

DESIGNING BLOCKCHAIN BASED NON-FUNGIBLE TOKEN CERTIFICATE SHARING FRAMEWORK

A thesis submitted to the
College of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements
for the degree of Master of Science
in the Department of Computer Science
University of Saskatchewan
Saskatoon

By
Prakhyat Khati

©Prakhyat Khati, October 2023. All rights reserved.

Unless otherwise noted, copyright of the material in this thesis belongs to
the author.

Permission to Use

In presenting this thesis in partial fulfillment of the requirements for a Postgraduate degree from the University of Saskatchewan, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by the professor or professors who supervised my thesis work or, in their absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of Saskatchewan in any scholarly use which may be made of any material in my thesis.

Disclaimer

Reference in this thesis to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the University of Saskatchewan. The views and opinions of the author expressed herein do not state or reflect those of the University of Saskatchewan, and shall not be used for advertising or product endorsement purposes.

Requests for permission to copy or to make other uses of materials in this thesis in whole or part should be addressed to:

Head of the Department of Computer Science
176 Thorvaldson Building, 110 Science Place
University of Saskatchewan
Saskatoon, Saskatchewan S7N 5C9 Canada

OR

Dean
College of Graduate and Postdoctoral Studies
University of Saskatchewan
116 Thorvaldson Building, 110 Science Place
Saskatoon, Saskatchewan S7N 5C9 Canada

Abstract

The sharing of academic achievement certificates and credentials requires enhanced security measures to ensure faultless and fraud-free practices, while also prioritizing data trust and user privacy. It is crucial to provide convenience and secure control over access rights based on user roles. Traditionally, educational institutions issue hard copy certificates to students who have fulfilled the prerequisites. However, when it comes to sharing validated certificates, especially for students pursuing higher studies, different issuers follow varied approaches. The traditional method of mailing certificates involves time-consuming and costly back-and-forth involvement with universities. Similarly, email-based approaches raise concerns regarding trust and authenticity. In all of these approach there exist intermediaries that are need for verification and validation. Existing sharing platforms restrict student's control over their data and limit the validation process. Moreover, once a certificate is shared through these methods, students often lose control over its further usage and distribution, which is not an ideal approach.

Until recently, there was no standardized approach to accurately monitor and verify the sharing of certificates, including the sender, recipient, and conditions. However, with the emergence of distributed ledger technologies, specifically designed for NFTs, a decentralized peer-to-peer network has now become the most efficient solution to address these challenges. This technology enables secure and verifiable sharing of certificates, ensuring transparency, trust, and greater control for students over their credentials. By utilizing NFTs, students can retain ownership and control over their certificates even after sharing them, thereby eliminating the concerns of loss of control and unauthorized distribution.

To achieve this, a distributed application layer was added on top of the centralized system to create a more feasible and practical approach. This study focuses on utilizing a permission-less blockchain, specifically the public network of the Ethereum blockchain, to develop a secure data sharing framework. The research proposes an architecture and delves into the necessary components and factors to consider during the design and implementation of the system. The aim is to provide students with complete ownership and permanent access to their digital certificates, which are verified by the university and accepted by employers. This framework supports immutability, authenticity, enhanced security, trusted records and is a promising means to share academic certificates involving students, universities and employers.

The framework is evaluated via a user study. The extended Technology Acceptance Model(TAM) and a Trust-Privacy Security Model are used to evaluate the usability of the NFT-framework. The evaluation allows uncovering the role of different factors affecting user intention to adopt certificate-sharing platforms. The result of the evaluation point to guidelines and methods for embedding privacy, user transparency and drivers of using the application.

List of my peer-reviewed publications with contents from this dissertation

- **P. Khati**, A. K. Shrestha and J. Vassileva, "Non-Fungible Tokens Applications: A Systematic Mapping Review of Academic Research," 2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2022, pp. 0323-0330, doi: 10.1109/IEMCON56893.2022.9946500.
- **P. Khati**, A. K. Shrestha and J. Vassileva, "Student Certificate Sharing System Using Blockchain and NFTs," 2023 Blockchain and Application 5th International Congress Conference, Guimaraes, Portugal, 2023

Acknowledgements

First and foremost, I would like to thank my supervisor Dr. Julita Vassileva for all the support, guidance, encouragement, and motivation during my master's journey. I am grateful that I had the chance to work under your supervision. Thank you so much for your mentorship, and for all the resources you have provided me with. I would also like to thank my advisory committee member Dr. Ralph Deters and Dr. Li Chen for your support, constructive feedback and invaluable suggestions . Thank you so much for your mentorship, and for all the resources you provided me with.

I am deeply thankful to all the members of the Multi-User Adaptive Distributed Mobile and Ubiquitous Computing (MADMUC) Lab and Computer Science Department, especially Dr. Ajay Shrestha who supported me throughout this journey. Finally, I would like to thank my parents, my brother Prayash and my loving wife, Sangeeta for their continuous support and encouragement.

