Acta Scientific COMPUTER SCIENCES

Volume 7 Issue 3 June 2025

Research Article

NFT Marketplace for Decentralized Certificates and Documents Using Blockchain

M Karthick[1]*, M Chandru[2], R Mythili[2], J Sandhika[2] and S Vaishalee2

[1]Associate Professor, Department of Information Technology, Nandha College of Technology, Erode-638 052, Tamilnadu, India

[2]UG Students – Final Year, Department of Information Technology, Nandha College of Technology, Erode 638 052, Tamilnadu, India

***Corresponding Author:** M Karthick, Associate Professor, Department of Information Technology, Nandha College of Technology, Erode-638 052, Tamilnadu, India.

Received: May 09, 2024

Published: May 30, 2025

Abstract

In the digital age, the authenticity and integrity of certificates are paramount. Traditional methods of certificate issuance and verification often face challenges such as fraud, inefficiency, and lack of transparency. Blockchain technology offers a promising solution by providing a decentralized, secure, and transparent framework for managing certificates. With the rising interest in blockchain technology and the potential it holds for secure, transparent, and decentralized applications, the concept of Non-Fungible Tokens (NFTs) has gained significant traction. This paper presents the development and implementation of an NFT marketplace specifically designed for the Issuance, verification and Validation of Decentralized Certificates (DCs). DCs represent a new paradigm in the verification and authentication of various credentials, such as academic degrees, professional certifications, and licenses, leveraging the immutable and tamper-proof nature of blockchain technology. The proposed marketplace provides a user-friendly interface for issuing, verifying, and Validating a Decentralized Certificates as NFTs, ensuring transparency, security, and ownership rights for individuals and organizations. Through smart contract functionality, the marketplace facilitates trustful transactions, eliminates intermediaries, and establishes a robust ecosystem for the seamless exchange of digital certificates. This paper discusses the technical architecture, features, and potential benefits of the NFT marketplace for DCs, highlighting its role in revolutionizing the way certificates are managed and validated in a decentralized and trusted manner. All things Considered, the proposed framework is designed to achieve transparency, usability, confidentiality, authenticity in distributed manner.

Keywords: Blockchain; Smart Contract; Non-Fungible Token; Decentralized; Certificate; Distributed Ledger

Introduction

If a fraudulent certificate is presented, it is challenging to Identify. Instead of being printed.

Distributed ledger technologies (DLTs) such as on paper, the certificate is issued using NFT. Non blockchain are emerging technologies posing threat to existing business models. Now a days used to verify and validate the ownership. There will be a lot of forged documents.

Fungible Token provides unique value which is everywhere. Anyone can use the certificate to cannot be changed, once it has been recorded.

Blockchain uses the NFT to store the data. Data demonstrate that they successfully finished.

The certificates are kept in IPFS-based accredited course with grades. For the Instance, decentralized storage. It uses the cryptography when a candidate applies for an office, these is stored in NFT. To mint and distribute certificates to the user in this procedure, the certificate issuer must first establish their identity. The certificate can be produced and given to the person who needs to obtain it once the issuer has confirmed the identity.

Polygon-Matic. The issuer and receiver address certificates are used to confirm that person.

The issuer has to provide the address in which the certificate is going to be minted. Once the address is added and the certificate is issued, then those visiting the certificate page provide a verified symbol with the issuer data. In the landscape of blockchain technology, there could be defined two types of tokens, including fungible tokens, in which all the tokens have equal value and non-fungible tokens (NFTs) that feature unique characteristics and are not interchangeable.

Actually, non-fungible tokens are digital assets with a unique identifier that is stored on a blockchain. NFT was initially suggested in Ethereum Improvement Proposals (EIP)-721, and it was later expanded in EIP-11556. NFTs became one of the most widespread applications of blockchain technology that reached worldwide attention in early 2021.

They can be digital representations of real world objects. NFTs are tradable rights of digital assets (pictures, music, films, and virtual creations) where ownership is recorded in blockchain smart contracts. Using Ethereum blockchain to create decentralized certificates as non-fungible tokens (NFTs) is an innovative approach.

Figure 1 represents, how the Non Fungible Token works in the Blockchain Methodology. It is helpful for the understanding of the Non Fungible Token.

