





Research Article

Digital Assurance and Traceability of NFT-based Certificates

Nihat Zaman¹ , Nursena Baygın² *

¹ Department of Computer Engineering, Erzurum Technical University, 25000 Erzurum, Türkiye

² Department of Computer Engineering, Erzurum Technical University, 25000 Erzurum, Türkiye

* Correspondence: nursena.baygin@erzurum.edu.tr

Received: 28 April 2023; Accepted: 28 May 2023; Published: 30 June 2023

Abstract: With the development of technology in today's world, many sectors are conducting their activities in digital environments. This development strengthens the connection between users and the industry, and more efficient results are obtained. However, along with many advantages of digitization, there are also problems such as security loss, copyright infringement, and data corruption. The ease of replicating and distributing data on the internet is due to various security vulnerabilities. This study proposes a solution for protecting certificates issued to individuals by companies/institutions in the digital environment, following a certain degree of success. Certificates are used for job applications, competency verification, and similar purposes. Currently, fake certificates and diplomas produced create problems for institutions and organizations that verify competencies. In this respect, it is possible for people without the required skills to take unwanted positions. This study aims to prevent fake certificates propose a system that enables certificate holders and institutions to verify certificates. Additionally, it is aimed to make certificates traceable and provable in digital environments. The proposed method aims to create certificates using blockchain technology through smart contracts and to make them available to users on a website. Furthermore, it is suggested to use NFTs, another technology offered by blockchain, to provide intellectual property rights to certificates, enabling them to be monitored and owned on the internet.

Keywords: blockchain, non-fungible token, copyright, IPFS

Araştırma Makalesi

NFT Tabanlı Sertifikaların Dijital Güvencesi ve İzlenebilirliği

Öz: Günümüz dünyasında teknolojinin gelişmesiyle birlikte birçok sektör dijital ortamda faaliyetlerini yürütmektedir. Bu gelişme kullanıcı ile sektör arasındaki bağı kuvvetlendirmekte ve daha verimli sonuçlar alınmaktadır. Ancak dijitalleşmenin birçok avantajının yanında güvenlik kaybı, telif hakkı ihlali, veri bozulmaları gibi problemler de bulunmaktadır. İnternet ortamında verilerin kolaylıkla çoğaltılıp dağıtılması çeşitli güvenlik açıklarından kaynaklanmaktadır. Bu çalışmada şirketler/kurumlar tarafından belirli bir başarı doğrultusunda kişilere verilen sertifikaların internet ortamında korunmasına yönelik bir öneri sunulmaktadır. Sertifikalar iş başvurusunda, yetkinlik doğrulama gibi amaçlar doğrultusunda kullanılmaktadır. Günümüzde üretilen sahte sertifika ve diplomalar yetkinlik doğrulayan kurum ve kuruluşların işini zora sokmaktadır. Bu doğrultuda yetkinlik sahibi olmayan kişilerin istenmeyen mevkilere gelebilmesi mümkün olabilmektedir. Bu çalışma ile sahte sertifikaların önüne geçilmesi, sertifika sahiplerinin ve kurumların sertifikaları doğrulamasını sağlayan bir sistem önerilmesi amaçlanmaktadır. Ayrıca sertifikaların dijital ortamlarda izlenebilir ve kanıtlanabilir olabilmesi hedeflenmektedir. Önerilen yöntemde blok zincir teknolojisi kullanılarak akıllı kontratlar vasıtasıyla sertifikaların oluşturulması ve internet sitesi üzerinde kullanıcılar tarafından alınabilmesi amaçlanmaktadır. Ayrıca blok zincirin sunduğu bir diğer teknoloji olan NFT'ler ile de sertifikaların fikri tapu mülkiyeti sağlanarak internet ortamında izlenmesi ve aitlik kazanması önerilmektedir.

Anahtar Kelimeler: blok zincir, NFT, telif hakkı, IPFS

Citation: N. Zaman and N. Baygın, "Digital assurance and traceability of NFT-based certificates", *Journal of Studies in Advanced Technologies*, vol. 1, no. 1, pp. 17-25, Jun 2023, doi: 10.5281/zenodo.8074838

1. Introduction

With the rapid development of technology, many systems have been updated and renewed. Industrial revolutions [1]–[3] have led to developments in areas such as mechanization, mass production, mass customization, the internet of things, big data, and cloud computing. These developments have brought innovations to human life such as fast production, personalized design, and communication between machines, but they have also caused various problems in many areas such as data security, supply-demand communication, and traceability. One of the most important of these problems is data security, which can pose serious threats. The WannaCRY virus attacked 300,000 computers in 150 countries in 2017, causing serious crises in many areas such as public administration, medicine, and finance [4]. The disclosure of user information damages the reputation of institutions and companies and also harms their market share. Cyberattacks require companies and governments to take serious measures in terms of information security. Scientists are conducting intensive research on data security issues, while companies are investing in data security.

