Bitlis Eren Üniversitesi Fen Bilimleri Dergisi
BİTLİS EREN UNIVERSITY JOURNAL OF SCIENCE
ISSN: 2147-3129/e-ISSN: 2147-3188
VOLUME: 12 NO: 4 PAGE: 1128-1138 YEAR: 2023
DOI:10.17798/bitlisfen.1343747

Digital Certificate Security: A Blockchain-based Approach for Fraud Prevention and Verification

Nihat ZAMAN[1], Işıl KARABEY AKSAKALLI[1], Nursena BAYĞIN[1*]

[1]*Department of Computer Engineering, Erzurum Technical University, 25000 Erzurum, Türkiye (ORCID: 0009-0001-6061-1482) (ORCID: 0000-0002-4156-9098) (ORCID: 0000-0003-4457-5503)*

Keywords: Blockchain, Digital Certificate, NFT, Smart Contract.

Abstract

With the rise of digitalization and increased internet usage, digital certificates' security issues have gained significant importance. The utilization of counterfeit certificates can lead to deceptive identity and capability verifications, allowing untrustworthy individuals to assume misleading positions. Simultaneously, factors such as data leaks and technical glitches can jeopardize the security of certificates. These challenges can complicate talent verification processes and result in unsuitable individuals being placed in incorrect roles. The proposed work aims to thwart forged certificates and ensure their verifiability within this context. The methodology employed in the study strives to mitigate potential data loss or accessibility problems by adopting a decentralized storage structure. The primary objective is to establish certificates that are reliable, traceable, and capable of being verified. A rapid and efficient user interface was developed using React.js to achieve this aim. Smart contracts were scripted on the Ethereum blockchain using Solidity, and data, including user information and certificate details, were stored within components like MongoDB. In the phase of practical implementation, diverse scenarios have been designed to facilitate the generation, verification, and monitoring of certificates. The proposed approach is geared towards deterring forgery and enhancing the credibility of certificates. Through this system, users and organizations can authenticate certificates and prevent the proliferation of counterfeit ones. Furthermore, the enhanced security and ease of sharing certificates on digital platforms offer substantial advantages to certificate holders. In summary, this study strives to enhance the safeguarding and dependability of certificates by addressing the security concerns posed by the era of digitalization.

1. Introduction

The initial utilization of blockchain technology commenced with Bitcoin. Bitcoin, the pioneering blockchain, was introduced in 2008 by an anonymous individual or group using the pseudonym Satoshi Nakamoto [1]. Nakamoto delineated Bitcoin as a "P2P electronic cash system." The published paper on Bitcoin highlights four fundamental attributes: traceability of transactions accessible to all, execution of immutable and secure transactions, peer-to-peer (P2P) transactions, and decentralized management [2].

With the emergence of Bitcoin and the acknowledgment of cryptocurrency, the concept of blockchain has garnered broader recognition. Subsequent to Bitcoin, another blockchain known as Ethereum was developed. Ethereum is conceived as a platform that fosters applications and smart contracts on the blockchain, alongside its own native cryptocurrency. This expansion has led to the utilization of blockchain in various domains beyond cryptocurrencies. Presently, blockchain finds extensive application, particularly in systems necessitating enhanced security. Furthermore, blockchain technology is intricately linked with

*Corresponding author: nursena.baygin@erzurum.edu.tr
Received: 15.08.2023, Accepted: 31.10.2023

various domains, including but not limited to personal asset registration, document archival, survey or election processes, the financial industry, payment transactions, fund transfers, trading platforms, exchange administration, authorization, validation, digital identity oversight, and document control [3-5]. In recent years, alongside established blockchains like Ethereum and Bitcoin, numerous novel blockchains and cryptocurrencies have emerged. Consequently, the number of individuals engaging with blockchains continues to grow. The user count, which stood at 106 million in 2020, surpassed 295 million in 2021. Based on projections, this figure is anticipated to exceed 1 billion by the conclusion of 2022 [6].

Web 2.0 is the collective term for a version of the internet that is familiar to many people today. The primary objective of Web 2.0 companies is to deliver services to users by converting the vast amount of user-generated big data into meaningful insights. On the contrary, Web 3.0 represents an evolution of Web 2.0 applications onto the blockchain, an architecture that places a significant emphasis on decentralized personal data and individual privacy, without any form of monopoly. Recent incidents of user data breaches have heightened interest in the features offered by Web 3.0. One of the Web 3.0 tools developed on the Ethereum platform is non-fungible tokens (NFT). NFTs play a crucial role in decentralizing the network, with a primary focus on establishing ownership rights. For instance, early adopters of an emerging network may be granted an NFT that serves as evidence of their initial use of the network. However, since NFTs are transferable, the holder has the option to transfer it even to individuals who have never used it. The introduction of NFTs enables a reliable determination of ownership and affiliation on the blockchain [7-9]. In this context, some studies in the literature are summarized in Table 1.

