Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 35, Issue 1, 2024 DOI: http://doi.org/10.23851/mjs.v35i1.1461

Research Article **Open Access**

Educational Certificate Verification System: Enhancing Security and Authenticity using Ethereum Blockchain and IPFS

Rafah Amer Jaafar[1], Saad Najim Alsaad[1], Mohammed Naji Al-Kabi[2]*

[1]Department of Computer Science, College of Science, Mustansiriyah University, 10052 Baghdad, IRAQ.
[2]Department of Information Technology, Al-Buraimi University College, OMAN.

*Correspondent contact: rafah_amer@uomustansiriyah.edu.iq

Article Info

Received
27/07/2023

Revised
07/09/2023

Accepted
15/09/2023

Published
30/03/2024

Abstract

Educational certificate counterfeiting is a major global challenge. There is no doubt that addressing both the problem of forgery and the verification of academic certificates is a fundamental issue that deserves research, development, and support at the highest levels. This paper presents a decentralized educational certificate verification system leveraging the Ethereum blockchain and the InterPlanetary File System (IPFS) to combat counterfeiting. Ropsten is used as a real-life Ethereum test network to demonstrate the effectiveness of the proposed system. IPFS is used to store educational certificate files on a decentralised file system. The smart contract is built in the Solidity language, compiled, and deployed using the online Remix IDE. The verification process is supported by scanning a QR code, which retrieves the validating certificate's information from the Ethereum network in real-time.

Keywords: Blockchain technology, Educational certificate verification, Ethereum blockchain, InterPlanetary File System (IPFS), Decentralized architecture, Certificate counterfeiting, Ropsten test network.

الخلاصة

تزوير الشهادات التعليمية هو تحدٍ عالمي كبير. مما لا شك فيه أن معالجة مشكلة التزوير والتحقق من الشهادات التعليمية مسألة أساسية تستحق البحث والتطوير والدعم على أعلى المستويات. يستعرض هذا البحث نظاماً لامركزياً للتحقق من الشهادات الأكاديمية بالإعتماد على (Ethereum blockchain)و (IPFS) لمكافحة عملية تزوير الشهادات. تم استخدام (Ropsten) كأحد شبكات إختبار (Ethereum) لإثبات فعالية النظام المقترح. يستخدم (IPFS) لتخزين ملفات الشهادات التعليمية ضمن نظام ملفات لامركزي. تم بناء العقد الذكي (smart contract) بلغة Solidity ، وتم تنفيذه ونشره باستخدام (Remix IDE) عبر الإنترنت. يتم دعم عملية التحقق من خلال مسح رمز الاستجابة السريعة ضوئياً QR ، والذي يسترد معلومات التحقق من صحة الشهادة بالإعتماد على شبكة (Ethereum) بشكل آني.

INTRODUCTION

The widespread issue of fraudulent educational certificates poses a significant challenge in today's academic and professional landscape. An educational certificate is granted after an academic stage as proof of its completion. Companies and institutes of higher education or companies use educational credentials to confirm applicants' educational histories. The vital role of educational documents attracts fraudsters to attempt to secure jobs based on forged academic certificates. To mitigate this threat, organisations can send a request to the certificate issuer to verify credentials and confirm their authenticity. Universities incur massive costs annually to process educational certificate verification requests [1].

Traditionally, verifying educational certificates is processed manually, and the information is confirmed using a central server. It requires a lot of ongoing effort to keep a central server working correctly and accessibly. Generally, the current combination of pen-and-paper-based and online storage systems leaves information vulnerable to hacking [2]. The use of technology in education has become increasingly popular in

recent years. However, there are concerns about security when it comes to certificates and credentials. To address these challenges, experts have proposed strategies to enhance security measures. One solution that has gained attention is blockchain technology [3][4]. Blockchain technology is well known for its security features, making it a suitable choice for combating certificate fraud in the education sector. The main reason for selecting blockchain is its properties of immutability and decentralization, which provide a solution to the issue of certificate fraud. Immutability ensures that once a record is added to the blockchain, it cannot be tampered with easily. This means that educational certificates registered on a blockchain are resistant to alteration or counterfeiting without being detected. The transparent nature of the ledger ensures that any attempt to manipulate or forge certificates will be immediately identified, preventing such activities. Moreover, decentralization plays a role in blockchain by eliminating the need for a central authority for certificate verification. Instead, the verification process is distributed across a network of nodes, making it highly resistant to manipulation. Blockchain technology has an impact on the field of certificates. Firstly, it bolsters the security aspect by ensuring that the certificates are protected. Secondly, it plays a role in building trust among individuals regarding the legitimacy and genuineness of credentials [5].

