Diploma as an ERC-721 NFT

By:

~~Student Full Name~~

~~Student Enrolment Number~~

Bachelor of Technology

Computer Science & Engineering

Under the Supervision of:

~~Supervisor Name~~

(Assistant Professor)

Department of Computer Science & Engineering

School of Engineering Sciences & Technology

Jamia Hamdard, New Delhi

2022-23

CERTIFICATE

I hereby declare that the work being presented in this report titled "**Diploma as an ERC-721 NFT**" is an authentic record of my work carried out under the supervision of ~~Supervisor Name~~ (Asst. Prof.).

The matter embodied in this report has not been submitted by me for the award of any other degree.

Name of the Student:	**~~Student Full Name~~**
Program:	**Bachelor of Technology**
Branch:	**Computer Science & Engineering**
Enrolment Number:	**~~Student Enrolment Number~~**

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Sign. Date

ACKNOWLEDGEMENT

I want to extend my appreciation to ~~Supervisor Name~~, Assistant Professor, for providing sincere guidance throughout the course of this project's development.

I express my gratitude towards my peers and seniors who have generously dedicated their time and provided constructive feedback on my project.

The author expresses gratitude towards the faculty members at the School of Engineering Sciences & Technology (SEST) for providing an optimal setting to carry out their project.

Finally, I express my profound gratitude to all acquaintances who have served as a catalyst for my inspiration.

ABSTRACT

In the contemporary digital era, the verification of a candidate's academic qualifications can prove to be tedious and prolonged work for organisations. The conventional method of verifying diplomas, which entails contacting the educational institution or physically examining the diploma, can require several days or even weeks to complete. The process of verifying the qualifications of multiple candidates can be excessively time-consuming for employers.

The traditional approach to diploma validation may be deemed unreliable, as well as susceptible to instances of fraud and forgery. The authenticity of a diploma is often called into question due to the prevalence of fraudulent copies, or the inability of the issuing educational institution to provide the necessary documentation for verification purposes.

The current methods of diploma validation may be perceived as unreliable and inefficient by employers. The utilisation of NFTs and blockchain technology has the potential to accelerate and enhance the verification of academic qualifications, thereby ensuring safety for all stakeholders involved.

Keywords: Diploma, Diploma Verification, Diploma Fraud, NFTs, Blockchain, Authenticity.

CONTENTS

CHAPTER 1

INTRODUCTION

The development of blockchain technology and NFTs (non-fungible tokens) in recent years has opened up new possibilities for innovation in a variety of industries, including education. NFTs offer a special answer to the issues that traditional methods of authenticating educational credentials encounter by enabling the secure storage and transmission of digital assets.

The work presented here focuses on the creation of a project that issues and verifies degrees using blockchain technology and NFTs. The project intends to offer graduates a more effective and secure way to access and share their educational credentials while also streamlining the employer verification procedure.

The manual verification technique used by educational institutions or physical document inspection is frequently time-consuming and unreliable when it comes to validating diplomas. These conventional techniques are also vulnerable to fraud and counterfeiting. An innovative approach to these problems is the use of NFTs and blockchain technology, which offers a safe and simple way for employers to confirm the legitimacy of a graduate's credentials.

This report gives a thorough study of the project's design and implementation, including technical information about the web interface that can be used to issue and validate diplomas. The effectiveness of employing NFTs to issue diplomas is also evaluated in the report, along with the potential advantages and drawbacks of adopting this technology in educational institutions.

CHAPTER 2

BACKGROUND

NFTs:

Tokens are digital assets that can represent various types of value, such as cryptocurrency, utility, or securities. They are fungible, meaning that each token is interchangeable with one another and has the same value. Tokens are often used in blockchain-based ecosystems to incentivize network participants, enable transactions, and facilitate governance.

NFTs, on the other hand, are non-fungible, meaning that each NFT is unique and cannot be exchanged for another NFT on a one-to-one basis, in contrast to conventional cryptocurrencies/tokens like Bitcoin or Ethereum. While tokens can represent multiple units of value, NFTs represent a singular, unique asset with its own specific data and metadata that distinguishes it from other NFTs. NFTs are distinct digital assets that are stored on a blockchain.

