NFT-Based Digital Certificates

\*Note: Sub-titles are not captured in Xplore and should not be used

|  |  |  |
| --- | --- | --- |
| Line 1*: Zhi Lin Wong* | Line 1: *Zhong Ming Teong* | Line 1 : *Zhi Xin Cheng Dylan* |
| Line 2: *Faculty of Computing* | Line 2:  *Faculty of Computing* | Line 2:  *Faculty of Computing* |
| Line 3: *Multimedia University, Cyberjaya* | Line 3:  *Multimedia University, Cyberjaya* | Line 3:  *Multimedia University, Cyberjaya* |
| line 4: *Selangor, Malaysia* | line 4: *Selangor, Malaysia* | line 4: *Selangor, Malaysia* |
| Line 5: *1201203299@student.mmu.edu.my* | Line 5: *1211200626@student.mmu.edu.my* | Line : 5  *1211200579@student.mmu.edu.my* |

|  |
| --- |
| Line 1: *Wei Yan Cheah* |
| Line 2: *Faculty of Computing* |
| Line 3: *Multimedia University, Cyberjaya* |
| line 4: *Selangor, Malaysia* |
| Line 5: *1201203703@student.mmu.edu.my* |

***Abstract***

The Blockchain-based NFT Digital Certificates Solution seeks to provide a secure, transparent, and effective way of managing and verifying academic certificates. The system basically has two components: the admin side and the student side. In the web applications of admin side, administrators can create certificates by filling in information concerning a student. These created certificates will be minted on the blockchain as NFTs for their immutability and non-fungibility. Further, at the admin panel, it provides the functionality to download the PDF of the certificates, which could be used traditionally.

On the students' side, it allows verification of the authenticity of their certificates by uploading the same to the platform. Here, the provided certificate is validated against the blockchain for validation of its record. Success messages from the system for such cases translate to confirmation of the issuance of a certificate, indeed by MMU.

The project is a very promising use case of blockchain and NFTs in solving major pain points of certificate management like fraud prevention and verification inefficiency. While offering a tamper-proof, user-friendly platform, what this system does is enhance the credibility of academic credentials and set the stage for further application of blockchain technology in education.

# Introduction

In the digital era, blockchain technology has emerged as a revolution solution for establishing trust, transparency, and security in various domains. One are where these qualities are paramount is the issuance and verifications of academic certificates. The traditional method of issuing and validating a cert is not only time consuming but also easy to lost and damaged of cert. This paper explores the implementation of a Non-Fungible Token (NFT) based digital certificate system, designed for Multimedia University Malaysia (MMU). This system allows MMU admin to secure upload certificates and enables student to verify and details of the certificates with ease and confidence.

Blockchain technology is a decentralized ledger system that ensures data confidentiality, integrity, and availability. Unlike conventional centralized system, blockchain operates on a peer -to- peer network, make it tamper-proof and highly secure. Non-Fungible Tokens (NFTs), a specialised application of blockchain represent unique digital assets that cannot be replaced or duplicated by anyone else. The unique feature of NFT makes an ideal medium for representing academic certificates, which are inherently personal and distinct to each recipient. By using the benefits of blockchain and NFTs, institutions can address longstanding challenges related to certificate issuance and verification, providing a modern and efficient solution.

Academic institutions in worldwide are facing significant challenges in issuing and verifying certificates. Traditional paper-based certificates are prone to forgery, loss, and degradation over time. Moreover, verifying the authenticity of certificates often requires manual intervention, which can be both time-consuming and error prone. These inefficiencies not only burden administrative resources but also compromise the credibility of academic qualifications.

For MMU, the lack of a streamlined and secure system for managing certificates can lead to administrative bottlenecks and reduced trust in the institution’s credentials. Students, on the other hand, face hurdles in proving the authenticity of their achievements, especially in professional or academic settings where quick and reliable verification is essential. If left unresolved, these challenges could erode trust, increase administrative costs, and limit the university’s ability to adapt to a digital-first world.

The primary objective of the research is to develop and implement an NFT-based digital certificate system for MMU which aims to achieve the following:

1. A secure and tamper-proof method for MMU admin to issue certificates.
2. A secure system to enable students to verify authenticity and details of certificates easily.
3. Leverage blockchain technology to ensure transparency, scalability, and long term reliability.