This paper is structured as follows: Section Two presents related works; Section Three gives a background of conceptions and tools that are used in the proposed system; Section Four describes the proposed system; Section Five discusses the experimental results of the proposed system; and the final section is the conclusion.

RELATED WORKS

Blockchain is used in various fields, including health, finance, and education. Although the application of blockchain technology in the education field is still in its early stages, it is currently the subject of a lot of attention. This section presents the latest practices in the field of education.

Aamna Tariq *et al.*, 2019 [6] introduced Cerberus, a system for verifying credentials. Cerberus utilizes a permissioned blockchain built on the Parity Ethereum client. Offers an approach to efficiently and securely verifying academic credentials. The verification process involves scanning a Quick Response (QR) code to access and retrieve validating information from the Cerberus network. This QR code enables real-time verification of student credentials using a smartphone app, making the verification process streamlined for students and potential employers. By employing a permissioned blockchain, Cerberus ensures that authorized entities like universities and watchdog organizations can participate in maintaining and validating credentials. This approach aligns closely with the existing ecosystem of verification while preserving security properties like data privacy, integrity, and revocation guarantees. Cerberus serves as an example showcasing how blockchain technology has the potential to revolutionize verification systems by offering a secure method for verifying academic credentials.

Diogo Serranito *et al*., 2020 [7] presented an ecosystem based on a permissionless blockchain (Ethereum platform) that runs two types of smart contracts: Consortium Smart Contracts and Higher-Education Institutions (HEI) Smart Contracts. The ecosystem lets HEI store the certificates they issued in the blockchain, and organizations can verify the validity and integrity of these certificates.

Binh Minh Nguyen *et al.*, 2020 [8] proposed a solution called the Vietnamese Educational Certification Blockchain (VECefblock) system to tackle the problem of certificates in Vietnam. By utilizing technology, the VECefblock system aims to ensure that academic credentials are genuine and trustworthy. The authors focused on using the Hyperledger Fabric platform, a blockchain system deployed on Amazon's EC2 service. This comprehensive system offers a solution for verifying certificates in Vietnam. By implementing a blockchain-based application, it provides a reliable platform to address the challenges posed by diplomas in the country. The authors recognized the potential of technology and leveraged its features, such as

forgery information, transaction verification, and smart contracts, to effectively combat this issue. Additionally, they presented principles for developing applications as a foundation for building VECefblock. The architecture, business processes, and data mapping structure of this system were thoughtfully designed to suit Vietnam's landscape. Through performance evaluations and practical tests, the authors demonstrated that the VECefblock system is feasible and functional in real-world deployment scenarios. The results obtained highlight the potential of technology in addressing problems, especially in the field of certificate management in Vietnam.

Raaj Anand Mishra *et al.*, 2021 [9] presented a decentralized application (DApp) designed to address the challenges associated with securely sharing student credentials. The current education ecosystem involves stakeholders such as students, schools, companies, professors, and government authorities. All these parties face efforts to ensure the authenticity and privacy of student credentials during the sharing process. To overcome these complexities, along with security-related issues and errors in credential sharing, the authors proposed a blockchain-based architecture. This architecture provides tamper-proof authentication features while also protecting privacy during the sharing process. The roles and core functionalities of stakeholders within the system are clearly defined in their work. Additionally, they presented a mechanism for integrating privacy into this architecture to safeguard student data. As a proof-of-concept demonstration, they implemented this privacy-protected architecture through a prototype DApp. The DApp makes use of nine contracts that serve as components. These contracts are deployed on the Ethereum blockchain for testing and validation purposes. The authors have expressed their intention to further improve the system's architecture by deploying it on a permissioned blockchain platform.

Elva Leka and Besnik Selimi, 2021 [10] submitted a blockchain-based application. The smart contract and Ethereum platform are used to store and verify educational certificates. The certificates are stored in a decentralized file system (IPFS). Their proposal provides data confidentiality by using the AES encryption algorithm before transactions are created.