Contents

Permission to Use	i
Abstract	ii
List of My Peer-Reviewed Publications with Contents from this Dissertation	iii
Acknowledgements	iv
Contents	v
List of Tables	vii
List of Figures	viii
List of Abbreviations	ix
1 Introduction	1
1.1 Motivation	1
1.2 Research Problem	2
1.3 Research Questions	3
1.4 Research Objectives	3
1.5 Thesis structure	4
2 Literature Review	5
2.1 Blockchain	5
2.1.1 Ethereum	6
2.2 Smart Contract	7
2.3 Non Fungible Token	8
2.4 Blockchain based Certificate Sharing Systems	10
2.5 InterPlanetary File System	14
2.6 Technology Acceptance Model	15
2.7 Summary	17
3 Proposed Design and Architecture	18
3.1 System Overview	18
3.1.1 Application Layer	19
3.1.2 Authentication Layer	20
3.1.3 Verification Layer	21
3.1.4 Blockchain Layer	21
3.1.5 Storage Layer	22
3.2 System Architecture	23
3.2.1 SignIn with Ethereum	26
3.2.2 Ethereum Query Gateway	27
3.2.3 Ethereum Wallet	28
3.3 System Development	29
3.3.1 User Interface	31
3.3.2 NFT Smart Contracts Deployment	38
3.3.3 NFT Smart Contracts Execution	40
3.4 Conclusion	42

4	System Evaluation: Methodology, Experiment Design, and Result	44
4.1	Methodology	44
4.2	Research Hypotheses	45
4.3	Experiment Design	46
4.3.1	Data Collection	49
4.4	Result	51
4.4.1	Descriptive Statistic	51
4.4.2	Measurement Models	54
4.4.3	Structural Model	58
4.4.4	Participants Comments	61
4.5	Discussion	62
4.6	Conclusion	63
5	Conclusion and Future work	64
5.1	Research Contributions	65
5.2	Limitations	65
5.3	Future work	66
	References	67
	Appendix A NFT Solidity Contract	70
	Appendix B Ethics Approval	74
	Appendix C Recruitment Form	75
	Appendix D Consent Form and Survey Questionnaire	76

List of Tables

4.1	Definitions of Constructs	46
4.2	Construct and items	47
4.3	Participants' demographics	50
4.4	Score Ranges and Categories	51
4.5	Analysis of Perceived Ease of Use (PEOU)	52
4.6	Analysis of Perceived Usefulness(PU)	52
4.7	Analysis of Intention to Use (ITU)	52
4.8	Analysis of Attitude towards the System (ATS)	53
4.9	Exploratory factor loading	55
4.10	Reliability Measures	56
4.11	Reliability and Validity Measures	57
4.12	Fornell-Lacker criterion Matrix	58
4.13	Direct Path Coefficient Analysis	60
4.14	Indirect path coefficient analysis	60
4.15	Total effect path coefficient analysis	61
4.16	Summary of Hypotheses Results	61
4.17	Important Comments from User Study	62

List of Figures

2.1	Applications of NFTs in different domains [22]	9
2.2	A classical TAM model [12] [13][14]	15
3.1	A general NFT certificate sharing system overview	19
3.2	Sample Data on Google Firestore Database	24
3.3	System Architecture	25
3.4	Example Message of SignIn with Ethereum	26
3.5	A Screenshot showing VS Code Setup	30
3.6	Google Firebase Console Interface	31
3.7	NFT certificate sharing dashboard	32
3.8	NFTcertificate SignIn Using Metamask	32
3.9	Student Original NFT certificate Dashboard	33
3.10	Student Dashboard After Certificate Issued	33
3.11	Student ViewNFT Minting Dashboard	34
3.12	Student Triggering Minting Transaction	35
3.13	Student ViewNFT Dashboard For All Certificate	35
3.14	Student Transferring Viewing Rights to ViewNFTs	36
3.15	Student Retrieving ViewNFT	36
3.16	University Collection	37
3.17	University Student profile	37
3.18	University Student NFTs description	38
3.19	Hardhat Configure	39
3.20	Remix IDE	39
3.21	ViewNFT Certificate Metadata JSON	40
3.22	Smart contract of NFT based certificate sharing system	41
3.23	Smart Contract Execution Sequence diagram	43
4.1	An extended TAM model for my study	45
4.2	Analysis of all the constructs	53
4.3	Analysis of all the constructs	59

List of Abbreviations

NFT	Non Fungible token
CAD	Canadian Dollars
DApps	Decentralized Applications
ETH	Ether(Ethereum Crypto Currency)
IPFS	InterPlanetary File System
TAM	Technology Acceptance Model
CID	Content Identifier
HTTPS	Hypertext Transfer Protocol
API	Application Programming Interface
RPC	Remote Procedure Call
JSON	JavaScript Object Notation
CLI	Command Line Interface
PoW	Proof of Work
PoS	Proof of Stack
ATS	Attitude Towards the System
DLT	Distributed Ledger Technology
ITU	Intention To Use
EVM	Ethereum Virtual Machine
PEOU	Perceived Ease Of Use
PU	Perceived Usefulness
UM	User Model