Table 1. NFT based certification studies in literature

Author(s)	Year	Objective	Contributions	Limitations
Alnuaimi et al. [10]	2022	Securing precious stones digitally	Digital certification of NFT-based jewelry and precious stones provides proof of information such as proof of ownership, sales history, bidding and quality	Since the proposed system is a decentralized application, it creates additional overhead. Latency, which is a general characteristic of the Ethereum network, was encountered
Murugavel et al. [11]	2023	Reducing the use of forged certificates using Polygon blockchain and NFT	Certificate printing is provided on a single platform. Additionally, the costs of transactions have been reduced by using Polygon	The application requires a central administration to obtain certificates from all organizations. This is against the logic of blockchain
Tahlil et al. [12]	2022	Developing an attack-resistant certificate application by preventing identity fraud in education	An NFT-based certificate security, transcript verification, self-sovereign (SSI) prototype has been developed	NFT may cause undesirable consequences as a result of its ability to transfer ownership to those who do not have a certificate
Nikolic et al. [13]	2022	Creating a blockchain-based digital certificate school management system and keeping information about certificates and participants and events	The certificates were stored in the Polygon Supernets blockchain and given to students in the form of NFT	NFT transfer is an important problem and it has been emphasized that it will be overcome with Soulbound tokens
Allwinnaldo et al. [14]	2023	Ensuring the security of digital certificates indicating the authenticity of exotic fish	It is aimed to prevent fraud in the exotic fish industry by producing NFT-based certificates. A cost-effective and efficient system is offered to users.	While blockchain provides security, it has given additional system costs to all nodes.

In this proposed study, our goal is to develop a system that integrates blockchain technology and NFTs to monitor and validate certificate ownership within a digital setting, all the while maintaining the security of these certificates. The system addresses the need for transparency and security by harnessing the advantages of blockchain technology. This approach aims to tackle the challenge of ensuring global certificate security and verifiability through the utilization of blockchain's transferable intellectual property capabilities. The research gaps observed as a result of the literature reviews are as follows:

- Certificate issuance and control mechanisms at the global level are inadequate. In addition, the security of existing certificates is uncertain.
- There are significant problems in certificate verification and recognition across countries and regions. The establishment of a blockchain-based certificate verification mechanism has the potential to contribute to the development of international cooperation and standards.
- One of the most important problems globally is the issuance and dissemination of counterfeit certificates. With certificates that can be verified from a single point, it is quite possible to prevent these situations.

In this context the following provides a concise overview of the key contributions and motivations behind our proposed approach.

- The aim is to utilize the blockchain to store certificates containing non-transferable qualified intellectual property.
- The objective is to authenticate users' and institutions' identities and link the resulting certificates to users' blockchain wallets.
- By creating a unified system, institutions can securely access individuals' NFT certificates and diplomas, effectively preventing the circulation of counterfeit credentials.
- The goal is to evaluate the existing paper diploma storage and verification methods and improve their effectiveness by transitioning to a blockchain-based environment.
- The systems and tools utilized by counterfeit certificate producers should be analyzed, necessary precautions should be implemented, and these vulnerabilities should be eradicated.
- The aim is to amass user certificates within a decentralized framework and integrate institutions, organizations, and users worldwide into this system.

The rest of this manuscript is organized in a subsequent manner: Section 2 delves into an exhaustive examination of the scholarly literature concerning blockchain and NFT, the pivotal technological components underpinning the scope of this pertinent study. Section 3 outlines the proposed methodology and includes visual depictions of the implementation. Section 4 furnishes the outcomes attained through the proposed approach.

2. Technical Component

With the integration of blockchain technology into our daily lives, numerous distinct and novel terms have arisen. This section elucidates the definitions of blockchain terminology and qualified intellectual property terms to enhance comprehension of the study.

2.1. Terminology of Blockchain

The notion of blockchain surfaced subsequent to the release of the Bitcoin paper. In Bitcoin [2], Satoshi Nakamoto opted for the term "proof-of-work chain" instead of blockchain. The terminologies associated with blockchain, including many others, were initially explored in the Ethereum White Paper. This section offers a comprehensive outline of blockchain terminology.

2.1.1. Block Description and Transaction Approval

A block is a segment that contains portions of data from valid transactions conducted on the chain. Within a block:

- Once the block is mined
- The blockchain's length in blocks
- Minimum gas fee needed to include the transaction in the block
- Effort needed to remove the block
- Distinct identifier for the block
- Distinct identifier of the preceding block
- Transactions encompassed within the block
- A password demonstrating the block's successful completion of the proof of stake [3, 15, 16].