With the development of the internet, copying and distributing data has become easier, leading to various problems in protecting copyright. As remote learning becomes more widespread, online courses are becoming increasingly popular. These courses, prepared by companies or public institutions, offer certificates to users who successfully complete certain training. This study proposes to ensure the security of these digital certificates and prevent their duplication, as well as establish a traceable structure. Blockchain technologies offer various advantages in terms of security and traceability in this regard. Nowadays, blockchain technology is used in many different fields such as healthcare, finance, and supply chain [5]. With its cryptographic infrastructure and decentralization, it offers revolutionary innovations in data security [6]–[8].

Another service provided by blockchain is the Non-Fungible Token (NFT) system, which produces immutable digital materials in the form of tokens [9]. Today, many use cases are being created for NFTs. One of these methods is providing ownership proof to users [10]. In this proposed study, NFTs will be used to prove and track certificate ownership on the blockchain. Fake certificates are currently a problem for companies and universities, both economically and ethically [11]. The aim of this study is to prevent the use of fake certificates and enable institutions to verify individuals' certificates and diplomas through a single system. When reviewing related literature [12] (certificate Vietnam), it was found that the aim was to protect patents, but the solution was different and the proposed application was a system that did not rely on non-transferable, unqualified intellectual property and was not directly accessible to users. Another developed project is the DSTAC project developed under the umbrella of Yeditepe University. The main goal of this project is to verify the certificates created through blockchain. In this context, it is seen that the study to be developed is completely different from other original ideas. In this study, we aim to find answers to the question of what can be done to make blockchain technology more widespread, which is attracting great interest from scientists and companies based on the following hypotheses.

- Blockchain technology is currently used in many areas, especially in the finance sector.
- NFTs are used to protect copyrights in areas such as music and art.
- The security of digitally produced certificates can be solved with blockchain technology

The aim of this study is to design a system that combines blockchain technology and the NFT system it offers to ensure certificate security, as well as to track and prove ownership of certificates in the digital realm. The system will address the need for transparency and security by utilizing the advantages of blockchain technology. The study aims to solve the global problem of certificate security and verifiability using the transferable qualified intellectual property technology of blockchain. The main contributions and motivation of this study are outlined below.

- Storing certificates with non-transferable qualified intellectual property on the blockchain.
- Verifying the identity of users and institutions and linking the created certificates to users' blockchain wallets.
- Allowing institutions to view a person's NFT certificates and diplomas on a single system, thereby preventing the use of fake certificates and diplomas.
- Analyzing the storage and verification conditions of paper diplomas in the current system and transferring them to the blockchain environment more effectively.

- Analyzing the systems and tools used by fake certificate manufacturers, taking necessary precautions, and addressing these vulnerabilities.
- Collecting users' certificates in a decentralized structure. Integrating institutions, organizations, and users worldwide into this system.

The rest of this study is organized as follows: section 2 provides the technical components of the proposed approach. Section 3 presents detailed information about the proposed method. Section 4 presents the results of the proposed method.

2. Technical Component

Since its introduction by Satoshi Nakamoto in 2008, blockchain technology has received significant attention from various industries [13]. Bitcoin blockchain was established to enable person-to-person money transfers by adopting principles of decentralization, immutability, anonymity, and transparency [14]. Seven years after the launch of Bitcoin blockchain, Ethereum blockchain was developed. In addition, to secure money transfers, Ethereum blockchain has contributed to making the blockchain more functional through smart contracts.

2.1. Blockchain

Blockchain technology is named as such because it keeps records of verified transactions on the blocks. A blockchain consists of two sides: validators and users. As shown in Figure 1, a user sends a transaction they wish to make to the blockchain. If the transaction is valid, it is added to the ledger by the record-keeping node. Once the transaction is verified, it is sent to validators to be confirmed in a block. The first validator to confirm the transaction adds the block to the blockchain. After the block is verified by other validators, the transaction is considered confirmed on the blockchain.

