Certificate Authentication System Using Blockchain

Murugan Sekar, A. Rajesh, S. Thirumal, and R. Anandan

1 Introduction

Data security is a major concern in this digital world. Blockchain features decentralized, peer-to-peer (P2P) and unalterable information that has a huge ability for a variety of purposes. It can be described as a distributed ledger technology that has a frequently appending public ledger. A group of blocks interconnect between them to form a blockchain and every block contains or follows information about all latest transactions once completed it was kept for good permanently on a blockchain network that is secured and immutable too. When a general agreement is achieved between various nodes, the details of the transaction are appended to a block that previously contains information for multiple transactions. The hash or numeric value of the appropriate last connection is found in every block. All blocks are interconnected and together these blocks will be forming a blockchain. Information is distributed because it is distributed to various nodes (distributed data management). As a result, the database is jointly maintained by these nodes. The block will not be validated in the blockchain until it is validated by several users. Also, the originality of the block cannot be changed freely. For example, blockchain-based smart contracts can create reliable systems to dispel doubts about the authenticity of the information. Blockchain is different from traditional databases in that the blockchain is decentralized as a result of there being no intercessor or negotiator, and it's confidential.

Figure 1 represents the evolution of different versions of the blockchain from 2005 to 2022.

M. Sekar (✉) · A. Rajesh · S. Thirumal · R. Anandan
Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India

S. Goundar, R. Anandan (eds.), *Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations*, EAI/Springer Innovations in Communication and Computing, https://doi.org/10.1007/978-3-031-35751-0_13

Fig. 1 Evolution of blockchain versions

Ethereum smart contracts have been introduced in early 2005. From then, the blockchain technology has been enhanced to blockchain 2.0. Problems related to digital wallet and decentralized transactions have been encountered in cryptocurrency; to solve these, blockchain 1.0 was primarily developed. Blockchain 2.0 focuses on worldwide decentralization and is used to send or receive assets through smart contracts and the emerging Bitcoin alternatives created a lot of value. The open-source and decentralized platform named Ethereum had good completeness and support for a variety of enormous applications. Ethereum played a major role in building a variety of smart contracts and decentralized independent organizations [1]. If bitcoin was considered as a world payment system then the worldwide computing system will be Ethereum. Android was an open-source software introduced by Google; similarly, Ethereum was also an open-source platform introduced for blockchain. Developers can form applications with the infrastructure provided by the Ethereum platform. Ethereum and its developers are developing and maintaining their infrastructure. The Ethereum has a list of key features: (1) incorruptibility: no third party can change the data; (2) security: avoids errors caused by personal factors since entities maintain decentralized applications instead of individuals; (3) permanence: even a private laptop or server failure cannot affect the properties of the blockchain. In the early 1990s, Nick Szabo initially proposed smart contracts. A smart contract that allows computers to perform a group of transactions was demonstrated by him. As blockchain became well liked, more and more attention is received by smart contracts. The key feature of the blockchain-based platform Ethereum includes smart contracts which were introduced into the technological world in 2015. A smart contract can be defined as "a digital contract written in ASCII text file and executed by a computer, incorporating the underlying engine, blockchain's anti-forgery mechanism" [2]. Smart contracts can be deployed by employing the Ethereum platform. Developers can specify any instructions in the smart contract if needed; develop numerous types of applications, as well as one contract can interact with another contract; data saving; and ether transactions. In addition to preventing contract meddling, they are present at all nodes of the network. With the relevant tasks performed by machines and services provided by Ethereum, the manual blunder could be minimized to overcome quarrels over these contracts. In the electoral system [3] smart contracts are principally employed.

During the academic career, students achieve enormous educational accomplishments or satisfy particular requirements which are documented and it plays a character in evaluating the skills, ability, personality, etc., of the individual who owns it.