Blockchain technology derives its name from its function of storing verified transaction records in blocks. A blockchain is basically composed of two key elements: validators and users. As shown in Figure 1, a user requests a transaction to the blockchain. The transaction is

broadcast and, if verified, is added to the ledger by validation nodes. Once validated, the block is sent to validators for authorization. The first validator to authorize the transaction gets the right to create the corresponding block. When the block is subsequently validated by other validators, the transaction is recorded in a block within the blockchain and added to the chain.

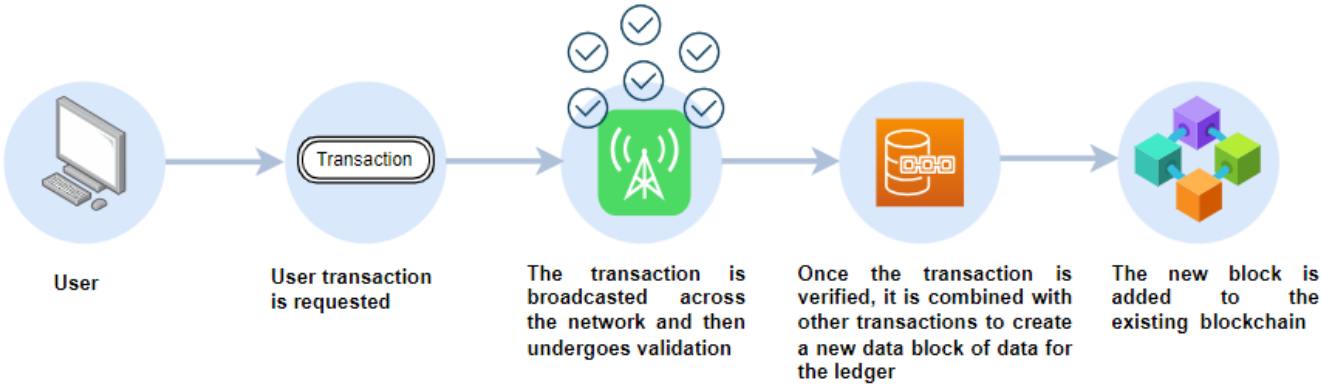

Figure 1. The working principle of blockchain

2.1.2. Address and Transaction

An "address" is a publicly accessible combination of alphanumeric characters enabling communication between blockchain users and smart contracts [17]. A "transaction" constitutes a fundamental element within the blockchain framework, denoting transfers or actions occurring within the chain [18].

2.1.3. Ledger

A ledger represents a heightened level of secure transfer, transitioning traditional accounting ledgers into the blockchain realm. This ledger serves as the repository for recording network transactions, rendering any alteration or deletion of ledger transactions impossible; a pivotal facet emblematic of blockchain technology [17, 19].

2.1.3. Smart Contract

Smart contracts are decentralized applications that execute automated transactions based on data and functions within the blockchain, following regulations defined by the contract's creators [17, 20].

2.2. Key Features of Blockchain

In the Bitcoin article authored by Satoshi Nakamoto, the foundational principles of the blockchain on which Bitcoin is constructed were elucidated [2]. These principles are outlined as follows:

2.2.1. Decentralized

In contrast to the conventional monetary system, where transactions frequently require endorsement from regulatory entities such as governments and financial institutions, blockchain technology introduces a distinct paradigm. Transactions executed on the blockchain solely necessitate validation from the involved users. This approach guarantees the security and resilience of blockchain transactions against external interventions [21]. Unlike conventional systems, blockchain operates without centralized authority, upholding data across a distributed network.

2.2.2. Transparency and Traceability

In conventional systems, authorities and diverse institutions exclusively retain the ability to audit all transactions, yet blockchain diverges from this norm. Each transaction conducted within the blockchain framework is archived in a ledger that remains both traceable and immutable to all [21]. This fosters an environment wherein all participants gain visibility into and real-time monitoring of their transaction history.

2.2.3. Immutability

Each transaction executed within the blockchain is meticulously documented through a mechanism known as a ledger. Subsequently, this ledger is employed to incorporate these transactions into blocks. The incorporated transactions become indelibly ensconced within the blockchain, impervious to any form of alteration or reversal.

This characteristic not only substantiates the dependability of blockchain transactions but also safeguards an incontrovertible chronicle of the conducted transactions [21, 22].

2.2.4. Anonymity

In centralized systems, individuals are required to divulge their personal data for the execution of transactions. In contrast, blockchain technology operates differently, as transactions within the network do not necessitate authentication [21, 23].