NFTs have a long history that dates back to the genesis of blockchain technology. A project dubbed Coloured Coins, which sought to generate distinctive, non-fungible tokens that might represent assets like stocks and bonds, presented the idea of NFTs in 2012.

However, NFTs did not become well-known until the introduction of the Ethereum blockchain in 2015. In 2017, the video game CryptoKitties, which let users buy, sell, and breed virtual cats known as NFTs, went viral and popularised the idea of NFTs.[1]

The applications and use cases for NFTs have grown ever since. Digital assets including artwork, music, films, and virtual real estate have all been represented by NFTs. NFTs have also been utilised to symbolise distinctive in-game assets and items in video games and virtual worlds.

The market for NFTs has expanded recently, with high-profile sales and auctions garnering international attention. A digital piece by the artist Beeple that sold for $69 million in March 2021 broke the previous record for the most expensive NFT ever sold.[2]

As NFTs continue to develop and influence how we perceive ownership and value in the modern digital era, they open up new possibilities for investors, collectors, and artists alike.

ERC-721 Standard:

The development of the ERC-721 standard began in 2017, as the Ethereum community started to investigate the potential applications of NFTs. At the time, ERC-20, which was created for fungible tokens that stand for identical units of value, was the most popular token standard on the Ethereum network.

However, a new standard was necessary due to the special characteristics of NFTs. Dieter Shirley put forth the ERC-721 standard in answer to this demand in late 2017.

Dieter Shirley's suggestion was accepted as an official standard by the Ethereum community in 2018.[3]

For the creation and management of NFTs on the Ethereum blockchain, the ERC-721 standard offers a set of regulations and best practices. It establishes a standard interface that NFTs are required to implement, with features for transferring ownership, verifying ownership status, and retrieving NFT metadata.

Support for distinct, non-exchangeable tokens is one of the main characteristics of the ERC-721 standard. ERC-721 tokens are distinct and have their own unique properties and metadata, unlike other token standards like ERC-20 that permit a set number of identical tokens. Because of this, ERC-721 tokens are the best choice for encoding non-fungible goods like works of art, music, and collectables. Additionally, it gives builders a means to make games and applications that rely on special, indisputably rare content.

The CryptoKitties video game was the first significant use case for ERC-721 tokens. The popularity of CryptoKitties proved that NFTs have the capacity to produce brand-new varieties of digital assets and collectables.[1]

The Ethereum ecosystem has enthusiastically embraced the ERC-721 standard, which has enabled the NFT sector to expand at an exponential rate.[3] The Ethereum blockchain's most frequently adopted NFT standard as of right now is ERC-721.

Advantages of Diploma NFTs Over Regular Diplomas:

There are several advantages to using NFTs for issuing diplomas:

1. **Immutable and secure:** NFTs are stored on a blockchain, which makes them immutable and tamper-proof. This ensures that the diplomas are secure and cannot be altered or forged, providing a higher level of trust and authenticity.
2. **Easily verifiable:** With a web interface that verifies the authenticity of the diploma, employers and other stakeholders can easily verify the validity of the diploma, without the need for complicated background checks or authentication processes.
3. **Portable and transferable:** NFTs can be easily transferred and traded between individuals, providing a more flexible and portable way to represent academic achievements. This means that students can take their diplomas with them wherever they go, without having to worry about physical copies or transcripts.
4. **Cost-effective:** Issuing diplomas as NFTs can be more cost-effective than traditional methods, such as printing physical copies and mailing them to students. This is especially true in a digital age where more and more processes are moving online.
5. **Future-proof:** By issuing diplomas as NFTs on a blockchain, they are future-proofed against changes in technology and advancements in the digital landscape. This ensures that they will remain valid and verifiable for years to come, even as new technologies emerge.

Overall, using NFTs to issue diplomas provides a more secure, efficient, and cost-effective way to manage academic credentials, while also ensuring that they remain valid and trustworthy in an increasingly digital world.