The need for a secure, efficient, and easy-to-use certificate management system has never been more pronounced. The continuing digitization of the academic and professional activities demands ever more robust solutions. This means that existing systems, usually based on paper or physical or virtual database, are not able to tackle contemporary issues, such as fraud, data breach, and inefficiency in verification processes.

The use of NFTs at MMU would improve the efficiency of the operational processes of the university and increase its image as an innovative university. The solution fills a gap in the modern academic cycle and is in line with the trends of changing the world to a more digitally transformed one and places MMU at the forefront of the race to incorporate new technologies in the sphere of education.

In summary, the research is aimed at meeting urgent societal needs by proposing a blockchain based system for issuing the digital certificates. The more effective application of NFT’s proposed by the system allows to completely change the paradigm of management of the certificates and guarantee security, transparency and access to all parties.

# Literature review

## Survey of Related Work

Various researchers have explored the use of blockchain and NFTs in different applications of secure digital certification and management. Several research analyses have been conducted to review how blockchain-based systems will be able to overcome fraud in certificates, inefficiency in verification processes, and non-transparency of data.

For example, *(Khati, n.d.)*has proposed a blockchain-based NFT system for certificate sharing to let the students mint certificates in the form of NFTs to provide verification and data provenance via signature schemes and hashing. Similarly, another researcher*(Karamachoski et al., 2020)* has developed a blockchain-based University Diplomas management system based on Smart contracts to improve transparency and security along with lessening administrative overhead. The use of NFTs in education, including identifying applications such as micro-certifications, transcripts, and academic rewards, are also conducted while emphasizing the technology's potential for improving data integrity and verification processes​ (Wu & Liu, 2023).

## Researcher has introduced the concept of "on-block certs," lightweight certificates stored directly on the Ethereum blockchain. This method eliminates reliance on traditional Certification Authorities (CAs) and improves fault tolerance and certificate integrity​ (Prado & Henriques, 2019). Additionally, the study conducted (Karamachoski et al., 2020)also mentioned how blockchain’s decentralized structure can simplify the certificate verification process and provide tamper-proof data storage, ensuring the authenticity of academic credentials.

## Identified Gaps

Despite these, some limitations persist with the current system, such as:

Scalability: Most solutions that currently exist are deployed on public blockchains, including Ethereum. For scaling with increasing numbers of users, it will face lots of performance and cost problems.

User Accessibility: Blockchain-NFT integration normally demands certain technical proficiency and creates difficult hurdles for the common, nontechnical admin.

Data Privacy: Most of the implementations keep the certificate data on public ledgers, which in turn may pose sensitive information exposure to unauthorized parties.

Low Adoption Rate: The adoption of NFT-based certification is still at its infancy, where many educational institutions and employers are quite skeptical about deviating from traditional ways.

## Relevance To The Project

This project builds on existing solutions by addressing identified gaps. It leverages the robustness of blockchain and NFTs while incorporating additional features tailored for MMU:

* Efficient Verification: Unlike systems focused solely on issuance, this project emphasizes easy verification of certificate validity and details through a user-friendly interface.
* Privacy-Centric Design: Encryption of data may be allowed in the project, along with selective access to allow only relevant parties to see important details of a certificate.
* Improved Scalability: It balances performance and the cost of performance through hybrid approaches, such as off-chain data storage with on-chain references to NFTs.

This project was integrated directly into the administrative processes of MMU for seamless issue and management of certificates, while also allowing students to securely and efficiently verify their credentials. This targeted application underlines how important it is to tailor blockchain solutions to institutional needs for functionality and usability.

# Methodology

This section explains the method employed in the construction and implementation of the NFT-Based Digital Certificate System for MMU. The system harnesses blockchain technology, NFTs and the relevant tools to promote safe, credible, and efficient processes in issuing and authenticating academic certificates.

## System Design Overview

The system is developed with the aim of overcoming the inefficiencies and vulnerabilities of conventional models of certificate issuance and verification. Through integration of blockchain technology and NFTs, the system gives each certificate a unique serial number, which cannot be forged and is stored permanently on a distributed ledger. The work is divided into layers to ensure that the functionality, scalability and usability of the design are considered in the work.