2.3. NFT

NFTs (Non-Fungible Tokens) are a category of cryptocurrencies that originate from Ethereum smart contracts. They were initially introduced in Ethereum Improvement Proposals (EIP)-721 and subsequently refined in EIP-1155. NFTs distinguish themselves from conventional cryptocurrencies like Bitcoin, which are considered fungible, with all units being identical. In contrast, NFTs possess unique characteristics and are immutable, enabling them to represent distinct digital assets [24]. Due to their creation on a decentralized blockchain, NFT authenticity can only be reliably verified within decentralized applications. This circumstance has led to the emergence of counterfeit NFTs sharing the same name and image, potentially deceiving individuals. NFTs are generated through smart contracts, which are integrated into the blockchain for public interaction. However, security vulnerabilities within the code of a smart contract can jeopardize the integrity of NFTs and the wallets of their holders. A viable solution to mitigate this risk is to subject the smart contract to cybersecurity assessments. Regrettably, this solution incurs substantial costs that many NFT projects and creators choose to evade, thereby compromising user security.

3. Proposed Method

This paper presents the development of a certification and verification system utilizing non-transferable tokens (NTT) on the blockchain. The previously introduced theoretical concept is realized through real-time implementation in this study [25]. Within the framework of this research, an examination of trends in the realm of NFT (Non-Fungible Token) and NTT is conducted, accompanied by a comprehensive review of related technological efforts. Analyses are conducted to comprehend the challenges associated with counterfeit certificate creation and the predicaments faced by victims of such fraudulent certificates. Concurrently, the foundational principles for our decentralized system are established.

The purpose of this system is to safeguard stored data, counteract counterfeit diplomas and certificates, and ensure the security of companies and institutions involved in the certification process. Operating on the Ethereum platform, this system employs the ERC-721 [5] non-fungible token standard for the creation of certificates. Both certificate issuers and recipients are mandated to verify their personal or organizational identities in adherence to legal obligations. This proposed methodology effectively curbs the proliferation of fake certificates and diplomas, as individuals and entities undergo the authentication process.

As can be seen in Figure 2, within the proposed methodology, a smart contract is generated by the organization, laying out the requisite conditions. Subsequently, users slated to obtain certificates are attributed with unique identities. Upon successful completion of their respective examinations, certificates are formulated and endorsed by the organization. Ultimately, certificates are dispensed to duly eligible users.

The following steps were performed in the proposed study:

- A comprehensive analysis of fundamental state functions and ongoing trends within the blockchain domain has been conducted.
- The advantages exploited by malevolent actors engaged in the production of counterfeit certificates/diplomas, as well as the challenges confronted by individuals and organizations falling victim to fraudulent credentials, have been thoroughly examined.
- The architecture, design concepts, and algorithmic structure intended for the creation of the decentralized website within this study have been determined.
- Appropriate methodologies have been formulated to facilitate the effective utilization of the blockchain environment by institutions/organizations and individuals.
- Strategic measures to ensure the global availability and accessibility of the developed system have been meticulously calculated.