1 Introduction

Over the past years, the widespread adoption of blockchain technology has captured the attention of various industries. Among the many areas where blockchain holds significant potential for transformation is the sharing and management of educational data. Educational data, including academic certificates and student transcript records, are highly valuable and uniquely identifiable personal information. Leveraging the concept of Non-fungible Tokens (NFTs), which are data units stored on a blockchain certifying the uniqueness of an asset, offers an innovative approach to address the authentication and legitimacy challenges associated with educational certificates. NFTs have gained recognition for their ability to establish the authenticity and provenance of both digital and real-world assets with a digital footprint. While several studies have explored the application of blockchain-based technologies in certificate management, the integration of NFTs within the domain of educational certificate management remains in its early stages of development.

1.1 Motivation

In recent years, there has been a remarkable surge in the number of students pursuing international education or seeking employment opportunities abroad. These students often encounter the need to provide proof of their academic credentials through certificates. However, the conventional paper-based certificate system involves a lengthy process of certification, translation, and authentication, leading to time and cost burdens. Moreover, students with multiple certificates face the tedious task of repeating this process for each credential, resulting in further delays and expenses. Additionally, the inability to retrieve shared certificates poses the risk of misuse and undermines trust in the security of these vital credentials.

To address the challenges of certificate sharing, some institutions have implemented centralized systems based on web2 technology. However, these systems still face obstacles such as the lack of global standardization, often being limited to specific universities or institutions. Another significant drawback is the absence of data provenance, making it difficult to trace the history and origin of certificates. Consequently, issues arise when verifying the authenticity of certificates and the credibility of the issuing institute, undermining trust and legitimacy.

Blockchain and other distributed ledger technologies have emerged in recent years as potential ways to provide reliable records with immutability qualities in a variety of use cases, including healthcare, agricultural research, tourism, etc. The idea of digital certificates has also been developed by these technologies, further strengthening the security and authenticity of data. When used in conjunction with blockchain tech-

nology, digital certificates make use of the technology’s decentralised nature to create and maintain a reliable system for confirming and certifying the identities, transactions, or characteristics of digital entities. These certificates can securely manage and store sensitive information like public keys, ownership information, or credentials by using cryptographic techniques. Additionally, the combination of digital certificates and Non-Fungible Tokens (NFTs) has opened up new avenues. NFTs can act as distinct and unchangeable digital assets thanks to the inherent security and immutability of blockchain technology. Digital certificates can be linked to these assets, whether they stand for works of art, relics, or digital real estate, adding a further degree of authentication and provenance.

A strong ecosystem is built by combining blockchain technology, digital certificates, and NFTs, which protects the validity and integrity of documents and digital assets. This integration revolutionises industries and empowers people online by creating chances for safe identity management, open commerce, and reliable digital ownership.

1.2 Research Problem

In the context of academic certificate sharing, there is a growing need for a robust network that facilitates the exchange of validated data, such as certificates and subject credentials, among students seeking higher studies or exploring exchange opportunities. The existing systems for sharing certificates in a verified manner either rely on traditional methods like postal mail or email or employ centralized systems within groups of universities using digital signatures for verification. However, these systems raise important questions regarding certificate ownership and access rights.

Currently, when a certificate is issued to a student, the student often has limited control over it. Data loss and privacy concerns persist as the existing systems do not offer a mechanism to retain ownership of the certificate after sharing it. Additionally, the process of sharing and validating certificates still relies heavily on the university, leading to delays and dependence on intermediaries. This is especially evident in South Asian countries where physical processes are involved in creating and sharing validated copies of certificates for international study purposes. Furthermore, verifying the authenticity of certificates and identifying the issuing authority can be challenging and cumbersome, lacking a comprehensive data history.

Although some existing systems attempt to address the challenges of physical mail sharing and validation, they fall short in providing a foolproof solution against certificate falsification. Complex methods to falsify certificates still persist, compromising their integrity and reliability.

To tackle these issues, this research proposes an NFT-based blockchain application for academic certificate sharing. The primary objective of this application is to eliminate the reliance on centralized authorities in various scenarios while empowering students with full control over the sharing and ownership of their certificates. By leveraging blockchain technology, the proposed system assigns a unique token, known as an NFT, to each certificate. This token is associated with a hash and digital signature, enabling verification

and validation by the intended recipients, such as employers or universities. The system ensures that the ownership of the NFT certificate remains with the student throughout its life cycle.

Furthermore, the proposed framework addresses the challenge of sharing multiple certificates for different purposes, such as job applications or admission to educational institutions or research labs. Through the framework, students can create additional viewNFTs based on the original NFT certificate, allowing them to tailor the transcript to specific requirements. This customization enhances the relevance and clarity of the certificates while still ensuring easy verification by interested parties.

The proposed NFT-based blockchain application aims to address the significant challenges faced by existing systems for sharing academic certificates, including security, validation, ownership, and integrity. By providing students with control over their certificates and enabling secure sharing and easy verification, this application has the potential to revolutionize the certificate sharing process and provide a tamper-resistant and ownership-centre solution for academic credentials.