The architecture is organized into three key layers:

1. Blockchain Layer

The blockchain layer is the first layer of the system and its primary purpose is to provide secure, transparent and immutable functionality to the system. Ethereum was used as blockchain technology because of its solid foundation, popularity and compliance with the NFT standards. This layer is to handle certification and storage where each certificate is created and tokenized as an individual token. The standard helps achieve uniqueness of tokens so that they cannot be forged or modified; therefore, students’ achievements record is immutable. Moreover, the decentralized and transparent structure of this layer assures trust among stakeholders because of the capability of public verification of the certificates that are stored in the blockchain.

1. Application Layer

The application layer is responsible for the main user interface, and it provides easy to use interface for both the administrators and the students. Built on HTML, CSS, and JavaScript, this layer gives a web-based system that is user friendly and visually pleasing. The certificate details are posted by MMU administrators on the platform to kick start the NFT issuance process and the students use the platform to confirm the legitimacy of the certificates by entering a serial number. In terms of usability, the application layer includes dynamic elements which include form validation, clear and easily navigable interface, and real time feedback for all the users who are in touch with the system.

1. Interaction Layer

The interaction layer is the one that provides a connection point between the application layer and the blockchain layer. Built using the Web3.js library, this layer allows secure communication between a front-end web application and Ethereum blockchain. It performs numerous functions including submitting transactions to the blockchain for the purpose of issuing certificates, retrieving Token Metadata and checking on the authenticity of certificates in real time. The use of Web3.js guarantees that all engagements are accurate and easy to use for the administrators and students, who have no coding background.

This modular architecture also enables the system to easily scale as well as accommodate new features that may be incorporated in the future as well as future technologies. This way of developing structures the design in a way that does not allow changes in one layer to affect the others.

A diagram of a digital certificate system

Description automatically generated

Fig. 3.1 Use-case diagram.

A diagram of a software flow

Description automatically generated

Fig. 3.2 System Architecture Diagram

## Smart Contract Development

The smart contracts are at the center of the system and offer the capability of issuing, controlling, and validating NFTs of academic certificates. These contracts were written in Solidity, which is the most used language in Ethereum smart contracts. The development process was followed by some specific principles such as security, efficiency, and transparency of the system.

* Key Functionalities

Minting NFTs: For each of the certificates that MMU issues, smart contracts create a token. The token’s attributes include name of the student, student id, program, date of graduation and reference number.

Certificate Verification: According to the contracts, the user can validate the authenticity of a certificate by using the blockchain. This process involves pulling out the metadata of the token and comparing it to the token ID that was given by the student.

Ownership Management: Every NFT carries the Ethereum wallet address of the intended recipient of the token. This makes certain that only the person with the authentic certificate could make decisions over it.

* Development Tools

Hardhat: Hardhat is considered the main development environment, it was implemented on top of it to make the work on writing, testing, and deploying smart contracts more efficient. During the development and testing, Hardhat provided strong tooling and plugins to facilitate contract deployment, network handling, and with the blockchain.

Ganache: For testing the smart contracts, a personal Ethereum blockchain was employed to mimic different transactions in a closed environment.

* Optimization

Contracting logic was improved and unnecessary operations were avoided to minimize the costs of gas.

Input validation and access controls were in place to ensure that no unauthorized action was performed and to protect information.

The smart contracts went through this process to test their reliability and the efficiency of the network. In each feature, the execution was performed under different conditions including those of the extreme edge to determine areas of weakness.

## Technologies Used

The system was built based on the blockchain, and web technologies were used to implement the system. The tools and technologies were chosen depending on their integration, as well as the extent to which they could meet the needs of the project.

1. Blockchain Network

Ethereum was selected for its capacity to host NFTs and its well-developed framework. Due to the active use and high popularity of the platform, as well as the large number of developers, this project was a logical continuation of the work.

1. Web Development Tools

The front-end of the application was developed using HTML, CSS and JavaScript. These technologies made the platform to be more interactive, well designed and very user friendly.

1. Blockchain Libraries

Web3.js proved to be the bridge between front-end layers and the blockchain layer allowing for interaction with the Ethereum.

1. Development Framework

Hardhat was used for writing, compiling, testing and deploying smart contracts onto the Ethereum blockchain.

During development, they used Ganache, which creates a local blockchain environment in which the system could be tested.

1. Wallet Integration

MetaMask was incorporated to facilitate wallet authentication and perform signing of transactions. This made sure that all the operations of blockchain were done effectively and securely.

