EasyChair Preprint

№ 12528

Blockchain-Based Educational Certification Systems Using a Modified Hash Algorithm

Alaa Abid Ali and Mohamed Mabrouk

March 18, 2024

Blockchain-based Educational Certification Systems Using A Modified Hash Algorithm

Alaa Abid Muslam Abid Ali [1,2] [0000-0002-7107-2365] and Mohamed Mabrouk [1,3] [0000-0003-0584-5988]

[1] University of Monastir, Research Laboratory in Algebra, Numbers Theory and Intelligent System,Tunisia,

[2] Al-Qadisiyah University, Al-Qadisiyah, Iraq,

[3] Military Academy, Fondok Jedid, Tunisia
alaa.abidmuslam@qu.edu.iq ,mohamed.mabrouk@ipeim.u-monastir.tn

Abstract. Blockchain is a crucial digital technology in information technology (IT) and other fields. The use of blockchain is growing because it uses encrypted and distributed databases related to transactions, making it difficult to modify, hack, or check. The education sector uses both on-site and online systems. The use of blockchain technology in education is still in its early stages of development. In this study, we propose secure certification system for educational applications has been presents that based on blockchain technology, which safely sends data over an untrusted network by encrypting the authorization and certification information using blockchain and modifying the Secure Hash Alogrithm3 (SHA3) . The potential benefits of blockchain technology in education certification include improved efficiency, security, and transparency of the educational system. The proposed system uses the back-end and PostgreSQL to save process information for institutes so that it can manage process information for students. For the front-end, we use React, type, tailwind, and web3, and build pages and connecting logics. This certification will be added to the student's wallet address in such a way that only certified students can see their certification and, if needed, check it by third. The results show that the proposed certification model that utilizes blockchain achieves a high level of security in all tests used.

.

Keywords: Blockchain, Cryptographic, Certification system, Ethereum, Smart contract,SHA3

1 Introduction

Blockchain is the foundational technology that supports and enables the functioning of cryptocurrencies. In addition to its financial applications, the potential of blockchain technology has become prominent in several sectors such as trade and supply chains, the creative sector, and the public and third sectors[1][2]. Blockchain technology uses a database that is immune to tampering and includes timestamps. It enables many entities, such as individuals, companies, and public bodies to confirm transactions and update information in a manner that is synchronized, transparent, and decentralized[3].

Rather than depending on intermediaries or third parties, trust among parties is established by adherence to rules or consensus processes employed to verify, validate, and incorporate transactions into a blockchain[4].

In the education field, blockchain is an interesting new field of technology that could make a big difference, which has several applications in education, from keeping track of data to making sure it is correct without losing its authenticity[5]. It has emerged as an important advancement in the field of education, providing new opportunities to resolve long-standing issues and enhance various aspects of the educational system[6]. The blockchain data can be viewed and checked 24 hours a day, seven days a week. Blockchain technology is mostly used to issue and verify educational certificates, such as degrees, transcripts, and students' skills, achievements, and professional abilities, which can be checked by any company in the world[7]. Blockchain technology speeds up the certification process, and it takes the company less time to check students' grades. This helps the education business by providing them with a safe way to share information about their students. This builds trust, cuts costs, and makes things more open. The blockchain system maintains a full record of events in data blocks ordered by time stamps. The old and new data blocks cannot be deleted, whereas the encryption system keeps data from being changed and fraudulent [8].

Blockchain creates a virtual infrastructure for storing documents and tracks students' credentials and achievements. This can benefit education by reducing administrative costs and bureaucracy[9][10]. In many sectors, scalability, privacy, and dependability problems cannot be solved without the blockchain technology. Blockchain technology is useful for education because it is safe, allows control of access to data, is cheap, verifies identity, makes data management easier, allows for more interaction and system interoperability, improves student assessments and career decisions, and makes things more open and accountable[11]. The use of blockchain technology in education has no limitations in a single domain but encompasses multiple scenarios, each with its own advantages and implications. In this paper, we propose a university certification system based on the blockchain technology in such a way that certification is transferred to security while providing reliability so that the certification is directly traceable to the issuing party. This work provides a blockchain-supported method that enhances the confidentiality and integrity of student and institute data. To improve the Blockchain encryption our proposed university certification system uses a modified SHA3 algorithm[12], in which an SHA3_256 is integrated with chaotic algorithm to generate a new hash value.