1.3 Research Questions

1. How can the NFT-based blockchain application ensure secure and tamper-resistant sharing of academic certificates while providing students with full control over the ownership and access rights of their certificates?
2. What are the potential benefits and drawbacks of implementing an NFT-based blockchain system for academic certificate sharing, and how do they compare to existing systems in terms of security, validation, ownership, and integrity?
3. How can such platforms be constructed and then evaluated based on the user experience models?
4. How do the multidimensional constructs, encompassing technical and usability factors, influence the attitudes and behavioral intentions of users to adopt and utilize the NFT-based system for certificate sharing?

1.4 Research Objectives

Based on the aims of this research, the following research objective is defined:

1. To conduct a literature review and background study:

The objective is to review relevant literature on NFT-based frameworks for certificate sharing, exploring existing systems and methods for user-controlled ownership and secure sharing of academic certificates. The aim is to identify gaps and explore how NFT technology can enhance privacy, security, and user control in certificate sharing.

2. To design and develop a decentralized certificate data sharing framework based on NFT technology:

The objective is to design and develop a decentralized framework utilizing NFT technology for secure and transparent certificate sharing. This involves defining the architecture, protocols, and algorithms for a decentralized network to store, verify, and share certificates among stakeholders. The framework should leverage NFT properties, such as ownership, uniqueness, immutability and traceability, to ensure integrity and authenticity of shared certificate data.

3. To implement the NFT-based certificate sharing framework:

The objective is to practically implement the designed decentralized certificate sharing framework based on NFT technology. This involves developing software components, smart contracts, and user interfaces to realize the framework. The implementation should adhere to defined protocols, integrate seamlessly with blockchain infrastructure, and provide necessary functionalities for certificate issuance, verification, sharing, and ownership control.

4. To evaluate the user experience model and the framework using an extended Technology Acceptance Model (TAM) approach:

The objective is to assess user experience of the implemented NFT-based certificate sharing framework using an extended TAM approach. This involves conducting usability studies to evaluate ease of use, user satisfaction, and perceived usefulness. Additionally, user intentions to adopt and utilize the framework for certificate sharing will be analyzed. The extended TAM model will provide insights into factors influencing user acceptance, allowing for refinement and optimization to enhance user experience and encourage widespread usage.

1.5 Thesis structure

This thesis is organized as follows. Chapter 2 present the related work and literature review for this thesis. It includes the necessary background on blockchain, smart contract, Non fungible token and different frameworks and their role in digital certificate sharing. Additionally, it provides some background information on the heuristic behavioural model based on the cognitive schemes' technology acceptance model (TAM). Chapter 3 gives a detailed description of the certificate sharing framework and how it was implemented with reference to my published paper entitled "Student Certificate Sharing Using Blockchain and NFTs". Chapter 4 presents an evaluation of the framework using the extended TAM model. The model aims to identify constructs affecting the framework adoption that influence the usability and intention to use. Chapter 5 concludes the thesis, summarizes the findings and contribution of the research and discusses the limitations and future work on the topic of certificate sharing framework.

2 Literature Review

In this section, I reviewed the relevant literature on blockchain and other related technologies such as smart contracts and non fungible token, that are relevant to building a credential/certificate sharing solution.

2.1 Blockchain

Blockchain technology has emerged as a groundbreaking innovation with the potential to transform industries and reshape the way we conduct transactions, store data, and establish trust. At its core, a blockchain is a decentralized and distributed ledger that records transactions across multiple computers or nodes [22]. Each transaction, or block, is cryptographically linked to the previous block, forming an unalterable chain of information. This structure ensures the immutability and security of the data stored on the blockchain [26]. One of the key features of blockchain is its ability to provide transparency and trust in a trustless environment. Every transaction recorded on the blockchain is visible to all participants, eliminating the need for intermediaries and enhancing accountability. The decentralized nature of blockchain ensures that no single entity has control over the data, reducing the risks of manipulation, fraud, and censorship. Here, the blockchain technology is powered by a consensus algorithm.

A consensus algorithm is a set of guidelines that govern how consensus is obtained among network participants. Consensus algorithms are essential for maintaining the blockchain's reliability and integrity. Blockchain networks use a variety of consensus techniques, each with unique properties and benefits. Proof of Work (PoW), which was first described by Satoshi Nakamoto in the original Bitcoin whitepaper [26], is one widely utilized consensus algorithm. Participants in a blockchain with a PoW algorithm are called miners, and they compete to solve challenging mathematical puzzles. New bitcoin coins are awarded to the miner who completes the problem first, and they are also in charge of adding a new block to the blockchain. This algorithm makes sure that a lot of calculation effort is done, which makes altering the blockchain's history challenging and resource-intensive.