Varshinee Chukowry *et al.*, 2021 [5] presented a system for verifying signatures that makes use of capabilities. Their research focuses on signing and validating documents using a permissioned approach. The authors recognize the importance of learning and skill recognition beyond classroom settings. They examined existing systems based on technology and put forward an innovative web-based system for digital badges and micro-credentials to help learners acquire desired skills efficiently. To implement their solution, they opted for the Ethereum blockchain due to its security features and decentralized nature. Their system encompasses quizzes, digital badges, registration, and course management. The study effectively demonstrated how this system overcomes the limitations of learning content management systems (LCMS). In light of the challenges posed by COVID-19, e-learning and technology-enhanced learning have become crucial, making the proposed microcredential system with technology a solution for learners. Its flexibility, cost-effectiveness, shorter duration, and recognition of skills have appealed to learners, significantly encouraging them to embrace microcredentials as an alternative to university courses. The study introduced a user system that allows learners to easily choose their desired courses, take exams, and earn recognition in the form of badges. Universities can make use of this system to offer badges to learners and provide access to courses and exams.

In this paper, a decentralised architecture of educational certificate verification using a permissionless blockchain (the Ethereum platform) and IPFS is proposed and implemented. The educational certification verification process is quick and effortless by scanning a QR code that retrieves validating certificate information from the Ethereum network in real-time. Table 1 shows a summary of the proposed system and related works.

Table 1. Summarization of related works and proposed system.

Ref.	Blockchain Type	Platform	Digital Currency	Off-chain Storage	Usability Verification
[6]	permissioned	Parity Ethereum	X	X	QR
[7]	permissionless	Ethereum	Ether	IPFS	X
[8]	permissioned	Hyperledger Fabric	X	local database	X
[9]	permissionless	Ethereum	Ether	IPFS	X
[10]	permissionless	Ethereum	Ether	IPFS	X
[5]	permissionless	Ethereum	Ether	IPFS	X
Proposed system	permissionless	Ethereum	Ether	IPFS	QR

MATERIALS AND METHODS

Background

In this section, the concepts and tools that are used in the proposed system are presented.

Blockchain

Blockchain technology has evolved greatly alongside the cryptocurrency Bitcoin. Block-chain is a distributed ledger that includes interconnected blocks. It is secured by tamper-proof cryptographic concepts. The Blockchain mechanism works with a decentralised architecture and is managed by the consensus of the network participants. Every participant (i.e., a node) in the blockchain network has a copy of the distributed ledger. Blockchain data is constantly growing as new blocks are added. Once blocks are added to a blockchain network, it is impossible to change data without the consent of the majority or all the network nodes. Each block in the blockchain contains a hash of the previous block to protect against tampering and ensure data integrity. The block's hash changes after any data in the block is altered. Any modification in the data is detected because the new block's hash is different from the hash that was previously stored in the next block [11][12]. Each block contains a list of transactions. Every transaction in the block is verified and stored using a consensus protocol [13].

Blockchain is categorised as public, private, or consortium. A public blockchain is considered a permissionless network (i.e., everyone can join the network, read or write to it, and contribute to its consensus protocol). Public blockchain networks are fully decentralised. The most prominent public blockchains are Bitcoin and Ethereum. A private blockchain is a permissioned network (i.e., only authorised users can join the network and can write or read in addition to validating transactions). Private blockchain networks are centralised. Examples of private blockchains include Multichain and Blockstack. A consortium blockchain is also considered to be a permissioned network (i.e., only pre-defined nodes can order the transactions and add new blocks. Other nodes can only send, read transactions, and verify new blocks). Consortium blockchains are partially centralised. Corda and Hyperledger are examples of consortium blockchain networks [12].

Ethereum and Smart Contract

Ethereum is the second-largest blockchain network in the world. It is a public, distributed, and open-source platform [14]. The Ethereum platform expands the blockchain conception with smart contracts. Smart contracts are programs (i.e., self-executing contracts programs containing the agreement rules among the parts) running on the Ethereum blockchain [15][16].

Smart contracts are written in high-level languages. These programs are compiled into Ethereum Virtual Machine (EVM) bytecode and then implemented by a machine. Solidity is the most popular language for writing smart contracts in the Ethereum blockchain. The smart contract is deployed onto the Ethereum blockchain using a transaction. The execution of the smart contract is associated with a gas price and a gas limit [17][18].