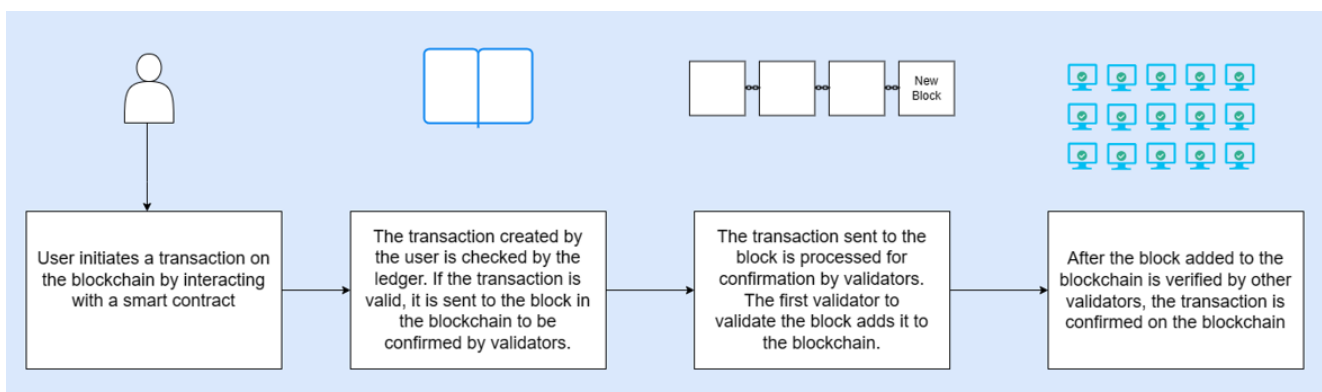


Figure 1. Transaction confirmation steps in blockchain

Blockchain is widely used in many fields today, especially in systems where security is required. In the literature, it is seen that the security advantages offered by blockchain are utilized in many applications such as the Internet of Things, RFID, healthcare, machine learning, copyright, mass customization, and more [15]–[19].

2.2. NFT (Non-Fungible Token)

Non-fungible tokens (NFTs) are digital assets created on the blockchain through smart contracts. NFTs can contain photos, sound, or video [20] and have many use cases today, including gaming, digital art, and identity verification. The fundamental difference between NFTs and cryptocurrencies is that NFTs do not have equal value. NFTs have two technological structures in their infrastructure. The first structure is on the blockchain, where NFTs are created through smart contracts. The second structure stores the content data of the NFT on the blockchain. When these two structures come together, an NFT supported visually and functionally is created. Blockchain users who want to own NFTs interact with them through smart contracts and carry out transactions such as purchasing and transferring. Another type of NFT is non-transferable qualified intellectual property. Non-transferable qualified intellectual properties are generally used to determine ownership of individuals [21]. As shown in Figure 2, the content creator first requests an NFT.

Then, the transaction is either approved or rejected according to the smart contract conditions. If the transaction is approved, the NFT is created, and the meta-data of the data is stored on the blockchain. The entire data is stored on IPFS.