Another popular consensus algorithm is Proof of Stake (PoS)[17]. In PoS-based blockchains, participants, known as validators, are chosen to create new blocks based on the number of coins they hold and are willing to "stake" as collateral. The higher the stake, the greater the chance of being selected as the validator. This algorithm eliminates the need for miners and the associated energy consumption of PoW, making it more environmentally friendly. It also provides a financial incentive for validators to act honestly, as they can lose their staked coins if they attempt to manipulate the blockchain. Recently one of the popular blockchain

”Ethereum ”shifted to PoS-based consensus algorithm.

Blockchain technology has distinctive qualities that add to its worth and differentiation. Immutability stands out as a crucial characteristic since it makes it very difficult to change or delete a block’s contents after it joins the blockchain. Blockchain is the best technology for applications that require tamper-proof records due to this feature’s strengthening of data integrity and security. Another important feature of blockchain is decentralization, as it runs on a dispersed network of nodes, each of which has a full copy of the blockchain. With no need for middlemen or centralized authorities, this decentralized structure reduces the possibility of single points of failure and makes it possible for trustless peer-to-peer transactions. By keeping a record of every transaction on the blockchain and making it accessible to all parties, blockchain also promotes transparency and auditability. This transparency enhances accountability and trust within the system, streamlining auditing processes and enabling efficient asset and transaction traceability. When a new transaction happens, it propagates over the network and is added to a block along with other pending transactions. Then, miners or validators compete to solve the blockchain’s related consensus algorithm. When there is unanimity, the block is added to the blockchain and linked to the preceding block using cryptographic hashes. A continuous chain is created as a result of this procedure, representing the entire transaction history. Participants approve transactions by checking cryptographic signatures and adherence to the consensus algorithm’s rules to ensure security and integrity. This validation procedure dramatically reduces the likelihood of hostile actors tampering with or changing recorded data, together with the decentralized and immutable characteristics of the blockchain.

The integration of blockchain technology has unlocked a wide range of potential applications, including in the field of education. The implementation of blockchain in education has facilitated various innovative use cases, such as enhancing credential verification, ensuring data integrity, and enabling decentralized learning platforms. Numerous studies have explored the potential of blockchain in education [15, 1], highlighting its ability to transform traditional educational systems and empower learners and institutions alike.

2.1.1 Ethereum

Ethereum, conceived by Vitalik Buterin in late 2013 [5], stands as a prominent player in the blockchain 2.0 landscape. Gavin Wood introduced its initial specification in early 2014 [38]. Ethereum distinguishes itself by incorporating the Ethereum Virtual Machine (EVM) code, a built-in Turing-complete programming language that enables users to create decentralized applications and define rules through smart contracts [5]. While the EVM code operates at a low-level bytecode language, smart contracts are typically written in high-level languages like Solidity and Vyper. Once deployed on the blockchain, smart contracts become immutable, preventing any modifications, including bug fixes.

The Ethereum blockchain comprises two types of accounts: externally owned accounts and contract accounts. Externally owned accounts are controlled by private keys, while contract accounts are governed by code. Both types of accounts can hold balances of Ether (ETH), the native currency token of the platform.

To regulate transactions, Ethereum employs Gas units as fees to deter abuse and prevent infinite loop execution in smart contracts [38, 5]. Gas serves as a computational step limit, with each step carrying a fixed cost and corresponding to a low-level operator. If a transaction’s Gas allowance is insufficient, the computation is reversed, but the Gas is still consumed. Miners, responsible for network operation, receive these fees as rewards. Miners also have the discretion to ignore transactions with insufficient Gas prices, leading to a trade-off for transactors between Gas price and processing time.

Ethereum provides two options for utilization: joining the public network or running a private/hybrid version, each with its own advantages and disadvantages. Public blockchains, characterized by decentralization, offer high immutability but may experience limitations in transaction throughput and latency due to the extensive propagation of transactions and blocks among numerous nodes. On the other hand, private and consortium blockchains restrict the number of participants, resulting in faster transaction processing but lower resistance to tampering. Privacy is another critical consideration, with public blockchains exposing all transactions to the public while permissioned blockchains control data access. Public networks eliminate infrastructure costs, unlike the private approach where users are responsible for network setup and management [7]. Moreover, the widespread adoption and value held in a public network attract individuals invested in its security, contributing to decentralized management.

Decentralization remains a fundamental characteristic of blockchain technology, making it vital to consider when choosing between a public or hybrid blockchain [6]. The Ethereum whitepaper emphasizes the aim of providing a blockchain platform for custom applications rather than requiring the creation of individualized Bitcoin-based versions. It argues that most custom applications lack the scale to maintain their own blockchain network with a robust decentralized consensus protocol [5].

2.2 Smart Contract

The Ethereum community introduced an automation layer on top of a public permissionless blockchain using smart contracts executed by the decentralized network. Smart contracts are pieces of executable codes that get executed when triggered by an authorized or agreed event [34]. They can be regarded as “if/then” condition statements stored on the distributed ledger. The state-transition mechanism provides the foundation for the applications built on top of smart contracts. One of the remarkable aspects of smart contracts is that all participants within the network share the states containing the instructions and parameters, ensuring transparency in the execution of instructions. This shared state mechanism guarantees that the performed instructions are accessible and visible to all parties involved. Consequently, blockchain technologies with smart contracts are extensively utilized in numerous Non-Fungible Token (NFT) applications to ensure ownership, provenance, and exclusivity of the assets governed by these smart contracts [22].