2 Related works

To address the issue of education transaction object authentication across institutions, Ali et al. (2022)[11] developed a blockchain-based framework for storing and sharing graduate certifications. The system was developed by using a private hyperledger blockchain. The system utilizes smart contracts in addition to hashing to secure and regulate certification deployment. Compared to the traditional methods of issuing and verifying certifications, the proposed system has a significantly higher throughput of

issued and verified certifications. E-certification is issued and validated within one minute, whereas the traditional process takes between one week and ten days. In addition, the suggested model can regulate data exchange, thereby protecting client confidentiality. Reza et al. (2022) [13], suggested and implemented a framework for the electronic exchange and approval of student certifications upon graduation. The proposed system allows for controlled sharing of students' information and maintains the confidentiality of the information via a private blockchain. The blocks are added to the blockchain network once data addition and hashing are performed. This model improves document security and reduces fraud risk. It also significantly reduces the identification time by a large amount, almost doubling the current speed. Maestre et al (2022)[14], suggests a Blockchain-based model for implementing certification and degree issues in open higher education. This model verifies that students trained in school have learned the skills they have claimed. The solution has been tested and found to be effective, and the system has become operational. Rani et al (2023) [15], suggests implementing decentralized certificate administration systems in higher education using blockchain technology. Data encryption, keywords, and digital signatures are saved using cryptographic techniques like SHA-256 and the Elliptic Curve Digital Signature Method (ECDSA). This system facilitates the storage and retrieval of educational certificates for students. College students are authorized to share the hash value of their certificates with entities in order to enable verification of the certificates using the blockchain. The proposed technique was implemented utilizing Ethereum with the programming language Solidity. This approach offers a platform for firms to verify the educational credentials of potential employees. Rahman et al. (2023)[16], presented a certificate authentication solution that utilizes blockchain technology. The administrator has the ability to generate, authenticate, and make corrections to the certificate if deemed necessary. In addition, the administrator can ascertain the number of times a certificate has undergone modifications. The verification of certificates can only be conducted by other users. Two blockchains were used to facilitate the implementation of adjustments. The successful implementation of a certificate authentication system can be achieved through the use of blockchain technology. The suggested approach is anticipated to offer numerous benefits, including facilitating a user-friendly university entrance process and streamlining job hiring procedures.

3 Methodology

The proposed e-certification system architecture was divided into three layers:

- Front-end Security and User Interaction layer: The primary objective of this layer is to provide communication between the students, enabling them to cast their certification, and the administrator, allowing them to carry out tasks related to the administration of the certification process. The system encompasses two primary tasks: authentication and authorization, which serve to verify and grant access to valid users (both students and administrators) in adherence to pre-established access control criteria.
- Access Control layer: The purpose of this layer is to support the operations of layers 1 and 3 by offering the necessary services that enable these levels to fulfill

their intended functionalities. These services encompass the definition of roles, establishment of their corresponding access control policies, and specification of certification transaction specifications.

- Transaction layer: The core layer of the architecture is responsible for mapping transactions from the Role Transactions/Management layer onto the blockchain transaction that will be mined in the context of e-certification. The mapped transaction includes authentication credentials given by a student in layer 1. The ledger Synchronization layer synchronizes.

A multi-chain ledger is implemented in conjunction with a locally deployed application-specific database utilizing a pre-existing database technology. The act of casting certifications results in the recording of data in the back-end data tables of the database. Once students' ballots are successfully recorded and incorporated into the blockchain ledger, they are granted the capability to monitor their certification activities by utilizing their individualized identity assigned to them. The security implications pertaining to the certification process are predicated on the utilization of blockchain technology, which employs cryptographic hashes to fortify the integrity and confidentiality of end-to-end communication. The certification results are additionally recorded in the application's database to streamline the auditing process and enable subsequent operations in the future.