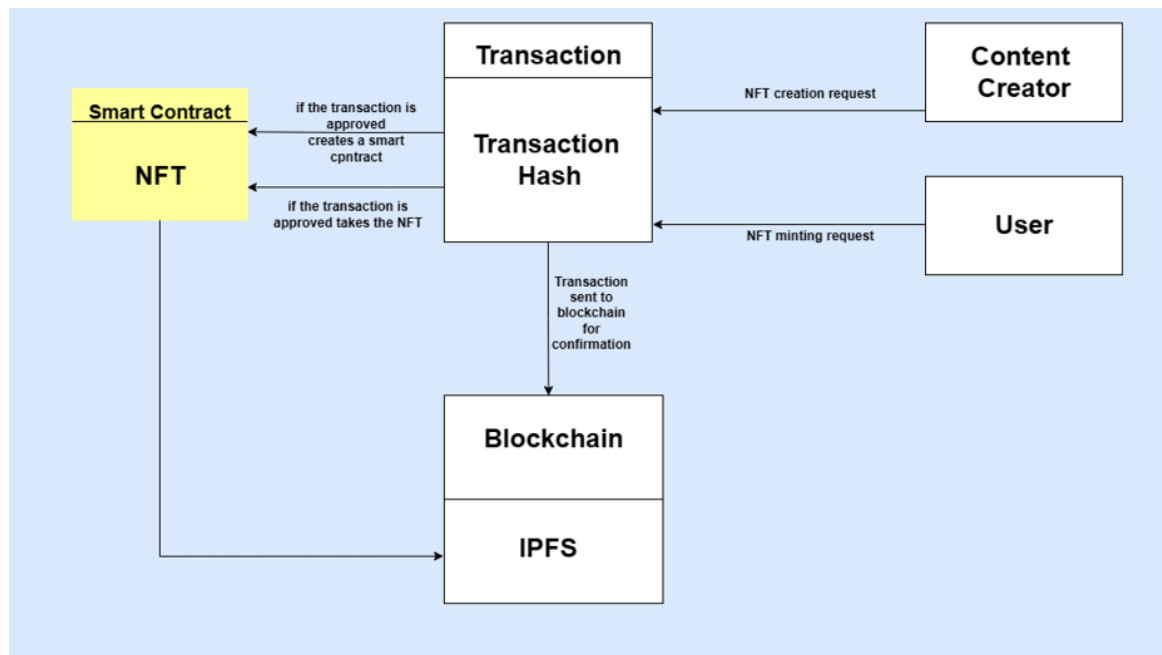


Figure 2. Working principle of NFTs

3. Proposed Method

A certificate is a document that shows a person's qualification in any subject that requires knowledge. Certificates are issued to individuals by authorized institutions or organizations based on their eligibility. In the proposed study, institutions or organizations that issue certificates and users who will acquire certificates require a wallet for blockchain interaction. For this purpose, Ethereum blockchain, which is widely used, is proposed. This study is a proposal and it is aimed to be tested on the test network and presented to user experience in the future.

In this proposed method, smart contracts will be used in the creation of certificates and diplomas. The certificates and diplomas will be created on a blockchain-based smart contract as non-transferable qualified intellectual property. The data of the created NFTs will be stored on the Inter Planetary File System (IPFS). The verification of the ownership of blockchain addresses of individuals and institutions will be carried out in accordance with the Law No. 6698 on the Protection of Personal Data of the Republic of Turkey. Following the use of the aforementioned criteria, institutions or organizations can share their certificates with users on the project website after verifying them on the website.