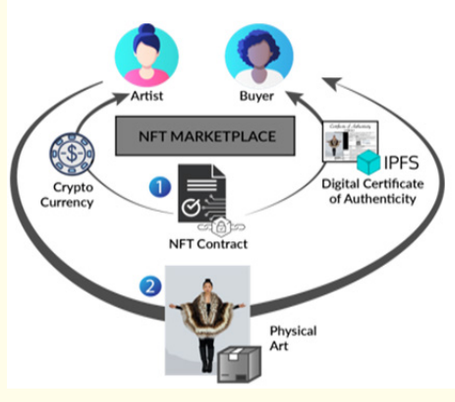

Figure 1: NFT Functioning Module

Each certificate could be represented as a unique NFT on the Ethereum blockchain, providing immutable proof of ownership and authenticity. Smart contracts could be utilized to manage the creation, transfer, verification and validation of these certificates, ensuring transparency and security. This approach could revolutionize the way certificates are issued and managed, offering benefits such as enhanced trust, accessibility, and interoperability. Representing the NFT marketplace for Decentralized.

Certificates we can get many advantages:

- **Immutable Records:** Certificates stored on a blockchain are tamper-proof and cannot be altered or forged, ensuring the integrity of the data.
- **Ownership and Authenticity:** NFTs represent unique digital assets, allowing individuals to claim ownership of their certificates and verify their authenticity without relying on centralized authorities.
- **Interoperability:** Blockchain-based certificates can be easily shared and verified across different platforms and systems, promoting interoperability and reducing the need for manual verification processes.
- **Transparency:** The decentralized nature of blockchain technology enables transparent and auditable certificate issuance and transfer processes, fostering trust among stakeholders.
- **Reduced Costs:** By eliminating intermediaries and automating certificate management processes, decentralized certificate marketplaces can reduce administrative costs and streamline operations.
- **Global Accessibility:** Individuals from anywhere in the world can access and verify their certificates through blockchain-based marketplaces, overcoming geographical barriers and enhancing accessibility.
- **Innovative Use Cases:** NFTs allows the innovative features such as embedding metadata, enabling dynamic updates, and integrating with other decentralized certifications (D-Apps), opening up new possibilities for certificate management and utilization.

This paper is organized as follows. Section II gives the introduction of related concepts. Section III describes the Background of the project. Section IV describes the proposed framework of the project. Section V Illustrates the key steps for NFT Marketplace for Certificates. The paper is concluded in Section VI.

Related works

Many solutions have been proposed and developed from perspective of using blockchain in education domain. We limit our discussion to the systems and architectures that propose blockchain-based verifying and distribution of academic certificates.

Malta has become the first nation-state to deploy blockchain technology in education, issuing digital diplomas, training certificates and equivalency statements, using the Block Certs standard. Block Certs is an open-source platform that is currently in develop-

ment by Massachusetts Institute of technology (MIT) that mainly focuses on issuing and verifying official certificates using blockchain [2]. Blockchain Certs is based on the self sovereign identity of all the participants by providing components to create, issue, view and verify certificates.

According to our literature review, there are some other proposed solutions in this domain such as EduCTX, UZHBC (University of Zurich Blockchain), EduChain, UNIC, Cerberus and SmartCert. EduCTX proposes a unified global higher education credit and grading system based on the European Credit Transfer and Accumulation System (ECTS), in which coins are transferred on the blockchain to signify academic study credits attained by students. It requires students and verifiers to maintain cryptographic credentials or digital identities to participate in the ecosystem.

UZHBC is a blockchain-based verification system, specifically for diplomas issued by the University of Zurich. It uses the public Ethereum blockchain and employees a smart contract for both issuance and verifications, and accepts a PDF of the credential as input. It does not incorporate accreditation body. EduChain enables academic institutions to interface with blockchain infrastructure of trust.

Educhain is building a series of solutions for academic institutions, such as enabling instant issuance and authentication of digital credentials, and a comprehensive "academic passport" of student achievements, using blockchain technology [4,10,14]. The University of Nicosia in Cyprus is also implementing blockchain technology as a way of recording students' achievements [6].