3.1 Certification System Phases

Certification systems can be divided into three phases: authentication, certification and counting. In the Authentication phase any users or administrator have a wallet value that was registered in the system database. In order to enter university pages, the user should enter his wallet hash value that will be compared by university server using blockchain strategy and if the user is registered then he can pass to the university pages. Table (1) illustrates the samples of users and administrator's wallet hash values in databases. In addition, each user or administrator has the gas value that can be used as a payment strategy for some requirement such as request certification from university.

Table 1. An illustration of database.

Name	Wallet hash value	Photo	Gas value
Institute	0x61207ECa7F1C578584566c042CD15 fc21801C307	File 1	0.923 BNB
Student 1	0x5d55Bf884151B145274eF96584842 5B995eA0567	File 2	0.0196 BNB
Student 2	0x57EFbd008AB5491C3abb5C8E5F290 F1a395577b1	File 3	0.0981 BNB
Student N	0x7857e2f0Ac58D7D820eb13CbBa0Da 7D67D299013	File N	0.0981 BNB

3.2 Modified SHA3 Algorithm

For blockchain, two common hash algorithms can be used such as SHA2 type (SHA256) or Keccak (SHA3) which are one of the best encryption methods because of the high sensitivity of its initial condition. However even that those types of hashing

algorithms are very strong and hard to cracked or guess the original values, theory is still a side of risk that an attacker can find a solution to crack it. Thus, to find a new method that can modify the original hash value is one of our strategies to improve security. Hence, we intend to integrate chaotic algorithms with hash algorithm to generate a new hash value. There are several types of chaotic maps. One of the most common and powerful types is the logistic map, which is a two dimensional (2D) chaotic map. Different types of feasible logistic maps have been proposed. But to choose one, it should have three properties, such as- Large Parameter, Robust Chaos, and Mixing Property. By analyzing all the properties, we are going to use traditional logistic maps. This chaotic key is used for encryption and decryption and has a size of 256 bits. The key can yield an integer sequence, which we then combine with the SHA3 hash value. The combination is accomplished by translating the SHA3 hash to hexadecimal Base16 then summarizing it with the chaotic key to form a new value, which is then converted to hex. The combination password algorithm scheme employs the following steps:

Modified SHA3 Algorithm :-
Input: Message=Hashed (By SHA3+Salt)
Output:Modified Hash
Begin
Step 1: Read Message M as bytes.
Step 2: Rotate the message 5 times to right.
Step 3: Apply XORing between Shifted Ms and K and get MS.
Step4: using keccak function to compute the final hash:
NH=keccak (MS, 1600, 1600-2*n, n, K).
Step 5: Save hash NH.
End

Where, NH is new hash value, MS is shifted message, K is they key value, and n number of rounds.

3.3 Modeling the User Interface for Certification System

The model is online certificate validation that is based on blockchain, which can handle everything needed to do with certificates, including storing, validating, and sharing them. It is based on the principle that "only the issuer is able to upload the certificate, while everyone else can only view it. The whole process is run on the blockchain in collaboration with the Interplanetary File System (IPFS) which is to provide data security. Ethereum is used to build models and on local blockchain and then deployed on test network Figure 1 The educational certification system-based blockchain technology.

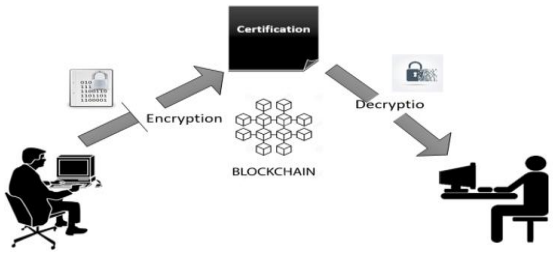

Figure 1. The educational certification system-based blockchain technology.