In the existing digital world, everything is stored in a digital format. Today, all graduation badges and credits contain data that can be simply forged lawlessly. Therefore, there exists a great want for an accurate methodology that will ensure the originality of information in these certificates, which suggests or confirms that the document comes from a trusted and licensed source and that it has not been tampered with. Numerous methods have been formulated to safeguard the electronic certificates of educational centers and accumulate their confidentiality. Similarly, the land certificate possession system in the Asian nation continues to be registered involving human intervention. The system has boundaries and ambiguity which will be explored by idle entities. Some limitations are the physical certificate can be lost. To resolve that, a land and asset certificate possession registering tool can be constructed using Hyperledger Fabric blockchain technology [4]. Blockchain was a key tool for safeguarding information, and when merged with different hashing algorithms, it was a robust methodology for securing information. This methodology aims to cut back on the issues that arise within the manual system. Blockchain technology is employed to scale back the rate of faux certificates and make sure that the safety, validity, and authenticity of educational certificates would be enhanced. In recent days, information technology has developed like a storm, so the need for data protection is increased. Graduates, during the continuation of their studies or while looking for work, need different certifications to interview. However, they often realize that they have lost their academic credentials and honors. Applying for a reissue of a hard copy will be long as a result of certificates square measure provided by completely different organizations and offline application is also necessary. On the other hand, requesting a soft copy or digital or electronic certificate saves time and individual efforts. By giving details for identity authentication, graduates can easily claim any certificate. However, owing to this convenience, fake diplomas, licenses, and certificates are in vogue. As a result, educational institutions and companies were not able to immediately authenticate the received documents. To solve this drawback, a blockchain-based certificate authentication methodology was formulated. The data is placed in various nodes, and if someone wants to alter a certain piece of internal data requires other nodes to alter it at the same time. Therefore, the system has extreme reliability.

2 Existing System

The academic certificate proves that the possessor has achieved certain educational qualifications or consummated certain requirements. These certificates or documents are utilized in three separate processes including issuance, sharing, and authentication [5]. It was a headache for the students and academic management to store these documents either in traditional paper format or digital format. And at the same time, it was a difficult and time-consuming process for employers during employee certificate verification tasks. Several articles recently highlighted the cases of university faux diploma certificates in 2020 in many countries [6]. The

research presents that more than 30% of degrees are lawlessly attained [7]. Nowadays, some universities pay over two million greenbacks a year for reviewing validation requests [8].

In certificate authentication method using Quick Response code [9], the paper certificates are protected using encryption algorithm but it can be easily decrypted, and on Unique Smart card verification method [10], students are provided with a smart card of the magnetic strip which contains the student details and certificate parameter and a Unique Identification number which will be encrypted using Blowfish algorithm before transmission. The above-discussed authentication methods using Quick Response code or Unique Smart Card for authentication of academic certificates do not ensure security. Since they can be easily manipulated, they are not reliable. Our work focuses on resolving these drawbacks in certification validation system.

3 Objective

The prime intention of this proposed system is to overcome the forgery certificate issues in the education sector by enabling the emerging blockchain technology, which ensures un-changingness and openly confirmable records, these attributes of blockchain are employed to produce the digital certificate that is anti-pirated and straightforward to authenticate. The encrypted data is obtained from digital certificate using hashing algorithm. The Merkle tree is formed and subsequent Merkle root is calculated until a single Merkle root is obtained. Then the single Merkle root data is stored in a blockchain and can be retrieved when needed. During verification stage, once again Merkle root will be generated and compared with the retrieved Merkle root from blockchain. If they are not equal, then we can confirm the integrity of certificate is compromised. In the end, academic documents like university certificates and transcripts can be more secure, reliable, and deliverable. This enhances the transparency and prevents any user from faking his qualification.

4 Related Work

Tuti et al. [11] implemented an innovative blockchain-based effective solution for validating certificates in educational systems utilizing the unique benefits of blockchain, a decentralized encryption system. The various results of previously executed research are focused through the library study method.

Namasu et al. [12] proposed a privacy-preserving technique for creating and maintaining health records that also provides an interface between the user and the nearby health centers. Medical certificates are used to take advantage of financial benefits such as tax, insurance claims, and litigation. The advantage of the proposed scheme is to ensure confidentiality by setting rules in smart contracts.

Garba et al. [13] implemented a sinewy and extensible domain authentication methodology that records a group of devoted Certificate Authority each related to the particular entity at the network in the blockchain. So, every Certificate Authority initially validates if it is devoted to executing the actual issuance process. The advantage of this method is it would need lesser storage space and lesser bandwidth to authorize certificates than various systems. The disadvantage is it needs to download the entire block header every time and Power of Work (PoW) requires high energy consumption.

Gayathri et al. [14] developed a document verification system using a chaotic algorithm that generates a numeric representation for the certificate. But the main disadvantage is the majority of chaotic encryption algorithms will be employing floating calculations which results in inefficient and complex implementation compared to the traditional ciphers [15].