UNIC is using Bitcoin Blockchain for many activities, such as fee payments, issuing academic certificates on Blockchain Technology and so on. It has commenced issuing all diplomas using the blockchain since 2017. To preserve the authenticity of the certificate, it uses the SHA-256 hash algorithm. Although UNIC does not offer a clear method of authenticity of parties and requirements for an employer to verify the certificate is inadequate. *Et al.* [13] authors propose a blockchain-based accreditation and degree verification system, called Cerberus. It uses on chain smart contracts for credential revocation, and it does not entail students or employers to manage digital identities or cryptographic credentials to use the system.

Development requirements

Since this type of application requires a blockchain network, this network incurs fees and is only used for full-developed applications. It can lead to huge financial losses in possible errors [8]. Therefore, to deploy our solution, would be appropriate first to test it locally, and then send to the Ethereum blockchain. For development of application we need to use:

- **Ganache:** Ganache is part of the Truffle suite of Ethereum development tools, and it is open source. It quickly creates a personal Ethereum blockchain network used to run tests commands and see how the chain operates. As Ganache comes with a GUI, and requires a separate desktop environment, we use Ganache-Cli hosted on Code Sandbox. By default Code Sandbox is an online IDE and prototyping tool [5] aimed at developing web apps, but in this case we will use it only for ganache-cli as it enables us to quickly create an online semi personal blockchain network.
- **Web3JS:** Web3JS enables the client to communicate with the blockchain network and enable us to deploy, view, add, modify and validate contracts on blockchain network.

Web3JS together with some HTML/CSS/JavaScript are used to create a simple interface to communicate with the blockchain. Additional libraries such as jQuery, Bootstrap are used to make the development easier and libraries such as Crypto-Js in order to encrypt data.

Remix

A Solidity word processor/IDE, Remix, is used to deploy smart contracts. It has a few extra features aside from simply writing code. After developing the smart contract, Rinke by Ethereum Test Network is used in order to compile and test the contracts.

Background

- Ethereum Blockchain- Ethereum [14] goes beyond just crypto-currency transfer, and it also enables developers to deploy Turing-complete smart contract scripts. Smart Contract Ethereum implements a complete Turing system to automatically move digital assets according to pre-defined arbitrary rules called smart contracts. The contents and conditions of execution are predetermined in smart contracts and will be automatically executed when the conditions are met [6].
- Smart Contract- Ethereum implements a complete Turing sys-

tem to automatically move digital assets according to pre-defined arbitrary rules called smart contracts. The contents and conditions of execution are predetermined in smart contracts and will be automatically executed when the conditions are met [1].

- Digital Wallet- Digital wallet is similar to a bank account, and it is a unique identifier for a user to send and receive the assets. Digital wallet is a fixed number of characters address which generated from a pair of public key and private key.
- ERC20- the ERC20 (Ethereum Request for Comments 20) [4], introduces a standard for Fungible Tokens. ERC20 tokens are blockchain based assets that each token is exactly the same (in type and value) as another token.

ERC721-The ERC721 (Ethereum Request for Comment) [2] introduces a standard for NFT. ERC721 token is unique and even 2 ERC721 token issued from same Smart Contract, they can have a different value. ERC721 helps us find a way to present distinctive details about an asset in the form of a token.

Existing certification methodology:

Certificate generation in existing systems

Certificate generation in existing systems typically involves several steps:

- **Identity Verification**: The entity requesting the certificate (e.g., a person, organization, or device) must undergo a verification process to confirm their identity. This could involve providing official documents, undergoing background checks, or other means of identity validation.
- **Certificate Signing Request (CSR):** For digital certificates, the requester generates a CSR, which includes their public key and identifying information. The CSR is then submitted to a Certificate Authority (CA) for validation and signing.
- **Validation Process:** The CA verifies the information provided in the CSR, ensuring that the requester has the right to request the certificate and that the provided details are accurate.
- **Certificate Issuance:** Once the validation process is complete, the CA generates the certificate and signs it using its private key. The signed certificate is then issued to the requester. Existing Systems in Secure Certificates.
- **Public Key Infrastructure (PKI):** PKI is a set of hardware, software, policies, and standards used to create, manage, distribute, use, store, and revoke digital certificates. It provides the foundation for secure communication over the internet by facilitating the issuance and management of digital certificates.
- **Certificate Authorities (CAs):** CAs are trusted entities responsible for issuing digital certificates. They verify the identity of certificate applicants and digitally sign the certificates they issue, thereby vouching for the authenticity of the certificate's contents.
- **Certificate Revocation Lists (CRLs):** CRLs are lists of certificates that have been revoked by the issuing CA before their expiration date. CRLs allow relying parties to check the status of certificates to ensure they have not been compromised or revoked.
- **Online Certificate Status Protocol (OCSP**): OCSP is an alternative to CRLs for checking the revocation status of certificates in real-time. It enables relying parties to query the CA's server to determine the current status of a certificate.
- **Certificate Transparency (CT):** CT is a system for publicly logging and auditing the issuance of digital certificates. It helps detect miss used certificates and other security incidents by providing transparency into the certificate issuance process.