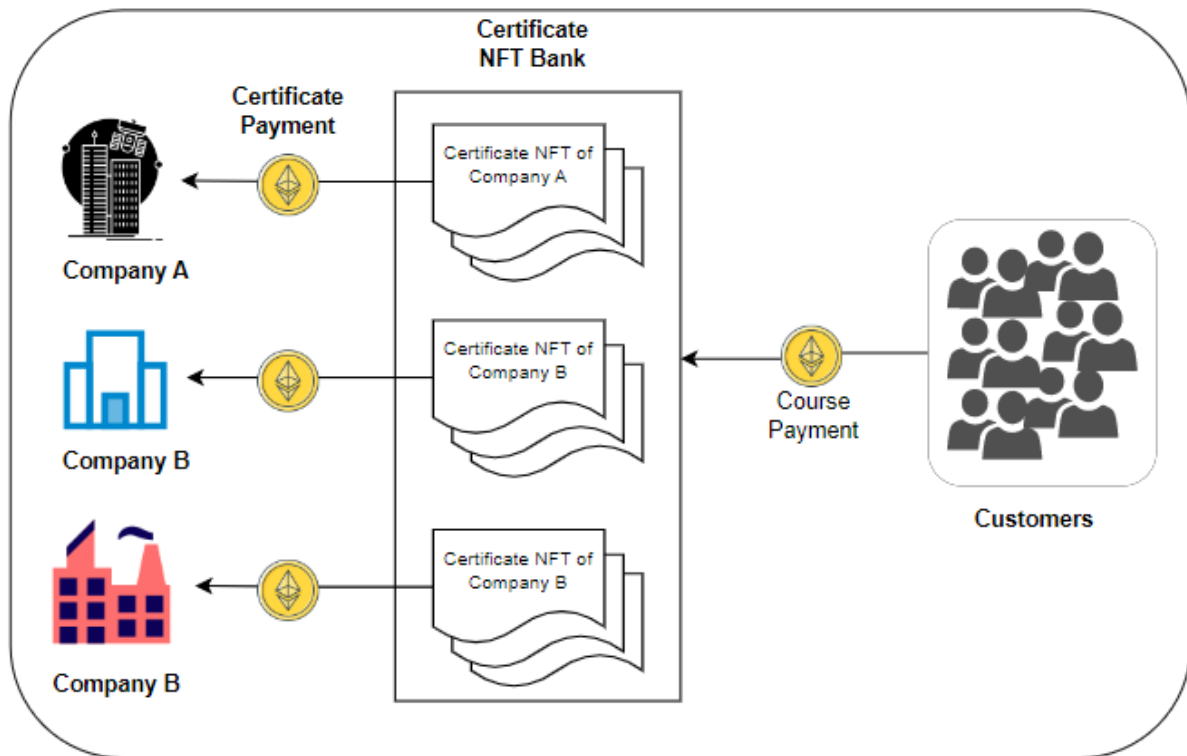


Figure 3. NFT-based certificate generation and sale

As shown in Figure 3, customers are expected to make payment for the course they have registered for. Upon successfully completing the course, NFT-based certificates created by the companies are delivered to the customers. As shown in Figure 4, the proposed system consists of four stages. The initial steps taken by the company that produces NFT certificates are shown in the first stage. The company registers to the system, undergoes identity verification, and gains the right to obtain NFT certificates from the NFT production platform. This enables the company to provide certificates to users who are eligible to receive them. In the second stage, the steps taken by the customer who registers to the system are displayed. The customer registers to the system and undergoes identity verification. After completing the courses created by the companies, the customer becomes eligible to receive an NFT certificate. The third stage involves the creation and distribution of the smart contract. The fourth stage shows the area where external certificates that need to be stored are stored, which is IPFS, and the blockchain that will provide traceability for the certificates. In the proposed method, the stages are planned to be carried out interactively rather than discretely.

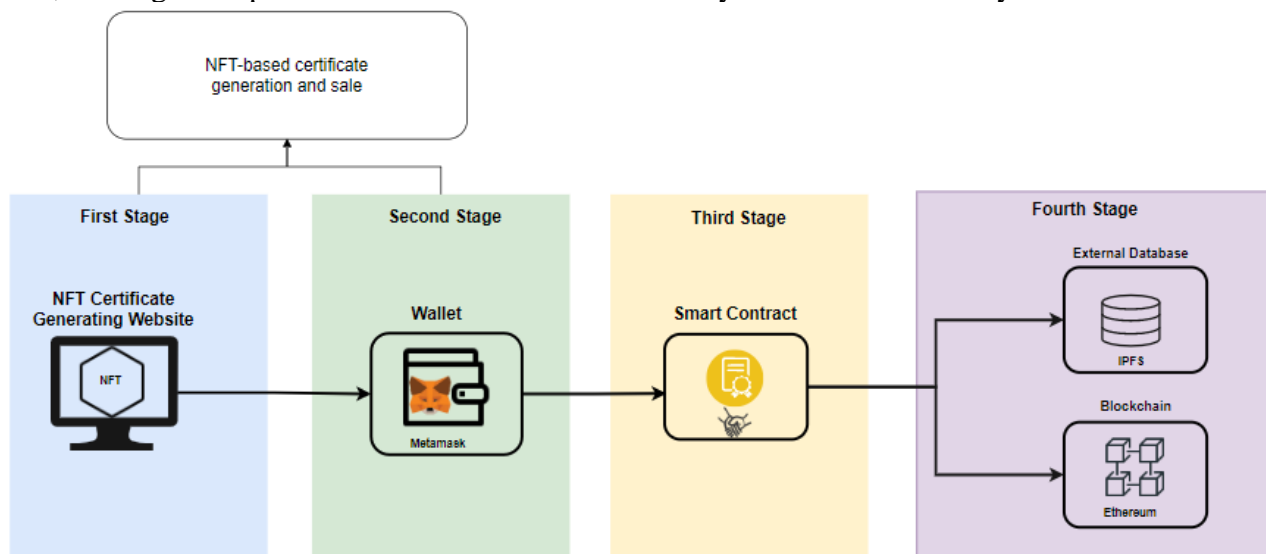


Figure 4. Block diagram of the proposed method

As shown in Figure 5, in the first stage, the company/institution obtains the necessary balance to operate on the Ethereum network and acquires Ether cryptocurrency by creating a wallet on the Ethereum blockchain. Then, it connects to the project-specific website with its Ethereum wallet. By connecting to the website, the company/institution creates its profile and submits it to the project website for verification purposes. After the verification of the company/institution's profile, it becomes ready to produce certificates.