## Implementation Details

In addition to that, the Implementation Details of the solution involve the use of Hardhat in the deployment and management of smart contracts. The system comprises two core components: CertificateNFT and UserContract. CertificateNFT is responsible for minting the NFTs that symbolise certificates while UserContract is responsible for certificate operations including validation and storage. Hardhat also helps in the deployment process through the configuration of smart contract instances and their connection on the block chain. This approach removes complexity, making the solution easily scalable and manageable in terms of blockchain resources resulting to a practical solution.

## Deployment

In the deployment phase, the effort was made in readiness of the system for use in the real world. The smart contracts were migrated to the test net through the help of hardhat, while the web platform was set up to work with the contracts that had been deployed. The deployment process included:

* Confirming the availability and usability of all features in the test net environment.
* To ensure that the performance of the system developed for the project achieved the goals set out for the project.
* Storing the procedure of deploying in such a manner that it will be easy to perform upgrade or migration in the future.

# results and analysis

This section gives the testing results, the measures of effectiveness and efficiency and the important observations made while implementing and testing the NFT-Based Certificate Verification System. The purpose is to determine how effective and practical the solution is and how well it may be scaled or replicated.

## Testing Outcomes

To confirm the usability of the system, several tests were performed to check the main components and possible peculiarities. Key scenarios included:

1. Smart Contract Functionality Testing

The smart contracts were deployed using Hardhat on the Ganache local blockchain environment. This step ensured that the contract was well deployed, the correct address generated and that the program was communicating well with the blockchain. In the deployment output shown in the Fig. 4.1, contract addresses for CertificateNFT and UserContract are presented. Moreover, the settings of the configured Ganache environment used for deployment and interaction with the smart contracts are presented in the details in Fig. 4.2 together with the available gas limit, gas price and the network settings.

A computer screen with white text

Description automatically generated

Fig. 4.1: Contract deployment output from Hardhat, showing contract addresses.

A screenshot of a computer

Description automatically generated

Fig. 4.2: Ganache CLI setup used for deploying and testing smart contracts.

1. Edge Cases Tested

Fig. 4.3 represents a failure notification of the certificate verification that occurs when the metadata or the owner information does not correspond to the data on the blockchain. This means that the certificate presented for verification is either forged, invalid or belongs to another person who is undertaking the verification process. This mechanism makes it possible to successfully verify only certificates that are produced by the system and are valid.

A black background with white text

Description automatically generated

Fig. 4.3: Verification failure notification.

1. Front-End Testing

Fig. 4.5 shows the admin login process, where the administrator uses a MetaMask account to authenticate and access the system. At the login page, the user is asked to connect the MetaMask wallet with the request for reading account data and enabled networks. This guarantees a safe and efficient decryption technique of blockchain base login for the administrator.

A screenshot of a computer

Description automatically generated

Fig. 4.5: Admin Login Using MetaMask

Fig. 4.6 below illustrates the MMU Certificate Generator whereby the admin key in the information of the certificate to be generated such as the name of the student, student number, program of study, date of issue and the wallet address of the recipient. Once the admin completes the form, they press the “Issue Certificate” button to create an NFT of the certificate and associate it with the recipient’s wallet. It also provides the admin the ability to download the issued certificate on the same page.

A screenshot of a computer

Description automatically generated

Fig. 4.6: Admin Certificate Generation Interface.

Once the certificate is generated using the MMU Certificate Generator, the system provides a popup notification of the successful minting of the certificate as shown below in Fig. 4.7. This means that the certificate has now been tokenized and associated with the blockchain platform. At the same time, the CLI displays the blockchain transaction information, as illustrated in Fig. 4.8. This entails the transaction hash, gas usage, block number, and the time when the new block was created. This information confirms that the smart contract fulfilled the certificate issuance on the blockchain process.

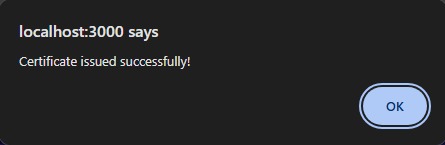


Fig. 4.7: Certificate Issuance Success Notification.

A black screen with white text

Description automatically generated

Fig. 4.8: Blockchain Transaction Details for Certificate Issuance.