The Model operation is follows.

1- Student Authentication:

- Permission is needed connect to his wallet with (Application).
- Students need to connect their account with their Institute by giving Institute Address Key
- Students need to connect their account with Institute.

2- Institute Authentication:

- Permission is needed to connect to university wallet with (Application).
- The issuer can add a student by adding his wallet address.
- The issuer can add certification of student that includes the study material and the degree achieved through his study years.

In case student need to share his certification to the third party (such as institute, companies, organization to certificates) to verify. The students need first to login to his account through authentication and using his university wallet hash value, if it verified then he can give access to any other one to investigate his/her certification. However, for security the institute side give access is limited time (such as 1 day).

After building smart contracts we have to deploy to blockchain network using Hardhat. In this project there are two roles (Institute and student), so access control and ownable have to use. In addition, a declare about document struct is made to save certification. In certification part, it can save name, photo, id, detail, processes and date. In smart contract, we can't use many parameters because it will increase gas fees. So, we use two structures of data.

For encoding, we utilized Keccak256 function[17] [18]in order to returns encode string to 256byte of string. For certification generation, the function is generating certification for student address with 4 types of function: private, public, internal, external.

- **Private:** can use only on this contract
- **Internal:** can use only on contract
- **External:** can use only outside (can call out contract)
- **Public:** it combined both Internal and External, where public function is required more gas than internal or external.

In addition, there are two rules one for student and one for institute. This function is similar with if operator. If condition is true, compiler goes, and if it is false, this function is closed with error message. Message sender: this is the wallet address that calls this function. Figure 2 show the proposed model structure.

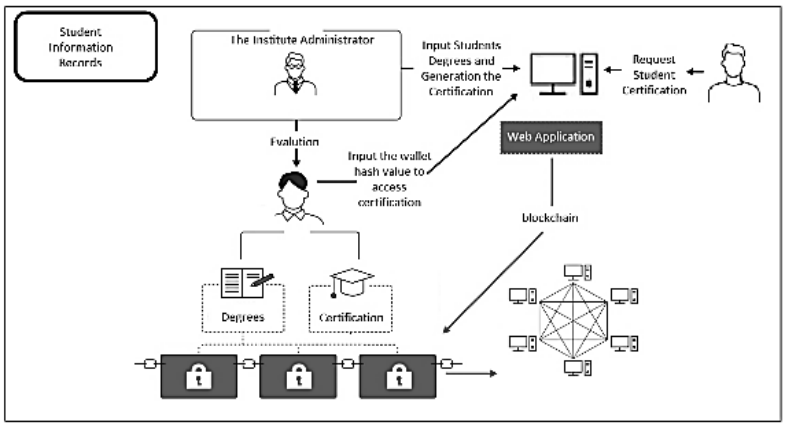

Figure 2: The proposed model structure.

4 Experimental Results and Discussion

This part is used to investigate the security strength of the proposed model using several analysis strategies. The first part is to investigate the process of modified hashing of blockchain. The second part is to investigate the real time certification process by developed a user interface system that is website that have two side one for institute and second for student in which student can access to his account and view his certification and can share his certification to third party (such as company request his certification). Finally, several security tests to evaluate the strength of the proposed mode.

4.1 Modify Hashing using SHA3_256

In this stage the plaintext message is encrypt using slandered SHA3_256 hashing algorithm. Then it will generate a chaos key set that based upon chaotic logistic map equation from [18]. In this part, chaos key set generation was test by using various control parameters population (x) and biotic potential (r). Hence, the keys change depending on the control parameter. These parameters interact with one another. After using several control parameters, size has a strong influence on key size, therefore it is beneficial to be in the range of 90 toward 100, r and x should both be increased, and it is beneficial to be in the range of 0.7 to 1. Table Modified Hash Value for Password After Combined Chaos Key with Hash-Salt Value.