Wang et al. [16] designed a system to prevent signing fraudulent certificates. Here, the Certificate Authority validated certificates and their updated annulment information of a web server are processed in blockchain, and verifier accepts only published and not revoked. This paper provides various countermeasures for compromised public key pairs which serve as an advantage for this system. The disadvantages of this system are it requires larger storage, has more validation delay, and leads to higher incentive cost.

Bahrami et al. [17] proposed a devoted and tinker-proof certificate authentication system that enhances the confidentiality and heftiness features of the system by eliminating problems caused by a single entity and so the dependence on any single party is reduced. It leveraged permissioned blockchain-based, sealed smart contracts for the authentication process. The advantage is it provided transparency. The disadvantage is permissioned blockchain has a high risk of collusion and overriding of consensus.

Afrianto et al. [18] developed a secured document storage system for job training institutes based on the open-source blockchain platform employing smart contracts to generate data. The InterPlanetary File System (IPFS) can be utilized to save documents in an Ethereum infrastructure. The advantage here is Metamask is used to store data which enhances security. The disadvantages are IPFS consumes a lot of bandwidth which is not appreciated by the metered internet user. IPFS employs transport encryption instead of content encryption. IPFS makes sure that the data sent from one node to another is confidential. But, anyone in the system can download and view that data if they have CID.

Budiono and Karopoulos et al. [19], designed a Covid-19 result certificate handling system which is an open and non-permissioned blockchain that is executed via Ethereum Virtual Machine. This can be done since blockchain employs a decentralized network to save its information with a confidential and common agreement mechanism [20]. But it is a costly affair and offers limited block size.

5 Proposed Method

In this proposed system at first, the hardcopy certificate data are digitalized and uploaded into the system by the issuer. The issuer can also upload multiple numbers of certificates. A hash code is generated for all the quarters of the certificate using the SHA3-512 algorithm which will produce a 128 characters length hash value and then the Merkle tree is formed using those hash values. In comparison with similar data structures, the Merkle trees take up only a little disc space and can be used to confirm the integrity of data efficiently. The root of the Merkle tree was added to the append-only blockchain network as a new block and a digital certificate will be issued to the qualifier or owner by the issuer Institution or University. When the verifier initiates the verification step, the system checks if the digital certificate matches the data present on the blockchain network and returns the appropriate output to the verifier. Figure 2 represents the execution flow of our methodology over the period of time.

Types of modules:

Issuer: Data digitalization
Algorithm: Hash Code Creation, Merkle Tree Formation, Block Creation
Verifier: Digital Certificate Authentication