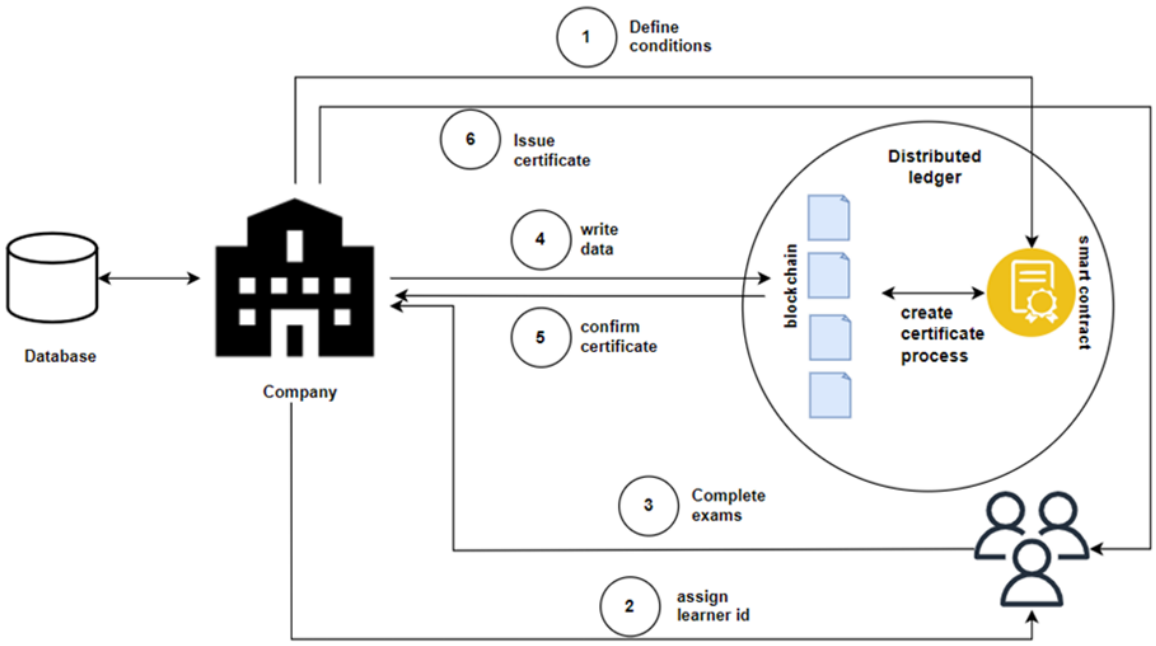

Figure 2. Diagram of the proposed method

The details of the proposed method are given below under subheadings.

3.1. Back-end of the Application

In this research, a novel blockchain-based solution is presented for digital certificate security. The main objective of the proposed model is fraud prevention and certificate verification processes for this purpose. The first phase of this blockchain-based model is the realization of the back-end component. The back-end component of the model developed to ensure digital certificate security basically consists of 4 main parts. These are certificate generation, certificate verification, certificate monitoring and main program respectively. At this point, a pseudocode for the certificate generation phase is given in Algorithm 1.

Algorithm 1. Create Certificate Function

Input: User Information and Certificate Details. **Output:** Blockchain Transaction ID.
1: COMBINE the user information and certificate details into a single certificate structure. 2: ADD a timestamp to the certificate to mark the current time. 3: SAVE the certificate onto the blockchain. 4: RECORD the transaction made on the blockchain when saving the certificate. 5: RETURN the recorded transaction ID.

As can be seen from Algorithm 1, the system takes user information and certificate details as input parameters. After that, the certificate is created using the user information, certificate details (content, etc.) and the current time stamp information. The generated certificate is registered to the blockchain and the transaction id information received after the registration process is completed is returned. The second phase of the model is certificate verification. This process is given in Algorithm 2.

Algorithm 2. Certificate Verification

Input: Certificate and Issuer Public Key. **Output:** Valid or Non-Valid.
1: // Verify the authenticity of the certificate using the issuer's public key. 2: IF Blockchain.VerifySignature(certificate, issuerPublicKey) is true 3: RETURN "Certificate is valid" 4: ELSE 5: RETURN "Certificate is not valid" 6: END IF

As given in Algorithm-2, the certificate verification function takes the certificate information and the issuer's public key as input parameters. Afterwards, the signature verification process is performed and the result of this process returns the certificate's validation/non-validation status. The third phase of the application is certificate monitoring, the pseudocode for which is given in Algorithm 3.

Algorithm 3. Certificate Monitoring

Input: All Certificate. **Output:** Monitoring Action.
1: // Retrieve and monitor certificates stored on the blockchain. 2: certificates = Blockchain.GetCertificates() 3: // Iterate through the list of certificates 4: FOR EACH certificate IN certificates 5: // Perform monitoring actions, if needed 6: END FOR

As shown in Algorithm 3, certificate monitoring involves reading all certificates in the network and traversing them through a loop. During the traversal, if necessary, the required operations are performed on the certificate. The section where the model is tested is the main function. A sample pseudocode covering a sample certificate generation and submission/verification to the network is given in Algorithm 4.

Algorithm 4. Main Function

Input: User Information, Certificate Detail and Issuer Public Key. **Output:** Storage Approval.
1: userInformation = {name: "Test Test", email: "testtest@test.com"}. 2: certificateDetails = {type: "Professional Certification", issuer: "Organization Test"} 3: issuerPublicKey = "0xissuerPublicKey1234" 4: // Create a certificate using user information and certificate details 5:certificateTransaction= CreateCertificate(userInformation, certificateDetails) 6: // Verify the certificate's authenticity using the issuer's public key 7:verificationResult= VerifyCertificate(certificateTransaction, issuerPublicKey) 8: // Check the verification result and print a corresponding message 9: IF verificationResult equals "Certificate is valid" 10: THEN 11: PRINT "Certificate is valid and has been stored on the blockchain." 12: ELSE 13: PRINT "Certificate is not valid or has not been stored correctly." 14: END IF

Algorithm 4 basically illustrates a certificate generation and verification activity. As mentioned at the beginning of this section, the back-end of the blockchain application consists of four phases. These phases are given in Algorithms 1, 2, 3 and 4 respectively.

3.2. Front- end of the Application

In this section, we detail the technologies used for the front end of the proposed method, its components, and the implemented design.

3.2.1. Front-end Components

The proposed method requires a powerful front end to facilitate user interaction and visualize data effectively. For this purpose, the React.js library was utilized for front-end development. React.js offers a component-based approach to building user interfaces (UI). This makes the code reusable and easier to manage. Each component has its own state and logic, and when the state of a component in the UI changes, React.js automatically redraws that component.