The Ethereum platform needs a mechanism for ensuring the smart contract does not obstruct the Ethereum blockchain by implementing an

infinite loop. Thus, Ethereum needs to charge a fee for executing transactions. It uses the Ethereum currency (Ether) for this clearing [18]. A smart contract allows for the execution of trusted transactions between anonymous parties. The result of executing transactions corresponds to a change in the state of the blockchain. Such a change in state is triggered by posting the transactions to the Ethereum blockchain. Transactions are collected in the block, and the blockchain nodes are required to reach a consensus in order to add the new block to the Ethereum blockchain [16].

The Ethereum wallet stores the account's public and private keys, and it is used to receive and spend Ether [17]. Ethereum applications work exactly as they are programmed into the smart contract without any possibility of censorship, downtime, and fake or third-party interference [14].

REMIX IDE

Remix IDE is an open-source website, an online IDE, and the easiest way to build smart contracts in Solidity. It contains a set of plugins with intuitive GUIs. Remix is utilised for the entire lifecycle of smart contract development. It allows the development and deployment of smart contracts for the Ethereum blockchain. It can also be utilised as a learning platform [19][20].

METAMASK

MetaMask is a valuable tool that plays an essential role in entering the world of blockchain. MetaMask is an Ethereum wallet. Through MetaMask, the following can be done [20]:

» Create accounts to be used in any of several Ethereum networks.
» Keep the accounts' private keys so that they can be exported or imported.
» Switch between different Ethereum networks so that accounts can reveal the exact balance for each network.
» Execute transactions between accounts.
» Transfer Ethers from one account to another.
» Keep tokens in MetaMask accounts.
» View transaction details on Etherscan, the Ethereum blockchain explorer.

Ethereum Networks

The Ethereum platform has several test networks that can be used for development purposes. The main advantage of test networks is that the cryptocurrency Ether has no real monetary value. Since implementing decentralised applications costs a certain amount of gas, debugging, and testing on test networks, the developer's money can be saved. When the test is finally completed, it needs to connect to the main network for real-world deployment. There are four test networks: Ropsten, Rinkeby, Kovan, and Goerli [14][20].

IPFS

Blockchain has become one of the main technologies being promoted nowadays. However, it is still very expensive to store large files as there is a maximum size of 1MB per block in the Bitcoin blockchain, which necessarily limits the size of files that can be uploaded. An urgent need for large file storage was addressed by the use of decentralised storage systems such as IPFS, SWARM, Storj, and Sia. IPFS is an addressable, open-source, peer-to-peer, and globally distributed file system. It can be used to store and share large files with high-throughput speed. Blockchain is inefficient at storing large files of data. However, it has been shown to be effective while storing document hashes in the transaction rather than in the file itself. The hash is generated each time a file is uploaded to IPFS, and the file's hash is stored in the transaction. For any changes in the file's content, the hash value will change [21].

In IPFS, files are replicated in multiple nodes. Moreover, it offers good performance since files can be accessed on adjacent nodes, typically closer than to central models. The IPFS does not contain a single point of failure, and nodes do not have confidence in each other. The files are stored using several geographically distributed servers [22].

In IPFS, any file that is stored obtains a unique hash value, and the files are distributed in the

files system. The table of distributed hash is structured as a Merkel Tree Directed Acyclic Graph (DAG). This ensures that untrusted nodes cannot change the file from the central access point [23][24].

Proposed System

In this paper, a decentralised architecture of educational certificate verification is developed using the Ethereum blockchain and IPFS. Ropsten is used as a live Ethereum test network, and IPFS is used to store academic certificate files on a decentralized file system. The proposed system consists of two stages: certificate issue and certificate verification.

Certificate Issue Stage

This stage is concerned with the steps of digital certificate initialization and storage in the blockchain. Figure 1 depicts the activity diagram, while Algorithm 1 illustrates the steps of the certificate issue stage.

Algorithm 1. Certificate Issue

Inputs: Certificate file, Certificate information (student's full name, college, department, university order number, and university order date), and Certificate's IPFS hash.
Output: Certificate's ID represented in the form of a QR code.