Solidity, the programming language used to write smart contracts, allows performing basic operations on its data types, resulting in lightweight code. These smart contracts, written in Solidity, are executed on the

Ethereum Virtual Machine (EVM), which consists of bytes representing different operations. Therefore, the integration of smart contracts, Solidity, and the Ethereum Virtual Machine (EVM) into blockchain technology has transformed the way transactions and agreements are carried out. This automation layer, facilitated by Solidity and executed on the EVM, enables automated execution based on predefined conditions. By leveraging the transparency and security provided by the blockchain, this technology allows for innovative applications like NFTs, where the underlying smart contracts and the EVM guarantee the authenticity and uniqueness of digital assets.

2.3 Non Fungible Token

A non-fungible token (NFT) is a unique piece of data stored on a blockchain that certifies the uniqueness of an asset. It can represent various items, ranging from works of art and music to collectibles, proof of purchase, rare postal stamps, real estate, and physical artwork. The tradability of these assets has garnered significant attention in recent years. NFTs allow for the digital trading of assets between parties, facilitated by automated payment and asset transfer through smart contracts on a token standard blockchain like Ethereum. In the context of Ethereum, the transfer of value and information between accounts causes a transaction to be recorded in the global state of the blockchain ledger. And in most cases, a native token such as Ether (ETH) is used as the standard fungible currency. One of the most commonly used standards to create NFT is the ERC-721 standard, which was introduced by the Ethereum community, and still dominates the market[22].

Tokens, in general, serve as objects representing something, such as a title certificate or a representation of facts. Through asset tokenization, ownership of real-world or digital objects can be transferred into digital tokens. In Ethereum, tokens are assets built on top of a blockchain, and smart contracts are used to implement tokens other than the native cryptocurrency. Tokens can be categorized into two types: fungible and non-fungible. Fungible tokens, like cryptocurrency coins, are interchangeable, with each coin being equivalent to any other coin. Fungible tokens typically conform to the ERC-20 standard. On the other hand, non-fungible tokens are distinct and non-interchangeable, representing ownership of specific digital assets cryptographically. The ERC-721 standard governs the creation and maintenance of non-fungible tokens, while ERC-1155 extends the standard's functionality, allowing for the management of multiple token types within a single contract[22].

Every token possesses a token symbol, Token ID, a distinct token contract address, creator address, transaction history, and metadata, which represents the actual content of the token. Due to the potentially large volume of metadata, storing it directly on the blockchain can be costly. Instead, the metadata is stored off-chain, and a hashed link to the metadata is stored on the blockchain. By storing the metadata off-chain, hashing its link, and associating it with the NFT, the expenses of creating asset NFTs can be effectively reduced.

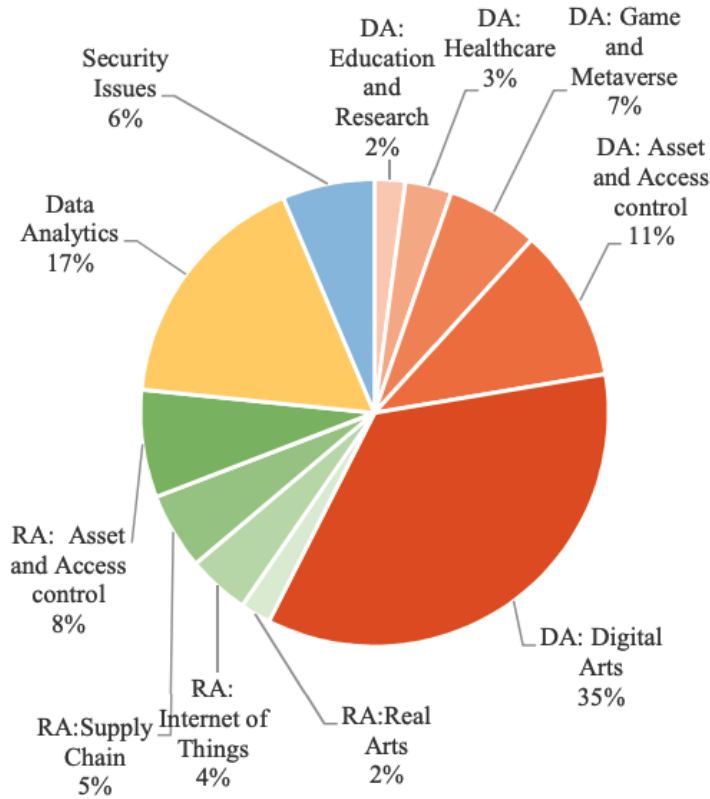


Figure 2.1: Applications of NFTs in different domains [22]