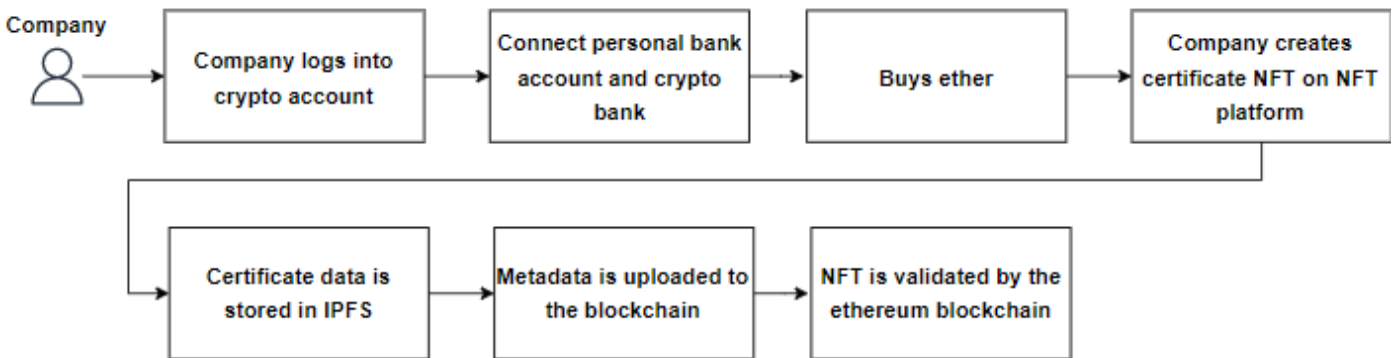


Figure 5. The first stage of the proposed method

As shown in Figure 6, in the second stage, individuals are required to create their own blockchain wallet and interact with the website to verify their identity within the legal framework. Users who have verified their identity can link their wallet to the website and have the right to purchase the certificates they deserve.

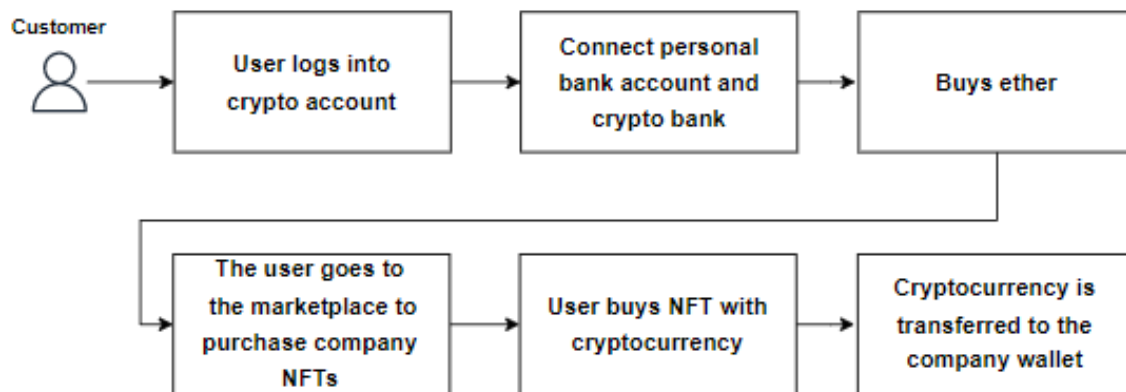


Figure 6. The second stage of the proposed method

As shown in Figure 7, the third stage refers to the smart contract created for the company according to the rules. Here, the transactions made in the first and second stages are executed and consensus is reached. A smart contract is created in accordance with the rules determined by the company, and the transfer of the NFTs to be created is aimed.

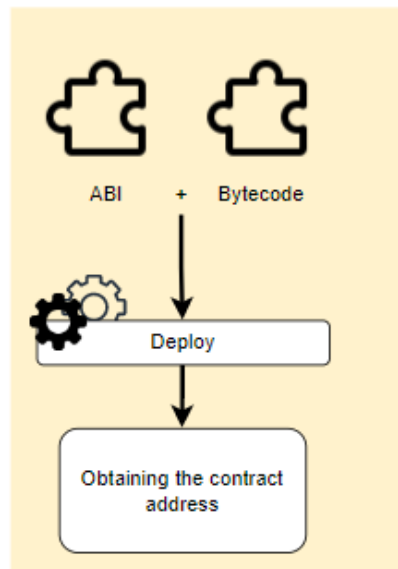


Figure 7. The third stage of the proposed method

As shown in Figure 8, the fourth stage refers to the area where all the meta and other data of the NFTs created in the first stage will be stored. The meta data of the certificates is stored on the blockchain and all the transactions performed on it are tracked, thus controlling the digital movement of the certificates. All versions of the certificates are stored on IPFS, reducing the load on the blockchain and achieving a more efficient system.