The front end is structured using a component hierarchy, which follows a modular arrangement. This approach enables primary components to be composed of various sub-components. This hierarchical structure facilitates the independent and isolated functioning of components, contributing to better code manageability and reduced potential for errors. The design and styling aspects are handled using the Tailwind CSS library, which offers extensive design customization and rapid prototyping capabilities. Additionally, the Axios library is employed for facilitating data exchange between the front end and back end. Axios serves as a tool for managing HTTP requests and establishing effective communication with the server side. API requests are utilized for data retrieval, creation, updating, and deletion purposes. Through this integrated framework, the proposed methodology operates efficiently and in an organized manner.

3.2.2. User Interface

The user interface has been meticulously crafted to facilitate the seamless creation and validation of certificates by users. The entire spectrum of user transactions is planned to be overseen through a user-friendly and intuitive interface, ensuring a smooth experience. The interface shown in Figure

3 has been tailored for companies seeking to establish project pages and distribute certificates to applicants. Upon inputting the necessary project details, the application undergoes submission to the administrator for evaluation. Upon successful completion of the application process, the company becomes eligible to dispense certificates. This design approach ensures a comprehensive and user-centric experience within the proposed system.

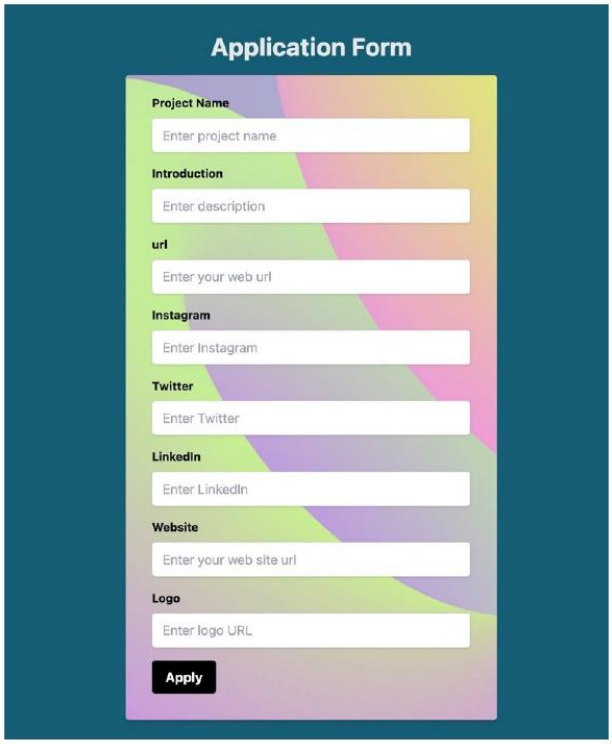

Figure 3. Project creation form

The interface depicted in Figure 4 showcases the roster of active certificate-issuing companies within the platform established in alignment with the proposed methodology. This designated page empowers users to peruse certificates by navigating to the respective project page from which they intend to acquire a certificate. As illustrated in Figure 5, the company page interface provides comprehensive insights into a company's particulars and the array of certificates it has issued. This dynamic interface design augments user accessibility and engagement, bolstering the efficacy of the proposed approach. Figure 6 shows an image of the certificate acquisition page. On this page, users are able to take ownership of the certificate reserved for them.

Figure 4. Active certificate page

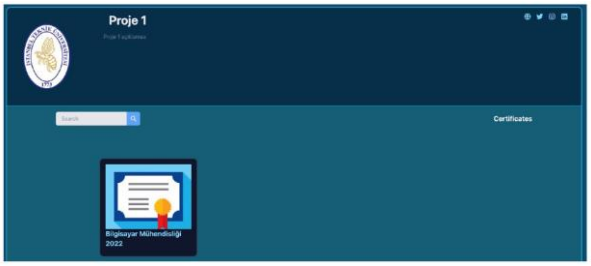

Figure 5. Company page interface design

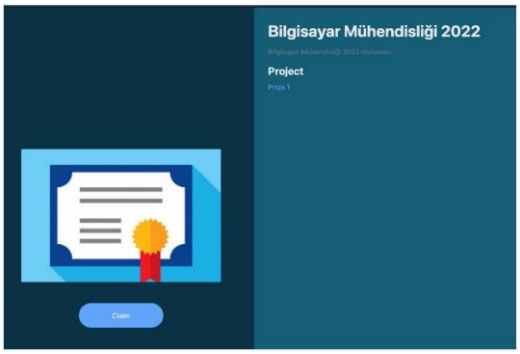

Figure 6. Certification page

3.2.3. Database and Data Management

This section furnishes details concerning the server-side components employed in the suggested approach and the underlying technologies utilized. The server side constitutes a pivotal facet of the proposed methodology, encompassing data processing and the implementation of business logic. Throughout this process, technologies such as Node.js and the Express library are harnessed. Node.js serves as a JavaScript-based environment that facilitates server-side processing, while the Express library functions as a conduit bridging the gap between the front-end and server-side for web applications. Moreover, the API (Application Programming Interface) architecture facilitates seamless data communication between the server and the client.