Table 2. Modified Hash Value for Password After Combined Chaos Key with Hash-Salt alue.

Cho. Key	Password Hash Value without chaos key	Password Hash Value with chaos key	Time (msec)
K1	40bcb9772ab072c90d 0dbfddef499e12af769 349267a725f8f3b1de5 2768cdb0	da8eeffd110b55fdd08 abe6e95abcb5663fa1c 4b73d78af6ddb9279f2 7aa97c9	1.2434
	406cb9772ab072c90d	d134ee47bd974528dd	1.2417

K4	0dbfddef499e12af769 34926ca726f8f3b1de5 2768cdb0	d668414e8e22cf73b35 d90838f27d1f1f02cd8 608a5d66	
K7	40bcb9772ab072c90d 0dbfddef499e12af769 34926ca425f8f3b1de5 2768cdb0	c2e1e341f693eaa1763 d686c4726814fb23794 0e5ee15a6f83c4ce9a5 ad16031	1.2421
K10	40bcb9772ab072c90d 0dbfddef439e12af769 34926ca725f8f3b1de5 2768cdb0	6b70bf33d31b28ed4f5 a7b0a3f89wf07468bc3 6a689c07893e9bd29a9 6819ffc	1.2425
K11	40bcb9772ab072c90d 0dbfddef499e12af769 34921ca725f8f3b1de5 2768cdb0	9d1bd1e1b9954a2532 0d0f513a607g9d36f30 ad6e05f4b2c221acdae 9b57daa1	1.2428

According to the data presented in Table 2, the newly generated hashed password consists of a 32-byte hexadecimal string format. It is important to note that this password changes with each iteration, occurring at a frequency of once per second. Consequently, the likelihood of an attacker or cryptanalysis program successfully guessing the specific password being utilized is significantly diminished, rendering it a challenging or potentially insurmountable task.

4.2 Blockchain Generation Test

A class named "blockchain" will be established, consisting of two distinct properties: "blocks" and "secret." The property "blocks" will serve as a repository for all the blocks contained inside the blockchain, while the variable "secret" will be utilized in the construction of the previous hash value for the initial block. In this study, we establish three distinct functions: create a block, validate the blockchain, and show the blockchain. The create block method is utilized for generating a novel block and subsequently adding it to the block property of the blockchain. The aforementioned attributes of each block are implemented in this context. The calculation of the nonce that fulfils the blockchain's prerequisite of having four leading zeros before each hash is performed. A validated blockchain function was employed to verify the integrity of the blockchain. This implies that it will verify the fingerprinting of every block within the blockchain and provide an indication of its stability. Each block inside a blockchain must possess an accurate hash value for the preceding block. In the event of any inconsistencies, it can be reasonably inferred that an individual has tampered with the blocks within the blockchain. The immutability and tamper-proof nature of blockchains are attributed to this characteristic of the technology. Ultimately, the function shows that the blockchain will be employed to exhibit all blocks contained within the blockchain.

Having successfully constructed the blockchain class, we employed it to generate our blockchain and then append a series of blocks to it. The user intends to append three blocks to the blockchain, subsequently verifying the integrity of the blockchain, and ultimately displaying the blocks and examining the resulting output. Figure (3) show the blockchain process.

Figure 3: The hash Blockchain process.

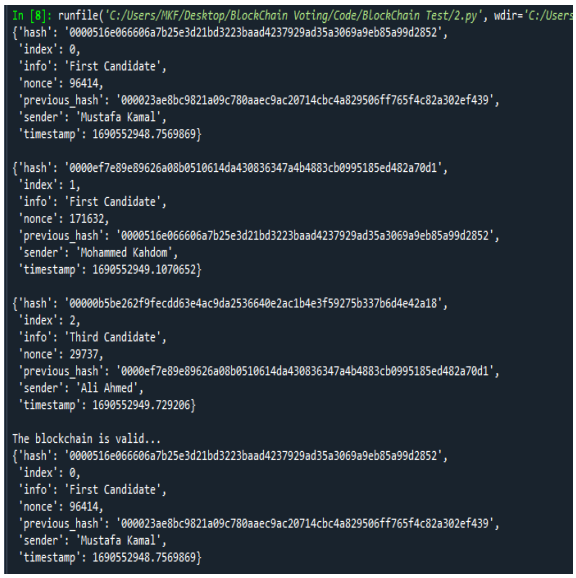

Figure 4: The Result When Modified Blockchain.