Step 1. Upload the certificate file to IPFS to generate the certificate's IPFS hash.

Step 2. Send information about the certificate and an IPFS hash to the smart contract.

Step 3. Generate the certificate's ID.

Step 4. If the certificate's ID does not exist on the Ethereum blockchain, then:

Step 5. Save the certificate on the Ethereum blockchain.

Step 6. Else:

Step 7. Certificate already saved on the Ethereum blockchain.

Step 8. End if:

Step 9. Convert the certificate's ID to a QR code and print it on the certificate.

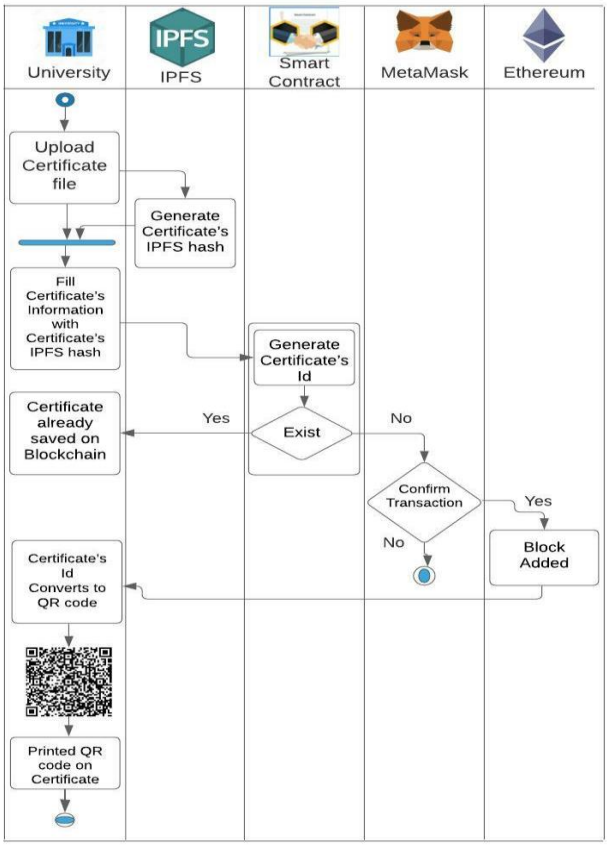


Figure 1. Activity Diagram of the Certificate Issue Stage.

CERTIFICATE VERIFICATION STAGE

This stage is concerned with all the steps for the verification of university-issued educational certificates. The activity diagram in Figure 2 and Algorithm 2 illustrates the steps of the certificate verification stage.

Algorithm 2. Certificate verification

Inputs: QR code on the certificate.
Output: Certificate's information, certificate's IPFS hash, and certificate file.

Step 1. Scan the QR code to generate the certificate's ID.

Step 2. Execute a smart contract to extract the certificate's information and the certificate's IPFS hash through the certificate's ID.

Step 3. Display the certificate's information with the certificate's IPFS hash that is saved on the Ethereum blockchain.

Step 4. Retrieve the certificate file from IPFS using the certificate's IPFS hash.

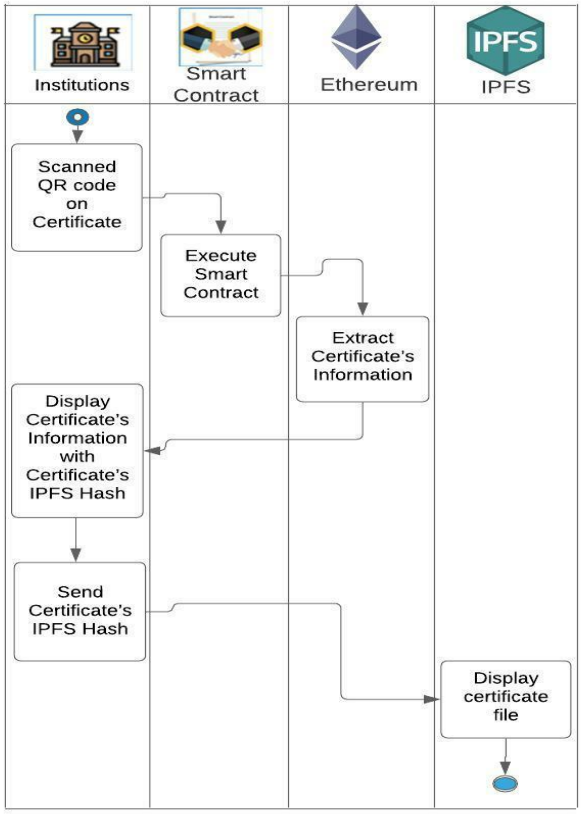


Figure 2. Workflow of the Certificate Verification Stage.