Initially, NFT technology found application primarily in the digital arts community. However, the rise in NFT trading market value in recent years has led to increased interest and exploration of NFTs across various domains. Research and applications have expanded beyond digital arts to include physical arts, physical assets like land plots and buildings, and virtual worlds within game-based platforms. In decentralized metaverses, such as virtual worlds, NFTs enable gamers to trade virtual land and digital representations (digital twins) of physical assets tokenized by NFTs. These digital twins represent unique digital assets and signify ownership of the corresponding physical assets. Apart from the virtual world and digital arts domains, there have been multiple research and application experiments involving NFTs, including tokenizing software licenses as subscription NFTs and transforming existing certification standards into NFTs. I have observed from my systematic review of about 106 scientific papers [22], the application of NFTs is found in various domains such as IoT, Supply chain, Asset and Access control, Education and Research, Healthcare, Game and Metaverse where properties like authentication, ownership, transferability, interoperability, standardization, security, and privacy play essential roles (see Figure 2.1).

2.4 Blockchain based Certificate Sharing Systems

Blockchain technology has the potential to revolutionize the way we share data, issue and verify credentials. In the early years of application of blockchain and its success in FinTech world, the attention shifted on how the properties of blockchain can be implemented in other application and also find out what things can be done that were not possible with the existing technology. Some of the promising areas of blockchain implementation were on education and educational data sharing, from research data to certificate credentials. The majority of approaches used bitcoin blockchain [25]. According to Nazaré et al. [36], a platform has been put forth as part of the Digital Certificates Project, aiming to facilitate the creation, sharing, and verification of educational certificates based on blockchain technology. This project, led by the Media Lab Learning Initiative at the Massachusetts Institute of Technology (MIT), focuses on utilizing the Bitcoin blockchain. The primary objective of this initiative was to tackle the challenges associated with digitizing academic certificates. However, it should be noted that this particular approach does not delve into exploring the potential use of blockchain in the context of a comprehensive global higher education credit and grading platform.

EduCTX [36] is a global higher education credit platform based on blockchain technology. It aims to create a decentralized and trusted environment for managing academic credits and grading systems. The platform leverages the concept of the European Credit Transfer and Accumulation System (ECTS) and uses ECTX tokens as a representation of credits earned by students for completed courses. EduCTX operates on a globally distributed peer-to-peer network, powered by the Ark Blockchain Platform. This network ensures transparency, immutability, and security of educational data. By utilizing blockchain technology, EduCTX seeks to provide a unified perspective for students, higher education institutions (HEIs), and other stakeholders like companies and organizations. Higher education institutions (HEIs) have the opportunity to become part of the EduCTX Blockchain network by joining as nodes. By doing so, they receive support and recognition from other HEIs in the network. EduCTX aligns with the European Credit Transfer and Accumulation System (ECTS) concept, which involves issuing and managing ECTX tokens. These tokens represent the credits earned by students upon completing courses, similar to the ECTS system. To validate their completed courses, students can share their Blockchain wallet addresses and exchange scripts with overseas universities or companies for verification purposes. EduCTX was among the first to offer a prototype implementation that demonstrated the feasibility of its concepts. In addition, it served as a first step towards a more transparent and technologically advanced higher education system. The concept of the proposed blockchain network is to connect multiple key participants in the existing education system through the use of blockchain technology. However the platform currently does not implement smart contract functionality, which limits its potential for automation and programmability. Smart contracts are essential for ensuring secure and reliable diploma issuance processes, as they can enforce predefined rules and conditions. The EduCTX platform does not provide a robust solution for safeguarding the confidentiality of student data.

The "right to be forgotten" principle defined in the GDPR [19] emphasizes the need for data privacy, especially in educational contexts. Storing only the hash of the diploma instead of the entire document can help protect student data, but EduCTx currently lacks this capability.

The "Blockchain for Education" platform [30] is a conceptual system architecture designed to address the challenges faced by certification authorities, learners, and employers in managing and verifying certificates. The framework offers a range of features tailored to each user groups: certification authorities, learners, and employers. Certification authorities benefit from features such as data import, certificate browsing, bulk certificate printing, signing and storing certificates on the blockchain, validation of certificate authenticity, and the ability to revoke certificates if needed. Learners can import their certificates, create application portfolios, manage and share them with potential employers, receive notifications on employer interactions with their certificates, and monitor time-limited certificates. However, they do not have ownership over their certificates. Employers, on the other hand, can read and verify certificates, streamlining the process of confirming their authenticity. Overall, the platform offers a comprehensive set of features to address the needs of these user groups in the certification ecosystem.

In addition to the features mentioned, the platform incorporates IPFS (InterPlanetary File System) for profile information storage, ensuring secure and decentralized storage of user data. The use of blockchain technology ensures that ownership of certificates remains on the blockchain, providing an immutable record of achievements. However, the platform lacks access control features, one limitation of the implemented system is that once the student shares a certificate, the student loses access to that certificate as it will be transferred to the employer. Student can no longer retrieve back the certificate after sharing it. The employer can verify the student certificate authenticity by comparing the hash value only. Furthermore, features such as sign-in method to the framework, which could be an important aspect of user authentication and access control is not present in the proposed framework. Additionally, the access rights and limitations of each user group are not detailed, leaving room for ambiguity in terms of what actions and functionalities are available to different types of users.