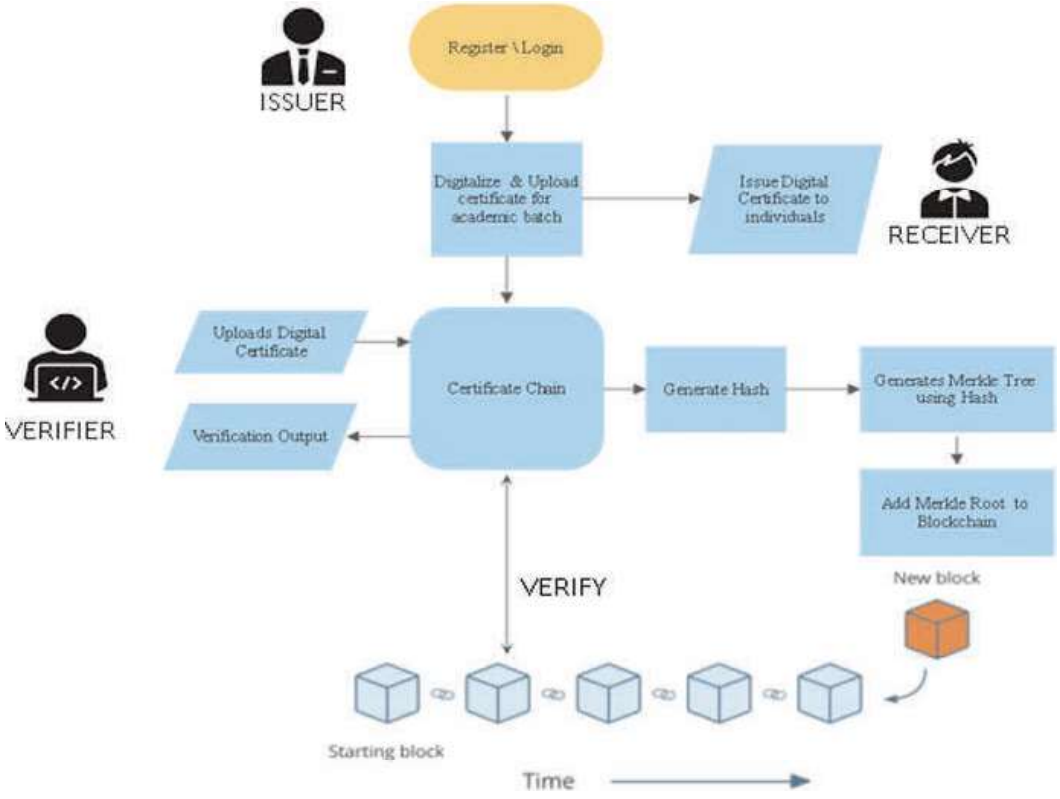

Fig. 2 Flowchart of certificate generation and authentication

Considering that many previous papers achieved similar or lower transition speed and security, we have ensured the drawbacks are overcome with this reliable prototype. Web Portal can validate certificates rapidly. Our developed Android application can run on offline mode also.

6 Method of Implementation

6.1 Data Digitalization

Here the academic certificates are initially digitalized by converting them into digital or electronic certificates. The academic certificates issued by the institution or issuer are digitalized for every individual qualifying. In this module, the institution or issuer will upload the academic certificates like 10th marksheet, 12th mark sheet, university certificates, public certificates, sports certificates, and so on. These records need to be verified by the respective sector before uploading to the interface because blockchain was immutable. Academic certificates for an entire academic year batch can be stored in a database or they can be uploaded to the system directly. After getting digitalized, certificates for individuals will be issued.

6.2 Hash Code Creation

Hash algorithms convert a digital message into a brief message digest for applications such as digital signatures. Any amendment within the original message results in an amendment to the digest, making it easier for you to detect intentional or unintentional changes to the original one. The SHA3-512 algorithm was employed to produce the numeric value of the academic record. SHA3-512 comes under the scope of the SHA-3 cryptographic hash family. SHA3 is considered more secure than SHA-2 for the same hash length. SHA3-512 provides more cryptographic strength than SHA-256 for the same hash length. SHA3-512 hash algorithm was compared with SHA1, Message Direct (MD5), Rijndael algorithm, and so on. And based on the evaluation SHA3-512 has more security than other traditional hashing algorithms and has a hash length of 128 characters.

6.3 Merkle Tree Formation

Merkle tree was a simple data structure that ensures proper mapping of huger data blocks as a connected tree or linked list. In Bitcoin and other cryptocurrencies, Merkle trees are used to encrypt blockchain data more productively and