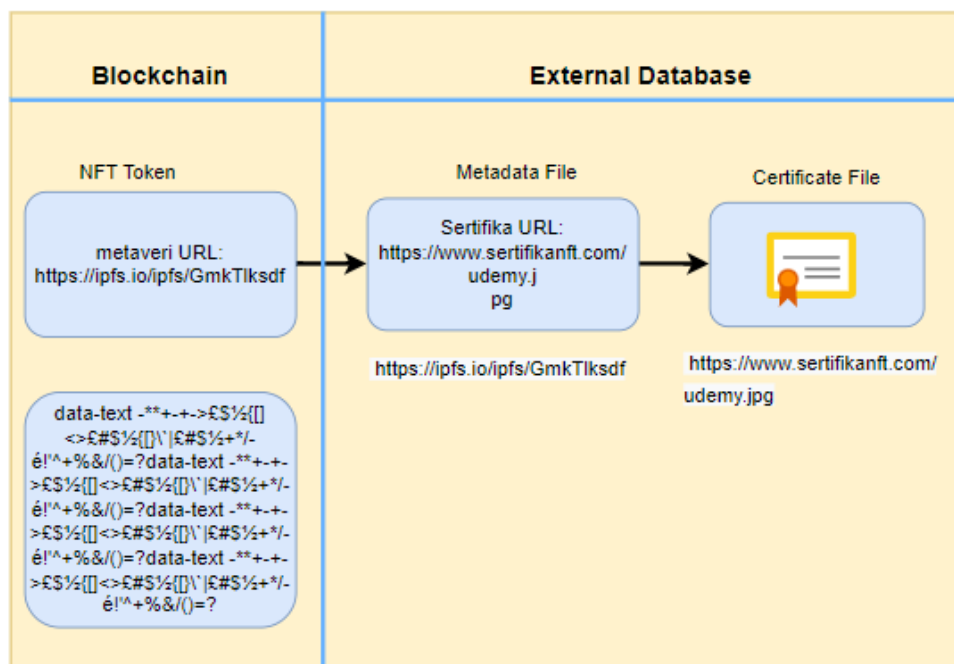


Figure 8. The fourth stage of the proposed method

4. Discussions and Future Work

One of the risks that will be encountered in this proposed study is that diploma/certificate holders lose access to their wallets. In the event of this situation, it is planned to destroy the certificates belonging to the person in the blockchain environment and to issue the same certificates to a new wallet that will be created. Another risky situation is the creation of title deeds similar to the Non-Transferable Intellectual Deed created for certificate/diploma purposes. As a solution to this situation, the website to be created will be subject to authentication of certificate/diploma creators. In addition, the certificate/diploma can only be obtained through the web page. At the same time, people will be able to check the authenticity of their NFTs via the web page.

In future studies, research will be conducted on the optimization and generalization of the fees resulting from the production of NFT-based certificates. It is planned that the system created at the end of the study will

be ready to be used in institutions and organizations. In case the foreseen part is realized successfully, it is planned to take the project to the next level and use the user certificates and diplomas as a validator in official applications.

5. Conclusions

Blockchain technology has become quite popular in today's world with the opportunities it provides. One of these opportunities, NFT, is gaining attention with its evolving structure. In this proposed study, the issue of certificate security, which is one of the problems of the digital world, has been emphasized. The misuse and fraudulent production of increasing certificates have led to the problem of certificate authenticity. The aim of this study is to ensure the security and traceability of certificates in the digital environment using blockchain and NFT technologies. The non-fungible and unique nature of NFTs is seen as a solution to copyright and data security problems of certificates. In addition, NFTs provide tamper-resistant certificates and easy verification. In our future study, we plan to make a real-time application of this proposed method. Fees are charged for transactions performed on the Ethereum blockchain. These fees have not been considered in this study.

Funding

This research is supported by the 1919B012223104 project fund provided by the Scientific and Technological Research Council of Turkey (TUBITAK).