As shown in figure (3), there are blocks on the blockchain and the validated block-chain function returns true. Next, we test if the blockchain works efficiently by inserting a new block between existing blocks and running the validated blockchain function to observe the result. Figure (4) shows the results when the modified blockchain is used. The validation of the blockchain function yields a false result owing to a mismatch in the fingerprinting process, resulting in compromised integrity of the blockchain.

4.3 Security Strength Test

4.3.1 NIST tests.

Table 3 presents the outcomes of the NIST tests conducted on the proposed algo-rithm results, validating the assertion that the proposed encryption algorithms possess robust security measures and are capable of withstanding many forms of assaults. The algorithm under consideration successfully passed all tests conducted by the National Institute of Standards and Technology (NIST) as a result of the adjustments made and the specific key employed in each known experimental test. The concept of "chaos keys" refers to a theoretical framework that explores the role of chaos in various sys-tems.

Table (3). NIST Tests results for Modified SHA3

Test Type	SHA3 Result	Modified SHA3 Result
Run Test	0.675	0.689
Serial Test	0.564	0.621
random excursion variant	0.332	0.451
random excursion	0.809	0.818
non overlapping template matching test	0.586	0.603
Frequency Monobit Test	0.832	0.877

Maurer's universal statistical test	0.913	0.935
longest run of 1s within one block Test	0.642	0.671
Linear complexity	0.689	0.690
Frequency test within a Block	0.487	0.521
DFT	0.708	0.722
Cumulative sum Test	0.834	0.836

Based on the data presented in the preceding table, it can be observed that the proposed modified sequences of the SHA3 algorithms successfully met the criteria of the NIST test compared to the original SHA3 algorithm.

4.3.2 Hamming distance Results.

The Hamming distance for every proposed SHA3 test using the generated chaotic keys differed in total bits. Table (4) shows the Hamming distances. The results demonstrate that the proposed SHA3's hamming distance is secure and resistant to statistical attacks.

Table 4. Hamming distance Test Results for Encrypted Data

Text Size in(byte)	SHA-3	**Modified SHA3 result**
128	48	40
256	101	95
512	289	275
1024	521	495
2048	**1010**	**980**

4.3.3 Data Quality Test.

Multiple objective tests may be employed to assess the similarity of the created hashes, and these tests can also be utilized to identify dissimilarities among them. The quality of the hash is assessed by testing the encrypted password/block against the original password/block, with the aim of identifying any discrepancies and ensuring the integrity of the hash. The Mean Square Error (MSE) represents the discrepancy between the original and encrypted password/block, with a higher number denoted. Another test relies on the Mean Squared Error (MSE) metric, which is commonly employed to evaluate the signal-to-noise ratio (SNR) and the Peak SNR. These two tests were performed by minimizing the values. The final test, the Structural Similarity Index (SSIM), was utilized to determine the internal correlation between blockchain hash values and password hash values. Additionally, an entropy test was conducted on the encrypted password or block, and it was observed that the values of all hashes were close to the maximum with all input passwords or blocks. Table 5 provides a detailed explanation of these tests.

Table 5. Quality Test for Encrypted Data.