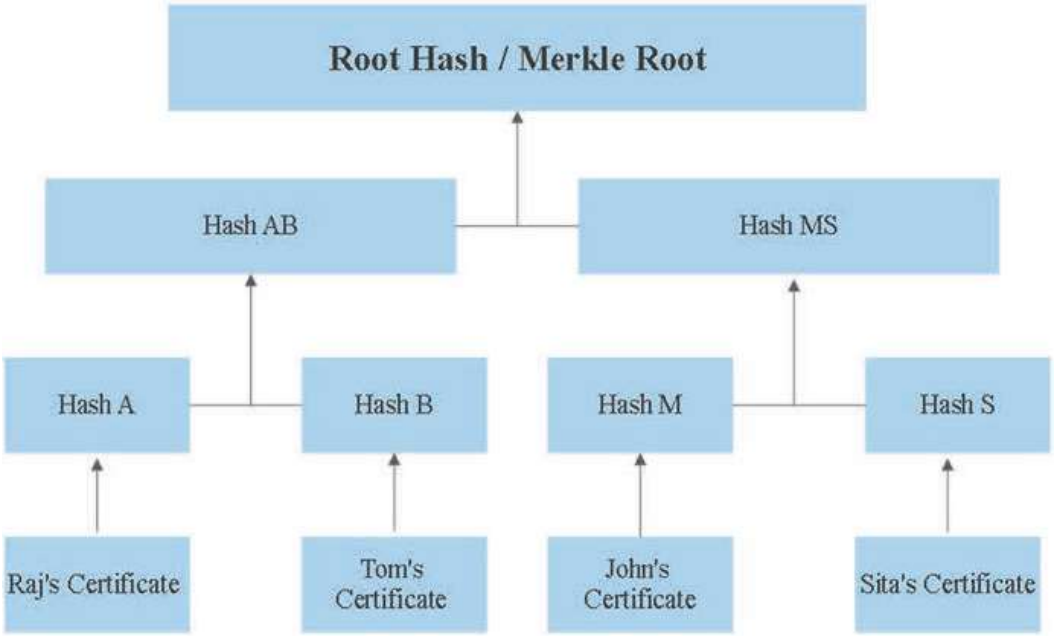

Fig. 3 Merkle tree formation

confidentially. They can also be called "binary hash trees". By repeatedly hashing pairs of nodes until only one hash remains (this hash is called the root hash or Merkle root), Merkle tree can be produced. They are built from the down up, from hashes of single appropriate certificates. Each transaction is hashed, then every pair of transactions is merged and hashed along, and then on till there's one single hash for the complete block. (If there is an odd range of transactions, a transaction is duplicated and its hash is merged by itself.) The Merkle trees are used in distributed systems for efficient data verification because it enables validation of a particular transaction without having the entire full blockchain. The root of the Merkle tree will be added to the Ethereum blockchain network. A smart contract is written to generate and validate the digital certificate instantly by comparing the value of the root hash, this contract is then deployed using Ganache, Ethereum local blockchain. Figure 3 provides an example of extracting Merkle root with the help of encrypted hash from four certificates.

6.4 Block Creation

Here every certificate will be created as a block. The data structure of the block acts as a container. For all blocks, a hash code will generate and get interconnected securely. During block creation, the count can be increased as per our requirements. The prime advantage of this unit is users are allowed to share the hash code with someone if needed.

6.5 Digital Certificate Authentication

The digital certificate will be submitted by the owner to verifier for pursuing higher education or for employment hunt. If there is an art of fraud done by modifying data in this digital certificate by the owner it will also change the Merkle root. The system checks if the root hash value of the Digital certificate matches the data present on the blockchain using smart contracts and triggers appropriate output to the verifier. We have also implemented the verification for the validity of the certificate.

7 Comparison and Evaluation Metrics

To compare the code complexity of SHA3_512 Merkle tree and MD5 Chaotic Algorithm, we use metric analyzer. Figure 4 is the Method Metrics Graph of SHA3_512 Merkle tree.

Figure 5 is the Method Metrics Graph of MD5 Chaotic Algorithm.

Cogc is the Cognitive Complexity
ev(G) is the Essential Cyclometric Complexity
iv(G) is the Module Design Complexity Metric
v(G) is the Cyclometric Complexity

Table 1 provides a comparison of system performance of SHA3_512 Merkle tree with MD5 Chaotic Algorithm.