CHAPTER 3

DESIGN & IMPLEMENTATION

The project can be divided into two major implementations:

1. Blockchain Implementation
2. Web app Implementation

The blockchain & the web app both work independently. The web app can be used to fetch data from the blockchain and show it to users who need to verify the credentials of diplomas and send data to the blockchain when *'office'* mint any new diploma. The contract has been developed in a way that anyone can develop a web app that can replace the official web app. Initially, the university should maintain at least one web app that enables users to verify credentials in a user-friendly manner, especially for those who aren't familiar with blockchain. Once there exists a certain number of open-source web apps that do provide similar functions, the university may choose not to maintain web apps any longer.

1) Blockchain Implementation:

The language solidity has been used for writing the contract on the blockchain. Although this project will be demonstrated on the Sepolia testnet, this contract should work just fine on any EVM-compatible chain i.e. Ethereum, Polygon, BNB Smart Chain etc.

The contract holds records for issued Diplomas and their associated data or attributes as a struct. Each Diploma has these eight attributes:

1. **university (type => string):** This holds the name of the university issuing diploma, this has been fixed at the contract level and need not be provided every time a new diploma is being minted. Apart from this attribute, value for all attributes needs to be provided when minting a new diploma.

   Example: "University of Westeros"
2. **studentName (type => string):** This holds the full name of the students to whom the diploma has been issued. The value for this attribute needs to be provided when minting a new diploma.

Example: "Alex Bob"

3. **enrolmentNumber (type => string):** This holds the enrolment number of the students. It is expected to be 10 digits long. The transaction will not get committed if provided with any other length of the input, although if provided with any non-numeric input of length 10, it would be accepted. Even if the enrolment number consists of anything other than a numeric value, the smart contract will work fine, but searching diplomas from the enrolment number would require additional steps which isn't in the scope of this project.

   It is also necessary to be extra careful with the enrolment number because the enrolment number provided is used to generate a *certificateNumber* equivalent to *tokenID* in ERC-721. The smart contract concatenates two zeros i.e. "00" at the end of the provided string and then converts it into *'uint256'* type which will be the *certificateNumber* of that diploma, in case of students already having any other diploma issued to them, new *certificateNumber* will be derived by incrementing *certicateNumber* until a new *certificateNumber* has been reached with no previous record. This implies that a student can be issued 100 diplomas before exhausting all possible *certificateNumber*, which is pragmatically impossible. For non-numeric input, the contract will use ASCII code when converting to *'uint256'* type i.e. 97 for a and 65 for A.

   Example: "2021208111" will generate 202120811100 as its first *certificateNumber* and 202120811101 as its second and so on.

   certificateNumber will always be of the *'uint256'* type.

4. **program (type => string):** This holds the name of the programs which the students have attended.

   Example: "Bachelor of Technology"

5. **specialisation (type => string):** This holds the specialisation, if any in the program which the student has attended.

   Example: "Computer Science & Engineering"

6. **gpa (type => string):** This holds the obtained GPA by the student.

   Example: "8.8"

7. **dateOfGraduation (type => string):** This holds the date of graduation. Every format of date has its advantages and disadvantages, upon prolonged consideration, I have settled with UNIX timestamp, which can be easily translated to any format and also preserve timezone information. Therefore, the

date must always be passed in UNIX timestamp format. The smart contract checks for only a length of input and reject the transaction if it isn't 10. 10-digit long UNIX timestamp can handle dates from September 2001 to November 2286.

Example: "1685593800"

8. **certificateURI (type => string):** This holds a URI which should point to a JSON file that should contain different attributes as its key and value as the value of the same key. We could also hold all the above 7 attributes in this JSON as well but that beats the purpose of storing metadata also on the blockchain, conventionally it points to JSON stored using IPFS which technically is immutable. Most marketplaces that show metadata of NFTs fetch this data from the JSON file. This project is dependable on this JSON for image file which is too large to store on blockchain cheaply and even in its absence we will have all our necessities fulfilled. This will be a cosmetic layer for our NFTs.

