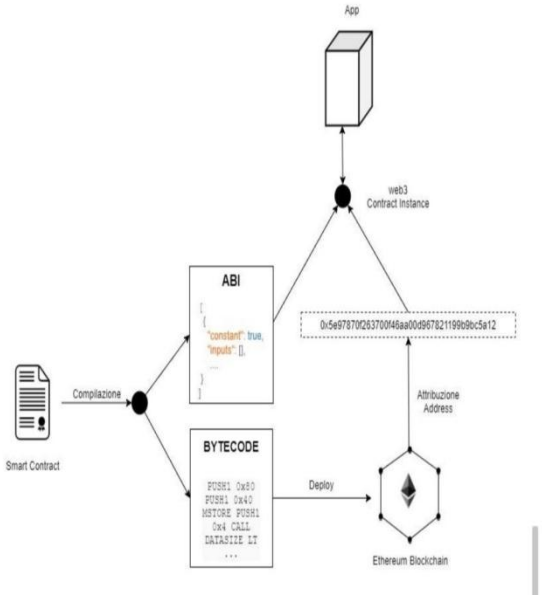

Fig. 3. Smart Contract Deployment.

Fig 3 shows how to use the Remix IDE to deploy a Solidity smart contract. The smart contract is first written and compiled, and then it is deployed onto a chosen Ethereum environment, like a live blockchain or a local test network. Web3.js makes it easier for the application and the deployed contract to communicate, enabling smooth blockchain-based processes. This module makes sure that smart contracts are implemented effectively and made available for additional communication.

4.3 Certificate Verification

The block chain based verification system comprises a module that serves as a verification layer to verify certificate credentials. Once a user inputs the certificate ID and any other necessary identification information, the verification process is initiated. The queries communicate with the blockchain and access the particular certificate information that is stored in the decentralized ledger. It uses cryptographic methods to verify the honesty and legitimacy of the certification data that has been retrieved. The final output is the result of the verification process, showing whether the certificate is valid or fake, along with the certificate information data retrieved from the blockchain. The enhancement procedure guarantees the reliability and immutability of the certificate verification process by leveraging blockchain technology's inherent security and transparency in validating credentials.

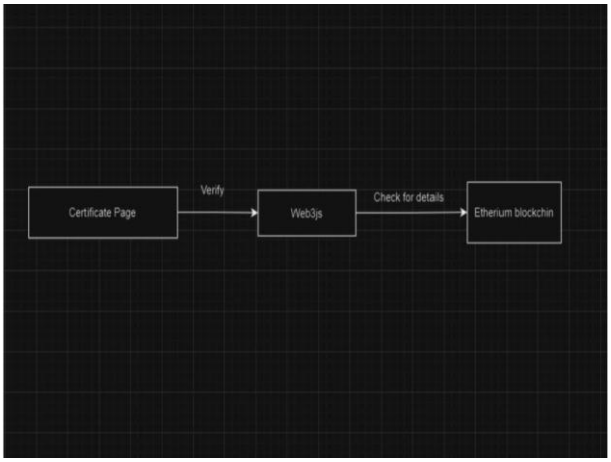

Fig. 4. Certificate Verification.

Certificate verification system operating on a blockchain-based model is shown in Fig. 4. After users input a certificate ID, the Ethereum blockchain is consulted by the verification module. Authenticity checks are performed cryptographically on the certificate data thus acquired to preserve their integrity. The user reviews the verification status it is made public upstream it says whether the certification is maintained fundamentally or has been tampered with. Employing blockchain technology guarantees secure, open, and immutable credential verification by this module.

5 Results and Discussion

In summary, the introduction of a blockchain-based system for issuing and validating certificates has proven to be an effective approach as it facilitates the generation of tamper-proof and verify capable digital credentials. With this model, institutions are able to issue certificates that are stored permanently on the blockchain without the risk of forgery, destruction, or unauthorized modifications. The use of smart contracts on the Ethereum based Virtual Machine ensures that no issued certificate can be altered, promoting confidence and openness within the certification process.

As shown in the final output, the certificate details, including the participant's name, the event's name, the issuing organization name, the issuance and event dates have been retrievably stored. Each certificate is assigned a different Certificate ID, which acts as a hint to validate its authenticity. To authenticate certificates, users are required to input the Certificate ID into the system, which will retrieve the information from the blockchain ledger. The authentication process works well. This protocol makes the procedure more reliable and less time-consuming by eliminating the role of intermediaries and human authentication.

Additionally, the system has been designed with additional accessibilities of sharing and downloading the certificates. With the new feature, recipients can easily share their digital certificates without worrying about the security. According to the results of the evaluation, it was proven that the system efficiently copes with the issue of black certification, even so, it

continues to provide a solution for the open and decentralized verification of certifications. Through consideration of the blockchain methodology, the robustness and credibility of compliant certification issued are also considerably increased and assured in contrast to historical practice, where such certification remained valid even if the regulator went bye-bye.