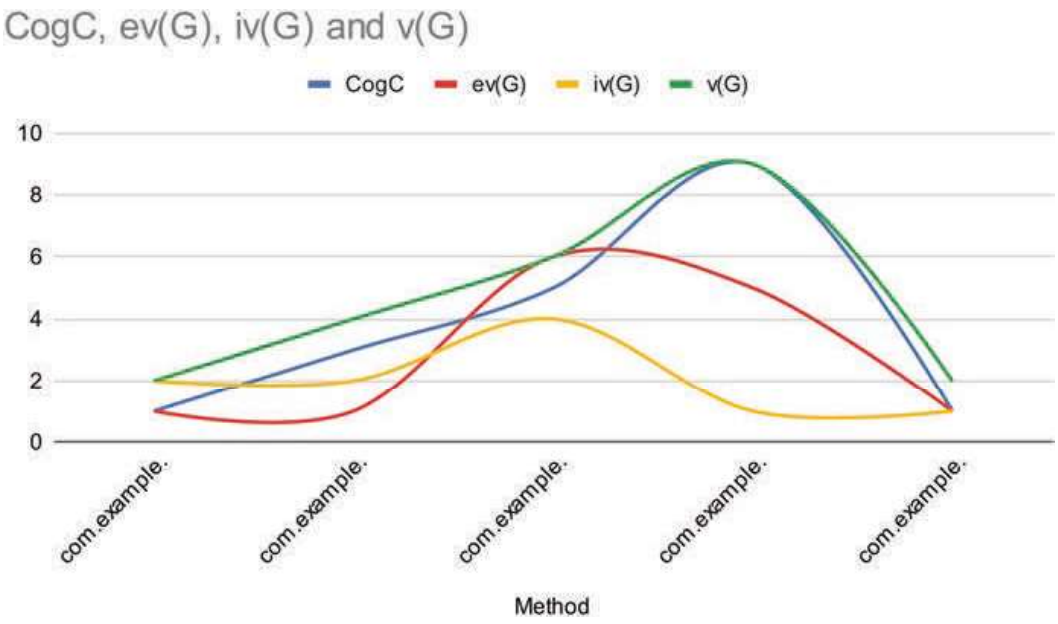

Fig. 4 Method metric plot for SHA3 512 Merkle tree

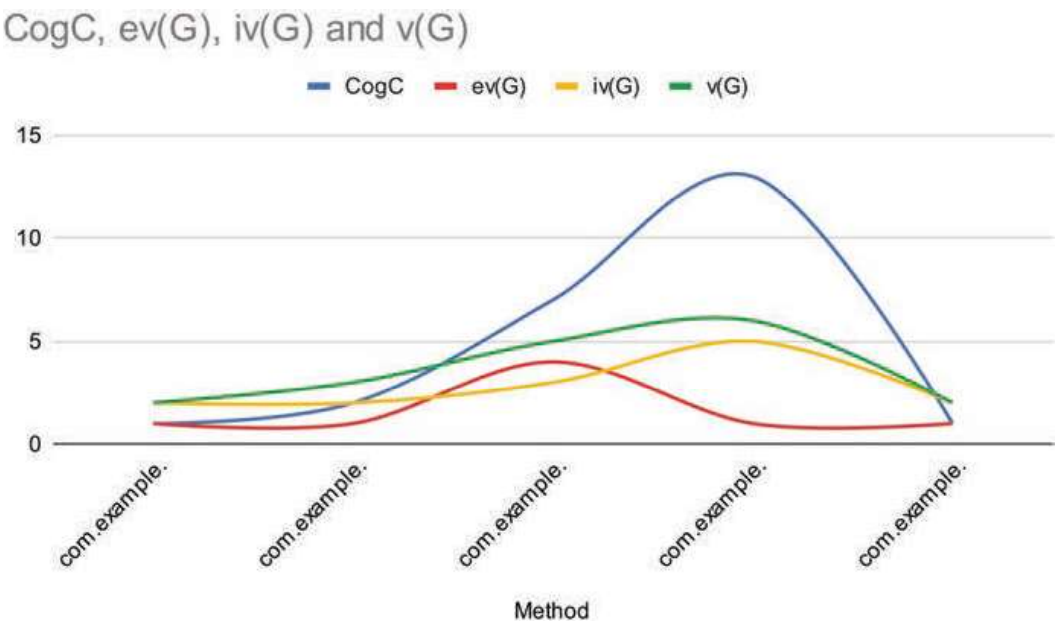

Fig. 5 Method metric plot for MD5 Chaotic Algorithm

Table 1 SHA3_512 Merkle tree vs MD5 Chaotic Algorithm

	SHA3_512 Merkle tree	MD5 Chaotic Algorithm
CPU usage	Initial: 31% Average: 6%	Initial: 36% Average: 9%
RAM usage	Initial: 124 MB Average: 75.1 MB	Initial: 131 MB Average: 81.1 MB
Gradle build	15 s	19 s
Checksum time	34 ms	77 ms

8 Conclusion

Certificates are a chunk of paper that's regularly issued in an elite way by a scholarly institution to graduates. Once the student moves to another institution or employment, certificate verification becomes difficult. It is possible to forge digital or paper certificates in ways that are difficult for users to detect. The importance of blockchain technology in the education sector is not distinctive from what has been done within the commercial sector. The espousal of blockchain in the world of education shall be employed for considerable improvements in the education sector.

In this work, we offered a blockchain-based innovative solution to the certificate fraudulence problem. Data security is achieved by employing the immutability parameter of blockchain. The proposed methodology makes use of distributed processing to make it nearly hard for sensitive information to be reformed or feigned. This prevents the probability of fraud or forgery acts and can enhance privacy and security through smart contracts. The smart contract authenticates the academic

certificate document with the help of hash identity generated. The developed application allows us to generate and validate the certificate in a secured and user-friendly manner.