Proposed system

Aims to provide a secure and decentralized platform for issuing, trading, and verifying educational and professional certificates as nonfungible tokens (NFTs).

Key features include decentralized certificate issuance through smart contracts, blockchain integration for secure verification, user-friendly interfaces, privacy measures, legal compliance, and interoperability standards [6,7].

The literature on NFT marketplaces for certificates and properties delves into the potential applications of blockchain and NFT technology in verifying and transferring ownership of real-world assets [3]. Researchers explore how NFTs can enhance the security and transparency of property transactions, streamline the certification process, and reduce fraud. Moreover, studies discuss the legal implications, regulatory challenges, and the role of smart contracts in automating property related transactions within NFT marketplaces. As this field evolves, the literature is likely to address practical implementations, user adoption, and potential hurdles in integrating NFTs with traditional property markets.

Scope of Blockchain

Blockchain technology, often called the "Internet of Value," holds immense potential for transforming industries through its decentralized and secure nature. Figure 2 Here are some of the broad scopes of this innovative technology across various sectors.

Figure 2: Scope of Blockchain.

Key steps for NFT market place for certificates

Step 1

Understand the NFTs and ethereum

Understand the basics of NFTs (Non-Fungible Tokens) and the Ethereum blockchain. NFTs are unique digital assets that represent ownership of a specific item or piece of content. Ethereum is a popular blockchain platform that supports the creation and trading of NFTs through smart contracts.

Step 2

Smart contract development

- **Design Smart Contracts:** Develop smart contracts for your NFT marketplace. This includes contracts for creating, buying, selling, and transferring certificates. The most critical contract will be for the NFTs themselves, defining their ownership and properties.
- **ERC-721 Standard:** Use the ERC-721 standard for your NFTs. This standard ensures that your certificates are non-fungible, meaning each one is unique and cannot be replicated.
- **Implement Business Logic:** Write the logic for minting new certificates, transferring ownership, setting prices, and royalties for creators.

Step 3

Frontend development

User Interface: Develop a user-friendly frontend where users can interact with your NFT marketplace. This includes: A landing page displaying featured certificates. Pages for browsing, buying, and selling certificates. Wallet integration for users to connect their Ethereum wallets (like MetaMask) [15]. Integration with Blockchain: Use web3.js or a similar library to interact with the Ethereum blockchain from the frontend. This includes displaying certificate information, fetching ownership data, and initiating transaction.

Step 4

Backend development

- **Server Setup**: Set up a backend server to handle various functionalities such as user authentication, data storage, and integration with the blockchain. Figure refers improvements of the existing system to proposed system.
- **API Development**: Create APIs to interact with the Ethereum blockchain, handle user requests, and update the frontend with real-time data.

Step 5

Smart contract testing

Thoroughly test your smart contracts using tools like Truffle and Ganache to ensure they work as intended. Frontend and Backend Testing: Test the frontend and backend functionalities to ensure a smooth user experience, proper data handling, and secure transactions.

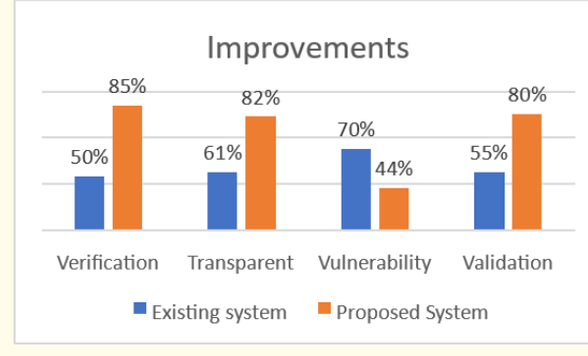

Figure 3: Improvements.