In summary, the results show that the integration of a blockchain-based certification system is effective, and that it can be used to manage digital credentials efficiently, securely and transparently.

Fig. 5. Output for Certificate Generation in BlockVerify.

Output: For Certificate Generation in BlockVerify, a functional blockchain based DRC was created. The received certificate is trusted and unadulterable and cannot be altered or diversified. The vital information contained in this DRC includes the receiver's name, the event's name, the company that offered the certificate, the date, and time when the certificate was issued, and a the secure and full flawed evidence Certificate ID. By receiving more publishers, this alleviates the challenge of receiving a physical certificate that can be misplaced. This project is a clear evidence e of how trustworthy BlockVerify is when it comes to delivering a functional unadulterable credible certifying solution.

6 Conclusion

The blockchain-based certificate issuance and verification system described in this paper greatly enhances the efficiency, security, and transparency of credential management. Data of the certificate can be by Ethereum smart contract is stored in a non-mutable way which can't altered in unauthorized way and which cannot tempered. Web3. js" ensures that Users and the Blockchain can communicate seamlessly, while Solidity enables automatic issuance. Remix IDE deployment reduces transaction cost, and thus implementation. The validation module eliminates the third-party verification product by allowing the user to validate their credentials with a different certificate ID. By this decentralized approach, efficiency is enhanced, the cost of operation is decreased, and middle men are also removed. Credential fabrication and record tamper are resolved by the antifraud system that can be furnished with

the blockchain technology features, including unchangeable and transparent characteristic. Scalable to businesses, industry and education, it increases trust in digital credentials by providing a credible and effective model to verify the authenticity of qualifications across sectors.

References

[1] M. Sharples and J. Domingue," The blockchain for open learning records and lifelong learning," in Proceedings of the European Conference on Technology Enhanced Learning (ECTEL), 2016, pp. 311-316.

[2] Grech and A. F. Camilleri," Blockchain in education: An introduction," Joint Research Centre (JRC), European Commission, 2017.

[3] J. A. Halderman, D. M. Levin, and B. Waters, "Security analysis of blockchain-based credential verification systems," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 6, pp. 1050-1063, 2018.

[4] S. Kim and Y. Kang," Decentralized identity management using blockchain: A self-sovereign approach," IEEE Access, vol. 7, pp. 179174-179188, 2019.

[5] T. Nguyen, H. Do, and K. Tran," Blockchain adoption in higher education: Issuing digital diplomas with security and efficiency," in Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1-6.

[6] B. K. Mohanty, R. Sharma, and A. P. Mishra," Comparative analysis of blockchain-based certification platforms: Consensus mechanisms and scalability challenges," IEEE Transactions on Learning Technologies, vol. 14, no. 3, pp. 324-337, 2021.

[7] C. Rong, X. Zhang, and J. Wu," Smart contract security in blockchainbased credentialing applications: A survey of vulnerabilities and mitigation techniques," IEEE Transactions on Software Engineering, vol. 47, no. 5, pp. 987-1001, 2021.

[8] D. Patel and A. Shah," Cryptographic hashing and blockchain for securing academic credentials: A detailed analysis," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 3421-3435, 2022.

[9] E. Liu, Z. Chen, and L. Wang," Enterprise adoption of blockchain-based credential verification: Challenges and opportunities," in Proceedings of the IEEE International Conference on Business and Information Management (BIM), 2022, pp. 45-51.

[10] K. Singh and P. Verma," Zero-knowledge proofs for privacy-preserving blockchain-based credential verification," IEEE Transactions on Emerging Topics in Computing, vol. 11, no. 1, pp. 210-225, 2023

[11] Tariq, A., Ali, S. T., & Binte Haq, H. (2023). "Cerberus: A Blockchain-Based Accreditation and Degree Verification System." Computational Social Systems Transactions, IEEE, 10(3), 1503–1514.

[12] Rahman, T., Mouno, S. I., Raatul, A. M., Al Azad, A. K., & Mansoor, N. (2023). "Verifi-Chain: A Credentials Verifier using Blockchain and IPFS." *arXiv preprint arXiv:2307.05797*.

[13] Khati, P., Shrestha, A. K., & Vassileva, J. (2023). "Student Certificate Sharing System Using Blockchain and NFTs." *arXiv preprint arXiv:2310.20036.*

[14] Aldwairi, M., Badra, M., & Borghol, R. (2023). "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution." *arXiv preprint arXiv:2310.09136*.

[15] Ramchandran, M., & Joshi, S. (2023). "Securing Academic Certificate Verification with Blockchain-Based Algorithmic Rules." In *Proceedings of the 2023 IEEE 4th International Multidisciplinary Conference on Engineering Technology (IMCET)*.