In fig. 4.9 below the MMU Certificate Generator is issued by the admin and what is produced is the following certificate. The certificate contains details about the holder including their name, student ID, program, classification, and the issue date. This certificate is a digital form of the accomplishment of the recipient and is actually lodged in the blockchain as an NFT. The metadata present in the certificate’s PDF file is shown in fig. 4.10 below. It consists of the certificate name and description, recipient’s name and wallet address, course and faculty, issue date, and a distinct object number. These are important for the genuineness of the certification and can be verified from the block chain records. The metadata improves the possibility of tracking and also creates a secure and non-changeable connection between the PDF file and the NFT.

A certificate of achievement with text and numbers

Description automatically generated

Fig. 4.9: Certificate of Achievement Generated by the System.

A screenshot of a computer

Description automatically generated

Fig. 4.10: Metadata Embedded in the Certificate PDF File.

1. Verification Testing

Fig. 4.11 depicts the student login page at which the student tries to log in with a wrong wallet address which does not correspond to the certificate address. As a result, the system denies access and displays an error message: ‘You are not allowed to access the student page’. If the correct wallet address is entered then the student is allowed in and redirected to the certificate verification page.

A screenshot of a computer

Description automatically generated

Fig. 4.11: Student Login with Incorrect Wallet Address

Fig. 4.12 presents the certificate verification page, which is the page that students upload the certificate PDF file for verification. There is a section to drop files by merely dragging into the box or to choose the file from the folder. When the file is uploaded and the ‘Submit’ button is pressed, the system checks the certificate’s genuineness against records in the blockchain.

A screenshot of a computer

Description automatically generated

Fig. 4.12: Certificate Verification Page with PDF Upload

Fig. 4.13 where the user has uploaded the certificate PDF file for validation. After the file is submitted, the system checks the validity of the certificate by comparing the token and relevant metadata that is located on the blockchain. If the token and metadata are valid and match the claimed owner, the system displays a success message: Certificate is valid and corresponding to the claimed owner and the metadata. This verify that the certificate is genuine.

A screenshot of a computer

Description automatically generated

Fig. 4.13: Successful Certificate Verification Message

## Key Findings

Efficiency:

In comparison with the paper-based systems of certificate, this solution showed better effectiveness in terms of issuing and verifying them. By optimizing the user interface, the amount of time taken in issuing certificates was slashed.

Reliability:

The integration of blockchain and NFTs made the data safe and highly secure because any changes made were irreversible. Verification tests were always able to match the metadata thereby implying high reliability.

User Accessibility:

The front-end interface which underwent simplicity was created in such a way that the blockchain could be easily interacted with by non-technical people.

# DISCUSSION

## Interpretation of Results

The results clearly show that the solution proposed in the paper adequately solves the problems described in the statement of the problem. The system effectively deploys blockchain and NFT to provide secure academic certificate issuance and validation. The basic features such as certification, validation, and record on the distributed ledger proved to be functional during the testing stage. A tamper-proof blockchain means that certificates are secure, easily trackable, and verifiable. Issuance and verification were made easy through the front-end interface that was developed for administrators and students. These findings confirm the capacity of the system in addressing typical issues like forgery, inefficiency, and obscurity in certificate management. But there are also areas for improvements that we discovered through the results of the study, particularly the scalability of the solution to institutions that issue and verify hundreds or even thousands of certificates at the same time.

## Limitations

1. Gas Limit and Cost Intensity:

The use of Ethereum blockchain incurs high gas fees when issuing and verifying the certificates. As much as Ganache’s test environment helped in reducing costs during testing, the solution will be expensive if implemented on Ethereum mainnet or any public blockchain due to high resource utilization. This could be solved by looking for other blockchains with lower transaction fees or by using other methods of sharding where non-critical data is stored off-chain.

1. Scalability:

With institutions coming in, the volume of certificates to be issued and certified may put pressure on the blockchain network, hence increasing the time taken to make transactions and the costs associated with the process. Further improvements in the contract form and structure of the system may be needed to accommodate increased throughput.

1. User Accessibility:

Despite the simplicity of the developed system, some users may have some difficulties, for example, students or administrators who do not have experience in using blockchain systems may consider MetaMask wallet setup or the whole process to be complex and challenging. Perhaps when there is a well-written document on the onboarding process or better tutorials, there will be a possibility of closing this gap.

## Implications

1. Ensuring Authenticity:

The system ensures the authenticity and accuracy of academic certificates to guarantee their credibility because of the properties of blockchain. This can help assure employers, educational institutions, and students that the credential is real, and reduce the possibilities of forgery while increasing the value of the credential.