Database management is one of the most important components of the proposed work. The data needs of the project were met using the MongoDB database. MongoDB is a document-based NoSQL database and offers a flexible data model that suits the requirements of the project. In our data model, separate collections were created

for users, projects, certificates and other related data. Figure 7 shows the tables in the database. These tables contain the assets necessary for the website to fulfill its function.

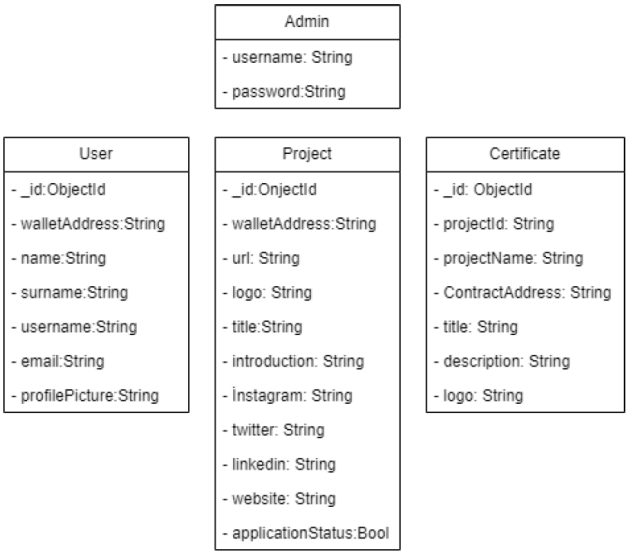

Figure 7. Database table of the proposed method

In this application, a decentralized storage structure is adopted. The reasons for choosing decentralized storage structure instead of centralized storage are given below:

- *Reliability:* In distributed storage systems, data is replicated across multiple nodes. This minimizes the risk of data loss.
- *High Security:* Data is encrypted in the distributed storage structure. In this way, unauthorized access to data is restricted and data integrity is ensured.
- *Scalability:* Distributed storage structure allows more data to be easily added to the system. With this structure, growth requirements can be realized.
- *Compatibility:* The distributed storage approach is compatible with blockchain technologies. This solution increases the security and verifiability of certificates.
- *Low Cost:* Unlike centralized server infrastructures, distributed storage enables effective use of available resources.
- *Continuity:* A problem that may occur in centralized servers can affect the entire system. In the distributed storage approach, independence is provided against possible problems. Because data is copied to many nodes.

3.2.4. Used Packages and Development Tools

Several libraries and packages were employed in the development of the proposed methodology. These libraries played a pivotal role in ensuring an efficient and user-friendly implementation of the proposed approach. Additionally, various development tools were utilized to test and effectively utilize the aforementioned packages and libraries.

Libraries and Packages

ThirdWeb: This package is used to realize the blockchain connection on the website. This package includes structures that facilitate the use of blockchain actions on the website.

Axios: Axios package was used to realize the data communication between the server side and the front end. Axios provides the communication of the tables created on the server side with the front-end thanks to the functions it contains.

React DataTable: React DataTable library is used to create tables and organize data.

React Carousel: React Carousel library was used to create the component with informative visuals on the home page.

4. Conclusion

The proposed methodology aims to mitigate the proliferation of counterfeit certificates and establish a robust verification system. The existence of fraudulent certificates complicates talent verification processes and may lead to the appointment of ill-suited individuals to deceptive positions. The primary objective of this methodology is to address this issue and ensure the trustworthiness, traceability, and verifiability of certificates. To achieve this goal, the methodology is crafted using three core components: React.js for the user interface, Solidity for crafting smart contracts on the Ethereum blockchain, and MongoDB for the storage and management of user data, certificate particulars, and organizational details. Throughout the implementation phase of the approach, diverse usage scenarios were identified for certificate generation, verification, and monitoring. System administrator users possess the ability to assess applications and conduct Know Your Customer (KYC) procedures. Project participants have the capability to create certificates by linking their blockchain wallets to the web platform. Meanwhile, regular users can connect their blockchain wallets to input their

profile data and generate their certificates. The primary aim of the proposed method is to elevate the reliability of certificates and furnish safeguards against fraudulent activities. Thanks to the integration of blockchain technology, every facet of the certificate lifecycle becomes traceable, and smart contracts facilitate the secure creation and verification of certificates. Through this system, both users and organizations can validate certificates, thwarting the proliferation of counterfeit documentation. One potential repercussion of this method is a reduction in the risk of forgery during job applications and talent verification procedures, streamlining the process of recruiting individuals with the requisite skills. Moreover, certificates can be shared and authenticated more seamlessly in digital realms, engendering greater confidence and assurance among certificate holders.