OpenZeppelin's ERC-721 Enumerable preset has been imported which has an optional extension of ERC721 defined in the EIP that adds enumerability of all the token ids in the contract as well as all token ids owned by each account.[4] The preset has all the required functions, events and interfaces as defined in the ERC-721 standard so that it need not be defined again and we can move forward with our desired requirements with the contract.

A variable has been added to store the address of the owner, which defaults to the address which will be deploying the contract, the ownership can be changed but only by the current owner of the contract. The owner also has the responsibility to add and remove the address to the role of *'office'*. Only the address with the *'office'* role assigned can perform some actions like *'mintDiploma()'*, *'updateDiploma()'* and *'recoverDiploma()'*.

The following functions are available to meet our requirements in additionally to the requirements as specified by ERC-721 standard:

1. **addOffice (address office):** This function can only be called by *'owner'*. This is used to add an address to the *'office'* role. *'Owner'* can add as many addresses to this role as required.

2. **removeOffice (address office):** This function can only be called by *'owner'*. This is used to remove any address from the *'office'* role. *'Owner'* can remove all addresses from this role if required.
3. **transferOwnership (address newOwner):** This function can only be called by *'owner'*. This is used to transfer ownership of the contract. There can exist only one *'owner'* for this contract. Transferring ownership doesn't add or remove any address from the *'office'* role.
4. **mintDiploma (address recipient, string memory studentName, string memory enrolmentNumber, string memory program, string memory specialisation, string memory gpa, string memory dateOfGraduation, string memory certificateURI):** This function can only be called by *'office'*. If any other address tries to call this method, this will revert to its original state and throw an error message, "Only office can mint Diploma." If called by the *'office'* role, it will check if the length of the string provided as **dateOfGraduation** is 10 and proceed only if it is only 10. The reason is, it expects a date in its UNIX timestamp. After that, it will check if the length of the string passed as **enrolmentNumber** is 10 and proceed further only if it is exactly 10. As we can see that sanitisation hasn't been done on all inputs at the contract level this is because minting a diploma can only be done by addressing having an *'office'* role. This is expected that the people responsible for the minting diploma will be extra careful or use some type of automation to make entries error-free.
5. **updateDiploma (uint256 certificateNumber, string memory studentName, string memory enrolmentNumber, string memory program, string memory specialisation, string memory gpa, string memory dateOfGraduation, string memory certificateURI):** Apart from an additional check to verify if the **certificateNumber** provided already exists or not, this function works same as **mintDiploma.** This function can be used to update on-chain data about any diploma. This function is expected to be used to update records in case of any students change their legal names or sometimes gender these days, although every attribute can be updated in case of wrong entries while minting a diploma.
6. **recoverDiploma (uint256 certificateNumber, address recipient):** This function also can be called by only the *'office'* role. When any students lose

access to their address they can request the university to recover their diplomas. This function transfers any existing diplomas identified by passed **certificateNumber** to a new **recipient** address provided. It is expected as time progress and students get comfortable with managing their wallet private key, the use of this function will become obsolete.

7. **getDiplomaDetails(uint256 certificateNumber):** This is a *public view* function which will be used extensively to fetch stored diplomas and verify their details. **certificateNumber** must be passed correctly of any existing diploma otherwise this will throw an error: "Diploma doesn't exists.". This is expected to be the most used function of the contract and is seldom used by the university. This function takes **certificateNumber** and returns all stored attributes with that diploma as a list of strings. Any employer or third party who wishes to verify the credentials will be using this function extensively. The returned list will contain only values of the attributes: **["university", "studentName", "enrolmentNumber", "program", "specialisation", "gpa", "dateOfGraduation", "certificateURI"]** While displaying on any app the value may be converted in a more user-friendly manner i.e. unix obtained by the **dateOfGraduation** field can be converted to a human-readable format.