MSE	**PSNR**	**SNR**	**Entropy**
890.97	0.00321	1.977	3.675
920.85	0.00642	1.311	3.744
897.57	0.00344	1.957	3.658
911.41	0.00852	1.433	3.762
921.96	0.00976	1.343	3.791
906.89	0.00669	1.480	3.756
910.62	0.00736	1.411	3.785

4.4 Operational Test

The dataset was generated on a local server using PostgreSQL. The environmental parameters and their corresponding values are listed in Table 5. To enter a university administrator or as a student, there is a need to enter the MetaMask password and then add a wallet address. University administrators should enter the university wallet address and then pass it to university pages. In university there is an ability to add students and their certification includes the materials and degrees as shown in figure 5.

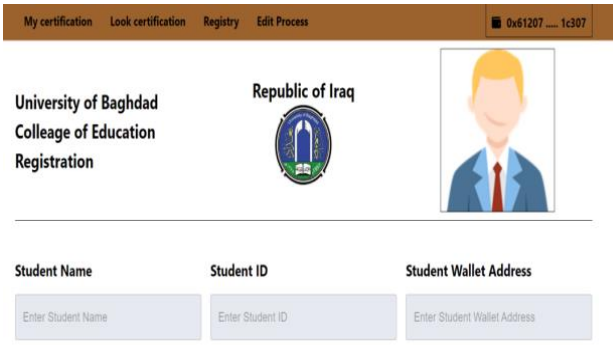

Figure 5. The university side of educational certification site.

Figure 6 . The student side of educational certification site.

For the student side, only one option is to see his certification and the second is to share his certification with another person. Figure 6 show the student page and an example of certification,

To share certification with third-party companies, the student should put the wallet hash value and pay the Binance Coin(BNB) value in order to provide access to certification, as shown in figure 7.

For company to view the student certification should follow the university link then pass the authentication process to enter certification site then add the student wallet hash value to view his certification as shown if figure 8.

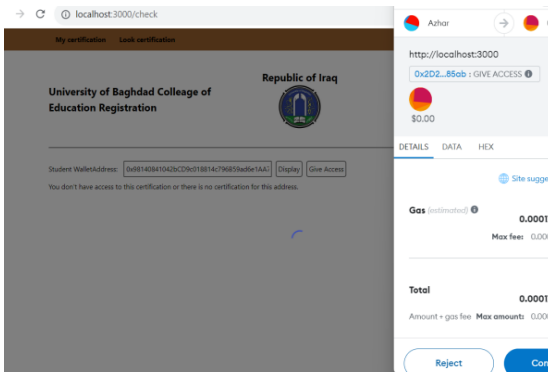

Figure 7. Adding access for company by student.

Figure 8. View student certification by company.

5 Conclusion

The credential verification procedure is important within the education system, as it serves to verify the authenticity and credibility of academic qualifications. Nevertheless, the conventional approaches employed to authenticate educational qualifications, including diplomas, degrees, and certifications, frequently encounter inefficiencies and susceptibilities, resulting in challenges, such as counterfeit credentials and protracted verification procedures. The utilization of blockchain technology presents a paradigm-shifting resolution to these issues, fundamentally altering the manner in which educational certificates are bestowed, preserved, and authenticated. The proposed model is online certificate validation based on blockchain using a modified SHA3 algorithm , which can handle everything required with certificates, including storing, validating, and sharing them. The system provides assurance to transfer certification without fear that the certificate will be forged or tampered with and also ensures speed in direct data exchange between educational institutions and entities requesting certificate authentication.