References

1. He, B. (2017). *An empirical study of online shopping using blockchain technology*. Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C.
2. Lin, X. (2017). *Semi-centralized blockchain smart contracts: Centralized verification and smart computing under chains in the Ethereum blockchain*. Department of Information Engineering, National Taiwan University, Taiwan, R.O.C.
3. Shi, Y. (2017). *Secure storage service of electronic ballot system based on block chain algorithm*. Department of Computer Science, Tsing Hua University, Taiwan, R.O.C.
4. Syawaludin, A. R. S., & Munir, R. (2021). Registration of land and building certificate ownership using blockchain technology. In *2021 International Conference on ICT for Smart Society (ICISS)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICISS53185.2021.9533191
5. Grech, A., & Camilleri, A. F. (2017). *Blockchain in education*. Publications Office of the European Union.
6. Palma, L. M., Vigil, M. A. G., Pereira, F. L., & Martina, J. E. (2019). Blockcahin and smart contracts for higher education registry in Brazil. *International Journal of Network Management, 29*, 1–21.
7. Attewell, P., & Domina, T. (2011). Educational imposters and fake degrees. *Research in Social Stratification and Mobility, 29*(1), 57–69.
8. Bajwa, N. K. (2018). *Modelling and simulation of blockchain based education system* [Ph.D. dissertation]. Concordia University.
9. Mayowa, O., & Jinmisayo, A. (2021). Design and implementation of a certificate verification system using quick response (QR) code. *LAUTECH Journal of Computing and Informatics (LAUJCI), 2*(1), 35–40. ISSN: 2714-4194.
10. Lingampalli, J. R., & Namdeo, V. (2021). Unique smart card verification system for validating university degree certificates. In *2021 5th International Conference on Intelligent Computing and Control Systems (ICI-CCS)* (pp. 1574–1578). IEEE. https://doi.org/10.1109/ICICCS51141.2021.9432360
11. Nurhaeni, T., Handayani, I., Budiarty, F., Apriani, D., & Sunarya, P. A. (2020). Adoption of upcoming blockchain revolution in higher education: It's potential in validating certificates. In *2020 Fifth International Conference on Informatics and Computing (ICIC)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICIC50835.2020.9288605
12. Namasudra, S., Sharma, P., Crespo, R. G., & Shanmuganathan, V. (2022). Blockchain-based medical certificate generation and verification for IoT-based healthcare systems. *IEEE Consumer Electronics Magazine, 12*, 83–93. https://doi.org/10.1109/MCE.2021.3140048
13. Garba, A., Chen, Z., Guan, Z., & Srivastava, G. (2021). LightLedger: A novel blockchain-based domain certificate authentication and validation scheme. *IEEE Transactions on Network Science and Engineering, 8*(2), 1698–1710. https://doi.org/10.1109/TNSE.2021.3069128
14. Gayathiri, A., Jayachitra, J., & Matilda, S. (2020). Certificate validation using blockchain. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1–4). IEEE. https://doi.org/10.1109/IC-SSS49621.2020.9201988
15. Noura, H., Sleem, L., & Couturier, R. (2017). A revision of a new chaos-based image encryption system: Weaknesses and limitations. *arXiv:1701.08371v1*, 1–7.
16. Wang, Z., Lin, J., Cai, Q., Wang, Q., Zha, D., & Jing, J. (2022). Blockchain-based certificate transparency and revocation transparency. *IEEE Transactions on Dependable and Secure Computing, 19*(1), 681–697. https://doi.org/10.1109/TDSC.2020.2983022

17. Bahrami, M., Movahedian, A., & Deldari, A. (2020). A comprehensive blockchain-based solution for academic certificates management using smart contracts. In *2020 10th International Conference on Computer and Knowledge Engineering (ICCKE)* (pp. 573–578). IEEE. https://doi.org/10.1109/ICCKE50421.2020.9303656
18. Afrianto, I., & Heryanto, Y. (2020). Design and implementation of work training certificate verification based on public blockchain platform. In *2020 Fifth International Conference on Informatics and Computing (ICIC)* (pp. 1–8). IEEE. https://doi.org/10.1109/ICIC50835.2020.9288610
19. Budiono, R., & Candra, M. C. Z. (2021). Managing COVID-19 test certificates using blockchain platform. In *2021 International Conference on Data and Software Engineering (ICoDSE)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICoDSE53690.2021.9648482
20. Karopoulos, G., Hernandez-Ramos, J. L., Kouliaridis, V., & Kambourakis, G. (2021). A survey on digital certificates approaches for the COVID-19 pandemic. *IEEE Access, 9*, 138003–138025. https://doi.org/10.1109/ACCESS.2021.3117781