The contract has been deployed with the following detail:

- **Network:** Sepolia Testnet
- **Contract address:** *0x40d2E6726F550ccD98d87F3d9df79E81cCd6f87e*

Two diplomas have also been minted with the following dummy data:

- **Recipient Address:** *0xBCC3b93a99Fa5574B0a85E2b2309ED693c7938B3*
- **Student's Name:** Alex Bob
- **Enrolment Number:** *2222222222*
- **Program:** Bachelor of Technology, Master of Technology
- **Specialisation:** Computer Science & Engineering
- **GPA:** 9.5, 8.9
- **Date of Issue:** 1685593800, 1748752200

- **Certificate URI:**
  https://drive.google.com/uc?id=11Wpx2x5LW23J6zQrhizfCQBVhcoJBtlr
  https://drive.google.com/uc?id=1z3J9lJitLSyht38hGPYOp3CgPsSCuovk

Generated Certificate Numbers: 222222222200, 222222222201

2) Webapp Implementation:

Flask framework has been used for the development of the web app along with HTML, CSS and JavaScript.

There have been two web apps developed:

1. **View:** The first web app is for the general public, where anyone can search for diplomas. This has been made accessible to the public at: https://diplomanft.el.r.appspot.com/
2. **Write:** The second web app is for internal use by the university that's why there isn't any need for it to be made accessible to anyone outside of university administration. *'Owner'* & *'Office'* will be using this app to easily mint diplomas or perform other required actions.

1. **View:** This app can be used to verify credentials, this fetches data from the blockchain and displays it after converting it in a more human-readable fashion. The tree representation of the contents of its root folder is as follows:

```
project folder:
│   func.py
│   main.py
│   var.py
│
├───static
│   ├───contract
│   │       contract.abi
│   │
│   ├───css
│   │       head.css
│   │       index.css
│   │       search.css
│   │       view.css
│   │
│   ├───icon
│   │       icon.png
```

```
│   │
│   └──────js
│           index.js
│           view.js
│
└──────templates
        index.html
        search.html
        view.html
```

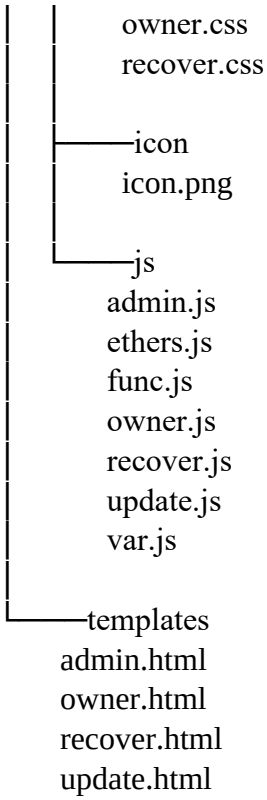
This webapp enables users to search using any of the following three methods:

1) **Wallet Address:** This will produce a search result containing all diplomas held by the provided address, details of diplomas can be opened by clicking on the desired diploma. If the provided address doesn't have a diploma or isn't a valid address, the user will get an appropriate error message.
2) **Enrolment Number:** This will produce a search result containing all diplomas issued to the provided enrolment number, details of diplomas can be opened by clicking on the desired diploma. If the provided enrolment number doesn't have a diploma issued to them or isn't valid, the user will get an appropriate error message.
3) **Certificate Number:** This will open details about provided certificate number. If the provided certificate number isn't valid, the user will get an appropriate error message.

2. **Write:** This app is intended to be used internally by the university admin, therefore this has been developed separately. This is expected to be used only a few hundred times a year majorly for minting diplomas. Due to its rare use, any development server would suffice for it.

   The tree representation of the contents of its root folder is as follows:

```
project folder:
│   main.py
│
├──────static
│   ├──────css
│   │       admin.css
│   │       head.css
│   │       head2.css
```



This web app enables the *'office'* role to mint new diplomas, recover diplomas & update diplomas in a user-friendly manner. The *'owner'* can grant & revoke the *'office'* role and can also transfer the ownership. The owner section can be reached by appending *'/owner'* at the end of the URL of the homepage.

Javascript has been used extensively for creating every transaction before sending them to the blockchain for confirmation. Wallet management has relied upon *'Metamask'. 'Office' & 'Owner'* wallets must be configured on 'Metamask' before transactions are sent.

Note: The authentication is being handled by the contract, therefore there hasn't been an additional layer of security in the web app. Any action if requested by an unauthorised wallet will be blocked on the blockchain.