References

1. Javaid M, Haleem A, Singh R. P, Suman R, and Khan S, "A review of Blockchain Technology applications for financial services," BenchCouncil Transactions on Benchmarks, Standards and Evaluations, vol. 2, no. 3, p. 100073, Jul. 2022, doi: 10.1016/J.TBENCH.2022.100073.
2. Ali A. A. M. A, Mabrouk M, & Zrigui M. A Review: Blockchain Technology Applications in the Field of Higher Education. Journal of Hunan University Natural Sciences, 49(10), 2022.
3. Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, and Ishfaq M, "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing," Future Internet 2022, Vol. 14, Page 341, vol. 14, no. 11, p. 341, Nov. 2022, doi: 10.3390/FI14110341.
4. Tan T. M. and Saraniemi S., "Trust in blockchain-enabled exchanges: Future directions in blockchain marketing," J Acad Mark Sci, vol. 51, no. 4, pp. 914–939, Jul. 2023, doi: 10.1007/S11747-022-00889-0/TABLES/5.
5. Alammary A, Alhazmi S, Almasri M, and Gillani S., "Blockchain-Based Applications in Education: A Systematic Review," Applied Sciences 2019, Vol. 9, Page 2400, vol. 9, no. 12, p. 2400, Jun. 2019, doi: 10.3390/APP9122400.
6. Haleem A, Javaid M, Qadri M. A, and Suman R, "Understanding the role of digital technologies in education: A review," Sustainable Operations and Computers, vol. 3, pp. 275–285, Jan. 2022, doi: 10.1016/J.SUSOC.2022.05.004.
7. Alam S et al., "A Blockchain-based framework for secure Educational Credentials," 2021.
8. Chen G, Xu B, Lu M, and Chen N.-S, "Exploring blockchain technology and its potential applications for education," Smart Learning Environments 2018 5:1, vol. 5, no. 1, pp. 1–10, Jan. 2018, doi: 10.1186/S40561-017-0050-X.
9. Jirgensons M and Kapenieks J, "Blockchain and the Future of Digital Learning Credential Assessment and Management," Journal of Teacher Education for Sustainability, vol. 20, no. 1, pp. 145–156, Jun. 2018, doi: 10.2478/jtes-2018-0009.
10. Shi S, He D, Li L, Kumar N, han M. K. K, and Choo K. K. R, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," Comput Secur, vol. 97, p. 101966, Oct. 2020, doi: 10.1016/J.COSE.2020.101966.
11. Ali M. A and Bhaya W. S, "Higher Education's Certificates Model based on Blockchain Technology," in Journal of Physics: Conference Series, IOP Publishing Ltd, May 2021. doi: 10.1088/1742-6596/1879/2/022091.
12. Ali, A.A.M.A., Hazar, M.J., Mabrouk, M. and Zrigui, M., 2023. Proposal of a Modified Hash Algorithm to Increase Blockchain Security. Procedia Computer Science, 225, pp.3265-3275.

13. Reza A. W, Islam K, Muntaha S, Rahman O. B. A, Islam R, and Arefin M. S, "Education Certification and Verified Documents Sharing System by Blockchain," International Journal of Intelligent Engineering and Systems, vol. 15, no. 6, pp. 682–691, Dec. 2022, doi: 10.22266/ijies2022.1231.60.
14. Maestre R. J., Bermejo Higuera J, Gámez Gómez N, Bermejo Higuera J. R., Sicilia Montalvo J. A., and Orcos Palma L, "The application of blockchain algorithms to the management of education certificates," Evol Intell, vol. 1, pp. 1–18, Dec. 2022, doi: 10.1007/S12065-022-00812-0/FIGURES/16.
15. Rani P. S. and Priya S. B, "Trustworthy Blockchain Based Certificate Distribution for the Education System," 2022 1st International Conference on Computer, Power and Communications, ICCPC 2022 - Proceedings, pp. 393–397, 2022, doi: 10.1109/ICCPC55978.2022.10072214.
16. Md. M. Rahman et al., "Blockchain-Based Certificate Authentication System with Enabling Correction," Journal of Computer and Communications, vol. 11, no. 3, pp. 73–82, Mar. 2023, doi: 10.4236/JCC.2023.113006.
17. Desai A, Choudhary M, Singh D, and Prof. A. Mali, "BLOCKCHAIN BASED DECENTRALISED DROPBOX," IJARCCE, vol. 12, no. 6, May 2023, doi: 10.17148/IJARCCE.2023.12616.
18. Liu and Jiasong, "Digital signature and hash algorithms used in Bitcoin and Ethereum," SPIE, vol. 12636, p. 126365H, May 2023, doi: 10.1117/12.2675431.