Step 6

Deploy smart contracts

Deploy your smart contracts to the Ethereum main net or a test net like Ropsten for initial testing. Deploy Frontend and Backend: Deploy your frontend and backend applications to a web server or hosting service like AWS, Heroku, or IPFS (Inter Planetary File System).

We have reduced the vulnerability and increased the Authenticity in our project of "NFT Marketplace for Decentralized Certificates and Documents using Blockchain.

Peer-to-peer networks with cryptographic techniques to create a safe and secure platform for application development. Thus we can generate, verify and validate the certificates and documents through this blockchain technology in secure and transparent manner.

☑ Considered; ☒ Not Considered;

Proposal	1	2	3	4	5	6	7
Blockcert (2016)	☑	☒	☑	☑	☒	☒	☒
EduCTX(2018)	☒	☒	☒	☑	☑	☒	☒
BCDiploma (2018)	☑	☒	☒	☑	☒	☒	☒
UZHBC(2018)	☒	☒	☒	☑	☒	☒	☒
NFT Marketplace (proposed)	☑	☑	☑	☑	☑	☑	☑

Figure 4: Comparison of the Existing proposal in NFT Marketplace.

1: Support any type of certificate; 2: Accredited institution; 3: Certificate revocation; 4: Privacy of personal information; 5: Cryptocurrency involved; 6: Verifiable Certificate; 7: Student's certificate are collected in single digital wallet.

Conclusion

In today's digital environment, content ownership is a huge issue. We have studied various technical papers on blockchain. During our course of study, we discussed on Ethereum to a large extent and NFTs are used to define a unique value. Value of the NFT based Certificate not equal to another NFT based Certificate. Blockchain-based certificates offer several advantages over traditional paper-based or digitally signed certificates. We weighed all its pros and cons and after due consideration, blockchain-based certificates offer enhanced security, transparency, efficiency, and accessibility compared to traditional certification methods. They have the potential to revolutionize the way we issue, verify, and manage certificates across various industries, providing a more trustworthy and reliable certification process. Peer-to-peer networks with cryptographic techniques to create a safe and secure platform for application development. Thus we can generate, verify and validate the certificates and documents through this blockchain technology in secure and transparent manner. In this project the Authenticity has increased and Vulnerability has been decreased.

Bibliography

1. Muhamed Turkanovi´C., *et al*. "Eductx: A blockchain based higher education credit platform". *IEEE Access* 6 (2018): 5112-5127.

2. William Entriken., *et al*. "EIP 721: ERC721 Non-Fungible Token Standard". Ethereum Improvement Proposals.

3. Karthik S., *et al*. "A multi-Mobile Agent and optimal itinerary planning-based data aggregation in Wireless Sensor Networks". *Computer Communications* 184 (2022): 24-35.

4. Vogelsteller Fabian and Buterin Vitalik. "EIP 20: ERC-20 Token Standard".

5. "Business Insider".

6. Jerinas Gresch., *et al*. "The proposal of a blockchain-based architecture for transparent certificate handling". In Witold Abramowicz and Adrian Paschke, editors, Business nformation Systems Workshops, pages 185–196, Cham, 2019. Springer International Publishing (2019).

7. blockcerts.org. "Blockcerts".

8. M Karthick., *et al*. "Real-time MRI lungs images revealing using Hybrid feed forward Deep Neural Network and Convolutional Neural Network". *Intelligent Data Analysis* 27 (2023): S95–S114.

9. Harry Halpin and Marta Piekarska. "Introduction to Security and Privacy on the Blockchain".

10. Wen-Tao Zhu and Jingqiang Lin. "Generating Correlated Digital Certificates: Framework and Applications".

11. Chinmay Saraf and Siddharth Sabadra. "Blockchain Platforms: A Compendium".

12. OECD. "Benchmarking Higher Education System Performance".

13. ethereum.org. "Ethereum".

14. Jiin-Chiou Cheng., *et al*. "Blockchain and Smart Contract for Digital Certificate".

15. Karthick M., *et al*. "An Efficient Multi-mobile Agent Based Data Aggregation in Wireless Sensor Networks Based on HSSO Route Planning". *Ad Hoc and Sensor Wireless Networks* 57 (2025): 187–207.