EXPERIMENTS AND RESULTS

The proposed system is implemented on a Lenovo laptop with the following specifications: CPU: Intel Core i7-9750H @ 2.60 GHz×12; Physical Memory: 16 GB; OS: Ubuntu 20.10 64-bit.

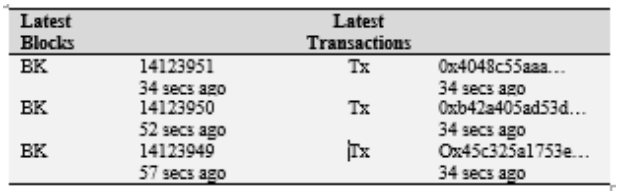
The client side of the proposed system is developed with HTML, CSS, JavaScript, and web3.js. Web3.js is used to interact with the Ethereum blockchain.

The smart contract of the proposed system is developed and deployed by Remix IDE. The smart contract is written in Solidity programming language. Table 2 depicts the structure of the proposed smart contract.

Ropsten is used as a real-life Ethereum test network tool to trace the output during the implementation process. Ropsten Ethereum is used for testing before the deployment of the proposed system on Mainnet (i.e., the main Ethereum network). Figure 3 depicts the Ropsten test network explorer.

Table 2. Structure of the Proposed Smart Contract

Variables		
Name	**Type**	**Description**
Certificate	Struct	To represent the certificate record
Certificated	Bytes32	The fixed length bytes32 used to store the certificate Id
StudentFullname	string	To store the student's full name
College	string	To store the college
Department	string	To store the department
UniversityOrderNumber	string	To store the university order number
UniversityOrderDate	string	To store the university order date
IsAdded	boolean	Boolean value to check if the certificate is added or not
CertificateHash	string	To store the certificate's IPFS hash
CertificateIds	Byte32[]	An array containing certificate Ids for all registered certificates
IdToCertificate	Mapping	Stores an indexed list of registered certificates
Functions		
Name		**Description**
CertificateIssue		Check If the certificate's ID does not exist on the Ethereum blockchain and then store the certificate on the Ethereum blockchain.
Keccak256		To generate the certificate's ID.
CertificateVerification		Returns certificate's information under the given certificate's ID.



Latest Blocks		Latest Transactions	
BK	14123951 34 secs ago	Tx	0x4048c55aaa... 34 secs ago
BK	14123950 52 secs ago	Tx	0xb42a405ad53d... 34 secs ago
BK	14123949 57 secs ago	Tx	0x45c325a1753e... 34 secs ago

Figure 3. Ropsten Test Network Explorer - Latest Blocks and Transactions

Figure 3 illustrates the latest blocks and latest transactions that are pending and confirmed on Etherscan. The Etherscan Explorer can also be used to track the status of pending transactions, and it gives an estimate of how long the transactions will take to be confirmed, as well as updates when the transactions are completed. The Etherscan explorer can search for the certificate's transaction using a transaction hash and search for the block containing the certificate's transaction by the block number. It also searches for the proposed smart contract using the address of the smart contract. The Ropsten Ethereum Faucet is exploited to withdraw Ether for testing the proposed system, as shown in Figure 4.

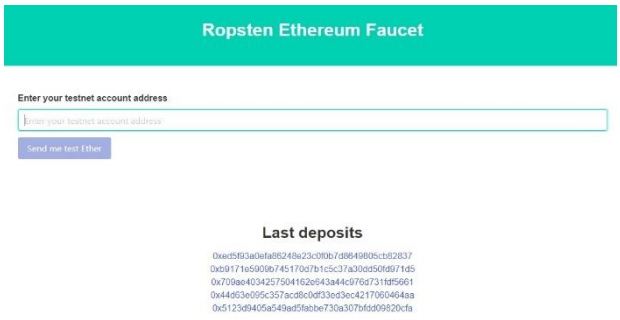


Figure 4. Ropsten Ethereum Faucet - Test Ether Withdrawal.