CHAPTER 4

LIMITATIONS

While using NFTs for diploma issuance has many benefits, there are some limitations to be aware of:

- **Technical obstacles:** Even though blockchain technology is becoming more widely used, there is still a learning curve associated with using it efficiently. Students, employers, and other stakeholders may need to be educated on how to use NFTs and blockchain-based verification systems, which could present a barrier to adoption.
- **Network congestion and fees:** As NFTs and blockchain technologies gain in popularity, network congestion may result in delays and higher transaction costs. This can result in the minting process taking longer and costing more money. Therefore, before deciding on which blockchain to use, the university should consider all affecting factors.
- **Dependency on the blockchain:** While blockchain technology is known for its security and immutability, it is still a relatively new technology with potential vulnerabilities. If a blockchain is compromised, it could potentially undermine the security and trustworthiness of the NFT-based diplomas.
- **Limited adoption:** While NFTs have gained significant attention in recent years, they are still a relatively new technology with limited adoption in certain industries and communities. This could limit the usefulness and practicality of NFTs for issuing diplomas, especially if employers or other stakeholders are unfamiliar with the technology.

Overall, although using NFTs to issue diplomas has many benefits, there are still certain limitations and possible challenges to take into account before expanding the use of this technology.

CHAPTER 5

FUTURE IMPROVEMENT

There are several potential advancements that might be done in the future to improve the usage of NFTs for awarding diplomas:

- **Interoperability:** As NFTs continue to gain acceptance, it will be crucial to make sure that they are simple to transfer and validate across many platforms and systems. It may be possible to increase interoperability and increase acceptance of NFT-based diplomas by standardising their format and verification procedure.
- **Integration:** It will be crucial to make sure that NFT-based certificates can be easily connected with current academic and employment systems to promote the widespread use of these credentials. It may be necessary to do this to connect NFT-based degrees with already-existing databases and verification systems.
- **Improved user experience:** It will be crucial to create user-friendly interfaces and tools for verifying diplomas based on NFT to promote adoption and user-friendliness. This could involve developing mobile apps or other tools that make it easy for students and employers to access and verify credentials.

.

CHAPTER 6

CONCLUSION

In summary, the utilisation of non-fungible tokens (NFTs) as a means of distributing diplomas possesses the capacity to transform the conventional approach of validating and disseminating academic qualifications. NFTs have the potential to offer a decentralised and secure solution for students to manage and share their academic credentials with various stakeholders, by utilising the security and immutability features of blockchain technology.

Although there exist certain constraints and obstacles to contemplate, including technical obstacles network congestion and fees, compatibility issues, reliance on the blockchain, and limited adoption, there are also numerous possible enhancements that can be implemented that would improve the utilisation of NFTs for the purpose of issuing diplomas.

In general, the utilisation of NFTs for academic certifications has noteworthy advantages such as enhanced security, efficacy, and transparency. Given the ongoing evolution and widespread adoption of blockchain technologies, it is probable that Non-Fungible Tokens (NFTs) will emerge as a progressively prevalent and powerful mechanism for validating and disseminating academic qualifications in the times ahead.

REFERENCE

[1] Cryptopedia Staff. “CryptoKitties: A Pioneer in Ethereum Gaming and NFTs.” Gemini, March 11, 2022. https://www.gemini.com/cryptopedia/cryptokitties-nft-crypto-ethereum-token.

[2] Reyburn, Scott. “JPG File Sells for $69 Million, as ‘NFT Mania’ Gathers Pace.” The New York Times, March 11, 2021. https://www.nytimes.com/2021/03/11/arts/design/nft-auction-christies-beeple.html.

[3] Entriken, William, Dieter Shirley, Jacob Evans, and Nastassia Sachs. “Ethereum Improvement Proposals.” Ethereum Improvement Proposals, January 24, 2018. https://eips.ethereum.org/EIPS/eip-721.

[4] ERC 721 - OpenZeppelin Docs. “ERC 721 - OpenZeppelin Docs.” Accessed April 28, 2023. https://docs.openzeppelin.com/contracts/4.x/api/token/erc721#ERC721Enumerable.