1. Streamlining Administrative Processes:

The solution makes processes of certificate creation and validation less labor-intensive and therefore cuts costs connected with administrative work. This system when implemented in institutions can bring efficiency in their operations and the institution can shift attention to core business of education.

1. Promoting Digital Transformation:

Since more industries are adopting blockchain and digital technologies, this system is in line with the current global digitalization. It puts institutions such as MMU ahead to be at the forefront in the adoption of blockchain into education and making the institutions more attractive.

# conclusion

The NFT-Based Digital Certificates System represents an innovative and robust solution for the enhancement of the security, transparency, and credibility of academic certificates. This is a blockchain-based system to address the two most significant issues facing certificate forgery and loss, where digital credentials are verifiable and tamper-proof.

On the admin side, an admin is facilitated to create a certificate by providing all relevant details about the student. These generated certificates are then lodged on the blockchain in the form of NFTs, creating a decentralized, tamper-proof record. In addition, the system offers the admin the possibility to download the certificates in PDF format, which enables offline use. Therefore, it provides flexibility and ease of use.

The system makes it easy to verify certificates on the student's side. A student is allowed to upload his/her certificates on the platform, and the system will cross-check the document with the data on blockchain. If a certificate is verified to be issued from MMU, the system would show "Verified Successfully" for the credence of the certificate.

The combination of blockchain and NFTs in this project creates new directions for the academic certification process. While ensuring authenticity and reliability, the system reduces fraud to a great level; it's user-friendly for the administrator and the student. Modern approach towards managing certificate-related issues and further explorations on the blockchain-based solutions may be considered grounded in this idea of the education sector.

##### Acknowledgment

We would like to take this opportunity to thank all the people who contributed to the successful completion of our project, the NFT-Based Digital Certificates System

Above all, we are deeply grateful to our Lecturer, Madam Uzma Jafar for the immense effort she invested in mentoring, commenting, and supporting us throughout this project. Her very valuable expertise and encouragement were instrumental in shaping our perceptions and approaches.

Further, Multimedia University and our faculty members are acknowledged for making available all the means and knowledge required to explore this new innovative field of blockchain technology and its application in digital certification systems.

On a personal note, special thanks go to our colleagues and classmates for the useful discussions and ideas that enriched our work by bringing in different visions related to our work. This form of teamwork from our team indeed will always be a source of great motivation.

Lastly, our deepest appreciation goes out to our families, who were so patient, encouraging, and gave endless support through this journey. Their faith in our combined capabilities kept us focused and determined to succeed.

Without the joint efforts, guidance, and support of all these persons, this work would never have seen the light of day. Consequently, we are eternally grateful for their contributions.

##### References

[1]Karamachoski, J., Marina, N., & Taskov, P. (2020). Blockchain-Based Application for Certification Management. *Tehnički Glasnik*, *14*(4), 488–492. https://doi.org/10.31803/tg-20200811113729

[2]Khati, P. (n.d.). *Student Certificate Sharing System Using Blockchain and NFTs*.

[3]Prado, N. F. R. A., & Henriques, M. A. A. (2019). On-block certs. *Revista Dos Trabalhos de Iniciação Científica Da UNICAMP*, *26*. https://doi.org/10.20396/revpibic2620181094

[4]Wu, C. H., & Liu, C. Y. (2023). Educational Applications of Non-Fungible Token (NFT). *Sustainability (Switzerland)*,*15*(1).https://doi.org/10.3390/su15010007

[5]Wu, C. H., & Liu, C. Y. (2023). Educational Applications of Non-Fungible Token (NFT). *Sustainability (Switzerland)*,*15*(1).https://doi.org/10.3390/su15010007

[6] Maurya, T., Singh, S. K., Thakur, V., & Chawla, S. (2024). Blockchain-Based Decentralized NFT marketplace for new fine art. International Journal of Innovative Research in Engineering & Management, 11(3), 5–10. <https://doi.org/10.55524/ijirem.2024.11.3.2>

[7] Lim, J. O., & Kamarudin, D. (2023). NON-FUNGIBLE TOKENS: ITS POTENTIAL ROLE IN COMBATTING CERTIFICATE FRAUDULENCE IN MALAYSIAN EDUCATION. International Journal of Education & Technology, 1(1). https://doi.org/10.59021/ijebt.v1i1.13