Notice in Figure 4, the address of the account associated with MetaMask must be entered in the text field. Figure 5 shows the transaction details of the receipt test from the Ropsten Ethereum Faucet.

Table 3 shows the list of certificate transactions that are executed on the Ropsten test network. Each transaction represents a certificate containing details such as the transaction's ID (Transaction Hash), block number (Block), and transaction cost (Tx fee) that is measured by Ether.

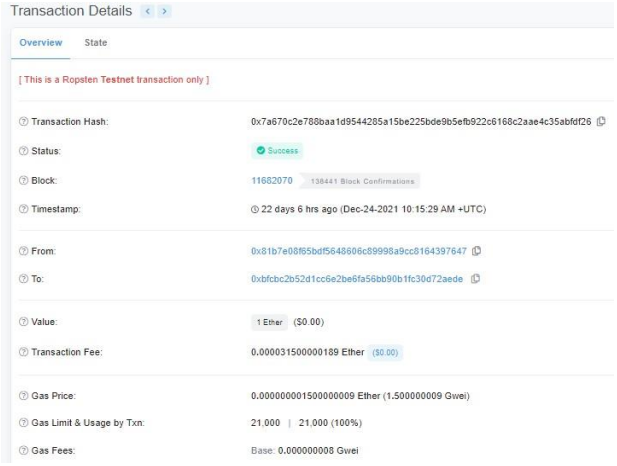


Figure 5. Receipt of Test Ether from Ropsten Ethereum Faucet

Table 3. List of Certificate Transactions Executed on the Ropsten Test Network

Tx	Transaction Hash	Block	Tx fee (Ether)
1	0xeb1bd99fab36e6d76d2d34e7192220d84f4c675ebd6158f47e2c70e2dca70aaf	11754720	0.000814317504885905
2	0x173c4b7fd145688f869d1111519b98fc448576a0672ac9a19319f35b5c66e893	11754689	0.000814047506186761
3	0x55bcbfb0ee5dcc9f684388363cef3eacd02d64237def69a816901a5dde03182f	11754618	0.000814460000488676

One of the goals is to tackle the problem of certificate fraud in the education sector. The system aimed to provide a tamper-proof method of verifying the authenticity of credentials by storing certificates on an unchangeable and decentralized blockchain. The outcomes of the experiment support the feasibility of this approach.

By utilizing the CertificateIssue function in the contract, the certificates are added successfully to the Ethereum blockchain. Unique certificate IDs were generated using the Keccak256 hashing algorithm. Served as keys for storing certificate information. The immutability of the blockchain, combined with the robustness of the Ethereum test network made it extremely difficult for fraudulent certificates to infiltrate the system. This aligns directly with the objective of combating certificate fraud.

Additionally, through the certificate verification function, users were able to retrieve certificate information by providing a certificate ID. This feature demonstrated that the proposed system has the capability to securely and transparently

verify certificates without relying on authorities or third-party intermediaries. As a result, the experiment showcased how blockchain technology can revolutionize and enhance security and reliability in the process of certifying education credentials.

The experimental results strongly confirm that the proposed blockchain-based certificate verification system is effective.

Through the utilization of blockchain's immutability and decentralization, we have developed a resolution for addressing the issue of certificate fraud within the education sector. These findings not only confirm the viability of the proposed system but also highlight its potential to make a substantial contribution to resolving the problem mentioned in the introduction. Ultimately, this will promote trust and authenticity in credentials. Moving forward, the following steps involve conducting real-world testing and implementing the solution on the Ethereum network to realize its impact fully.

CONCLUSIONS

This paper proposes blockchain as an anti-counterfeiting technology for educational certificates. A decentralised architecture of educational certificate verification based on the Ethereum blockchain and IPFS is proposed and implemented. The proposed system provides certificates with immutability to prevent certificate counterfeiting and reduce the costs of verifying authenticity. In addition, the educational certificate verification process is fast and effortless by scanning a QR code that retrieves validating certificate information from the Ethereum network in real-time. The proposed system proved to be of great value by addressing limitations in the traditional educational certificate verification process.

A future topic of research is the development and implementation of the second proposed system on a permissioned blockchain platform, such as Hyperledger fabric, to complete its performance.