References

- [1] Gu, Z. Yin, C. Cui, and Y. Li, "Integrated Functional Safety and Security Diagnosis Mechanism of CPS Based on Blockchain," *IEEE Access*, vol. 8, pp. 15241–15255, 2020, doi: 10.1109/aACCESS.2020.2967453.
- [2] M. Mindas, "Edited by Dariusz Plinta Advanced Industrial Engineering," no. December 2016, 2020.
- [3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85.
- [4] X. Li, "An evolutionary game-theoretic analysis of enterprise information security investment based on information sharing platform," *Managerial and Decision Economics*, vol. 43, no. 3, pp. 595–606, 2022, doi: 10.1002/mde.3404.
- [5] A. Kurnaz, "A Review on Usage Areas of Blockchain Technology in Architecture," *International Journal of Scientific and Technological Research*, no. June, 2021, doi: 10.7176/jstr/7-04-07.
- [6] G. Karame, M. Huth, C. Vishik, and M. Huth, "An overview of blockchain science and engineering," pp. 1–5, 2020.
- [7] A. Nawawi, I. Makarov, and A. Plastun, "Applications of Blockchain Technology beyond Cryptocurrency," *Finance Research Letters*, vol. 11, no. 2, pp. 1–6, 2019.
- [8] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Computer Law and Security Review*, vol. 34, no. 3, pp. 550–561, 2018, doi: 10.1016/j.clsr.2017.11.008.
- [9] M. Finck and V. Moscon, "Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0," *IIC International Review of Intellectual Property and Competition Law*, vol. 50, no. 1, pp. 77–108, 2019, doi: 10.1007/s40319-018-00776-8.
- [10] Sina Osivand, "Smart collectibles; use case of NFT tokens," *Open Access Research Journal of Engineering and Technology*, vol. 1, no. 2, pp. 024–031, 2021, doi: 10.53022/oarjet.2021.1.2.0113.
- [11] G. Grolleau, T. Lakhal, and N. Mzoughi, "An introduction to the economics of fake degrees," *Journal of Economic Issues*, vol. 42, no. 3, pp. 673–694, 2008, doi: 10.1080/00213624.2008.11507173.
- [12] S. Bian, G. Shen, Z. Huang, Y. Yang, J. Li, and X. Zhang, "PABC: A Patent Application System Based on Blockchain," *IEEE Access*, vol. 9, pp. 4199–4210, 2020, doi: 10.1109/ACCESS.2020.3048004.
- [13] B. Singhal, G. Dhameja, and P. S. Panda, *Beginning Blockchain*. 2018. doi: 10.1007/978-1-4842-3444-0.
- [14] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," <https://bitcoin.org/tr/>, vol. 15, no. 4, pp. 580–596, 2008.

- [15] M. Baygin, O. Yaman, N. Baygin, and M. Karakose, "A blockchain-based approach to smart cargo transportation using UHF RFID," *Expert Syst Appl*, vol. 188, Feb. 2022, doi: 10.1016/j.eswa.2021.116030.
- [16] T. Tuncer and S. Dogan, "Quantum-Dot Cellular Automata based Fragile Watermarking Method for Tamper Detection using Chaos," *International Journal of Information Technology and Computer Science*, vol. 10, no. 12, pp. 27–32, Dec. 2018, doi: 10.5815/ijitcs.2018.12.04.
- [17] T. TUNCER, "Analysis of CRT-based Watermarking Technique for Authentication of Multimedia Content," *International Journal of Computer Network and Information Security*, vol. 10, no. 6, pp. 60–67, Jun. 2018, doi: 10.5815/ijcnis.2018.06.06.
- [18] H. Yetis, M. Karakose, and N. Baygin, "Blockchain-based mass customization framework using optimized production management for industry 4.0 applications," *Engineering Science and Technology, an International Journal*, vol. 36, Dec. 2022, doi: 10.1016/j.jestch.2022.101151.
- [19] O. Yaman, T. Tuncer, and F. Ertam, "Automated book location and classification method using RFID tags for smart libraries," *Microprocess Microsyst*, vol. 87, p. 104388, 2021.
- [20] D. Ghelani, "What is Non-fungible token (NFT)? A short discussion about NFT Terms used in NFT," *Authorea*, 2022.
- [21] B. Vitalik, "Soulbound," 2022. <https://vitalik.ca/general/2022/01/26/soulbound.html>