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

Ethics: There are no ethical issues after the publication of this manuscript.

References

[1] S. Ghimire and H. Selvaraj, "A survey on bitcoin cryptocurrency and its mining," 2018: *IEEE*, pp. 1-6.
[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, 2008.
[3] A. Gorkhali, L. Li, and A. Shrestha, "Blockchain: A literature review," *Journal of Management Analytics*, vol. 7, no. 3, pp. 321-343, 2020.
[4] A. Kurnaz, "A Review on Usage Areas of Blockchain Technology in Architecture," *International Journal of Scientific and Technological Research*, no, 2021.
[5] M. K. Shrivas and T. Yeboah, "The disruptive blockchain: types, platforms and applications," *Texila International Journal of Academic Research*, vol. 3, pp. 17-39, 2019.
[6] crypto.com. "Crypto Market Sizing Report 2021 and 2022 Forecast." crypto.com. https://crypto.com/research/2021-crypto-market-sizing-report-2022-forecast (accessed 2023).
[7] S. Osivand, "Smart collectibles; use case of NFT tokens," *Open Access Research Journal of Engineering and Technology*, vol. 1, no. 2, pp. 024-031, 2021.
[8] S. M. H. Bamakan, N. Nezhadsistani, O. Bodaghi, and Q. Qu, "A decentralized framework for patents and intellectual property as nft in blockchain networks," 2021.
[9] D. Ghelani, "What is Non-fungible token (NFT)? A short discussion about NFT Terms used in NFT," Authorea Preprints, 2022.
[10] N. Alnuaimi, A. Almemari, M. Madine, K. Salah, H. Al Breiki, and R. Jayaraman, "NFT Certificates and Proof of Delivery for Fine Jewelry and Gemstones," *IEEE Access*, vol. 10, pp. 101263-101275, 2022.
[11] B. Kamaleshwaran, M. Sneha, and S. Kavitha, "Digital Certification–Certification Credential as Non Fungible Token (NFT)," 2023: *IEEE*, pp. 1-7.
[12] T. Tahlil, S. S. Gomasta, and A. B. M. S. Ali, "AlgoCert: Adopt Non-transferable NFT for the Issuance and Verification of Educational Certificates using Algorand Blockchain," 2022: IEEE, pp. 1-8.
[13] S. Nikolić, S. Matić, D. Čapko, S. Vukmirović, and N. Nedić, "Development of a blockchain-based application for digital certificates in education," 2022: *IEEE*, pp. 1-4.
[14] M. R. R. A. Allwinnaldo, R. N. Alief, I. S. Igboanusi, J. M. Lee, and D.-S. Kim, "Advance NFT-Based Digital Certificate for Efficient Exotic Fish Ownership."
[15] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," 2018: *IEEE*, pp. 1-11.
[16] J. Zhang, S. Zhong, T. Wang, H.-C. Chao, and J. Wang, "Blockchain-based systems and applications: a survey," *Journal of Internet Technology*, vol. 21, no. 1, pp. 1-14, 2020.
[17] Ö. Özkan, *Kişisel Verilerin Korunması Hukuku Ve Blokzinciri Teknolojisi Raporu*, Türkiye Bilişim Vakfı. İstanbul: Blockcahin Türkiye, 2019.
[18] S. Gupta and M. Sadoghi, "Blockchain transaction processing," arXiv preprint arXiv:2107.11592, 2021.
[19] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, p. 1198, 2019.

[20] S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed iot network," *IEEE Access*, vol. 9, pp. 13938-13959, 2021.

[21] Ü. Gökhan and Ç. Uluyol, "Blok zinciri teknolojisi," *Bilişim Teknolojileri Dergisi*, vol. 13, no. 2, pp. 167-175, 2020.

[22] F. Hofmann, S. Wurster, E. Ron, and M. Böhmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization," in *2017 Kaleidoscope: Challenges for a Data-Driven Society (ITU K)* 2017.

[23] N. Andola, V. K. Yadav, S. Venkatesan, and S. Verma, "Anonymity on blockchain based e-cash protocols—A survey," *Computer Science Review*, vol. 40, p. 100394, 2021.

[24] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges," arXiv preprint arXiv:2105.07447, 2021.

[25] N. Zaman and N. BayĞIn, "Digital Assurance and Traceability of NFT-based Certificates," *İleri Teknolojilerde Çalışmalar Dergisi*, vol. 1, no. 1, pp. 17-25, 2023.