Disclosure and Conflict of Interest: The authors declare that they have no conflicts of interest.

References

[1] S. Rasool, et al. (2020) "Docschain: Blockchain-based IoT solution for verification of degree documents," IEEE Transactions on Computational Social Systems, vol. 7, No. 3, pp. 827-837.

[2] D. Kulkarni, (2021) "Leveraging Blockchain technology in the Education Sector," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 10, pp. 4578-4583.

[3] C. Turcu, C. Turcu, et al. (2019) "Blockchain and its Potential in Education," arXiv preprint arXiv:1903.09300.

[4] W. Gräther, et al. (2018) "Blockchain for education: lifelong learning passport," in Proceedings of 1st ERCIM Blockchain workshop 2018, 2018: European Society for Socially Embedded Technologies (EUSSET).

[5] V. Chukowry, et al. (2021) "The future of continuous learning–Digital badge and microcredential system using blockchain," Global Transitions Proceedings, vol. 2, No. 2, pp. 355-361.

[6] A. Tariq, et al. (2019) "Cerberus: A blockchain-based accreditation and degree verification system," arXiv preprint arXiv:1912.06812.

[7] D. Serranito, et al. (2020) "Blockchain ecosystem for verifiable qualifications," in 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2020: IEEE, pp. 192-199.

[8] B. M. Nguyen, et al.(2020) "Towards a blockchain-based certificate authentication system in Vietnam," PeerJ Computer Science, vol. 6, p. e266.

[9] R. A. Mishra, et al. (2021) "Privacy protected blockchain based architecture and implementation for sharing of students' credentials," Information Processing & Management, vol. 58, No. 3, p. 102512.

[10] E. Leka, et al. (2021) "Development and Evaluation of Blockchain based Secure Application for Verification and Validation of Academic Certificates," Annals of Emerging Technologies in Computing (AETiC), vol. 5, No. 2, pp. 22-36.

[11] Z. Zheng, et al. (2017) "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE international congress on big data (BigData congress), 2017: IEEE, pp. 557-564.

[12] A. I. Sanka, et al.(2021) "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research," Computer Communications.

[13] T. M. Fernández-Carames, et al. (2020) "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," IEEE access, vol. 8, pp. 21091-21116.

[14] G. Zheng, et al.(2021) Ethereum Smart Contract Development in Solidity, 1st ed., Springer.

[15] F. Ma et al. (2021) "Security reinforcement for Ethereum virtual machine," Information Processing & Management, vol. 58, No. 4, p. 102565.
[16] A. Vacca, et al. (2020) "A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges," Journal of Systems and Software, p. 110891.
[17] S. Bistarelli, et al. (2020) "Ethereum smart contracts: Analysis and statistics of their source code and opcodes," Internet of Things, vol. 11, p. 100198.
[18] T. Osterland, et al. (2020) "Model checking smart contracts for ethereum," Pervasive and Mobile Computing, vol. 63, p. 101129.
[19] R. M. A. Latif, et al. (2020) "A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology," Multimedia Tools and Applications, pp. 1-24.
[20] W.-M. Lee, (2019) Beginning ethereum smart contracts programming: With Examples in Python, Solidity and JavaScript, 1st ed.
[21] N. Nizamuddin, et al. (2019) "Decentralized document version control using ethereum blockchain and IPFS," Computers & Electrical Engineering, vol. 76, pp. 183-197.
[22] F. R. Vidal, et al. (2020) "Revocation mechanisms for academic certificates stored on a blockchain," in 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020: IEEE, pp. 1-6.
[23] K. M. Alam, et al. (2020) "A Blockchain-based Land Title Management System for Bangladesh," Journal of King Saud University-Computer and Information Sciences.
[24] A. Muwafaq, S. Alsaad, (2021) "Design scheme for copyright management system using Blockchain and IPFS, " International Journal of Computing and Digital Systems, 10, 613-618.

How to Cite

R. A. Jaafar, S. N. Alsaad, M. N. Al-Kabi, “Educational Certificate Verification System: Enhancing Security and Authenticity using Ethereum Blockchain and IPFS”, *Al-Mustansiriyah Journal of Science*, vol. 35, no. 1, pp. 78–87, Mar. 2024, doi: 10.23851/mjs.v35i1.1461.