To further enhance the "Blockchain for Education" platform, the integration of Non-Fungible Tokens (NFTs) can be deployed. NFTs would provide a means to include richer metadata and additional verification mechanisms for certificates. Each certificate could be represented by a unique NFT, enabling more granular tracking and verification of individual credentials. This integration would enhance the platform's functionality and offer a more comprehensive and robust solution for managing and verifying educational certificates. Therefore, in this thesis I have used NFT as a key element to enhance the abilities of the existing systems.

VECEfblock [27] is a blockchain-based system designed specifically for education certification in Vietnam. The existing problem in the country is the lack of trustworthiness in diplomas and certificates, as there is no efficient way for anyone other than the issuer to authenticate them. This is mainly due to the absence of a reliable certificate database or, in some cases, the unreliability of the available data. To address this issue, VECEfblock introduces a hybrid solution that combines the use of blockchain technology and an application

layer. The primary objective of VECefblock is to establish trust and ensure the authenticity of educational certifications. The blockchain layer serves as a secure and tamper-resistant storage for the certification data, while also providing mechanisms for validation and data sealing. This ensures that the certificates cannot be forged or tampered with. On the other hand, the application layer facilitates the interaction with the data, allowing relevant parties to access and verify the certifications as needed. By leveraging blockchain technology, VECefblock aims to overcome the limitations of traditional certification systems in Vietnam. It provides a transparent and decentralized approach to certification management, enabling reliable verification and authentication processes. With VECefblock, educational institutions, employers, and other stakeholders can have confidence in the trustworthiness of diplomas and certificates, thereby addressing the issue of fake or unreliable credentials in the country.

However, it is important to note that the choice of Hyperledger Fabric for VECefblock in Vietnam’s education certification system is primarily driven by the need for control and governance. The permissioned nature of Hyperledger Fabric aligns well with the specific requirements of the system, allowing authorized entities such as educational institutions and relevant authorities to have restricted access to the network and participate in consensus processes. This level of control is crucial for maintaining the integrity and security of certification data, but it has limitations. While Hyperledger Fabric [2] offers significant advantages in terms of privacy and permissioned access, it is worth acknowledging that a public and permissionless blockchain platform, for example Ethereum’s open and decentralized nature enables broader participation and transparency, making it suitable for applications where inclusivity and public trust are paramount. Additionally, Ethereum’s native support for smart contracts provides programmability and automation capabilities that could enhance the functionality of the certification system. For instance, the use of non-fungible tokens (NFTs) on Ethereum could enable unique ownership of certificates, as each certificate represents an individual’s unique achievement. Moreover, smart contracts on Ethereum can facilitate seamless sharing of certificates with multiple institutions and employers, allowing for easier verification and validation.

The “Eternal Digital Certificate” [28] is a comprehensive school management system that leverages blockchain technology and non-fungible tokens (NFTs) to handle summer school events and certificate issuance. The system comprises multiple components: a user-friendly React application as the interface, smart contracts deployed on the Polygon Supernets blockchain (or any Ethereum-based platform), and an IPFS storage component. Users access the React application and authenticate themselves using their Ethereum private keys via crypto wallets such as Metamask. While all users can view the events list, only authenticated participants gain access to detailed event information. The smart contracts, namely the Faculty State Contract and EDC Certificate Contract, operate on the blockchain platform. The Faculty State Contract stores all event-related data, allowing administrators to manage events, courses, participants, grades, and certificates. While anyone can read the contract’s current state, only administrators possess the permissions to modify or delete data. The EDC Certificate Contract stores student certificate data as NFTs, ensuring tamper-proof and easily verifiable certification. Each student receives a unique NFT per event, with the

contract providing functions for issuing and retrieving certificate NFTs. The NFT metadata is stored on the IPFS, and the contract stores the URI pointing to this data. Administrators exclusively possess the authority to issue certificates once students have successfully completed their assigned courses.

To summarize, the "Eternal Digital Certificate" system offers a user-friendly solution for managing summer school events, issuing NFT-based certificates, and securely storing all pertinent data on the blockchain platform and IPFS. The system can issue only one certificate per event or per academic achievement, however, which limits the sharing capacity, for example, if a student wants to apply to multiple educational institutions or jobs. To address this limitation, a potential solution would be to implement a system that allows students to generate multiple certificates or NFTs for different contexts. This could involve creating a mechanism within the system that enables students to select the specific event or set of courses they want to generate a certificate for. By allowing flexibility in issuing certificates, students can cater to various employment opportunities or schools and include in the each the certificate specific achievements they wish to highlight. It is also important to note that the "Eternal Digital Certificate" system described in [28] is not currently implemented and evaluated. It is included in this review primarily because it emphasizes the significance of NFTs in ensuring tamper-proof and easily verifiable certificates.

NFTCert [40] is a platform that allows the educational institution to create their student NFT-based certificates and transfer the ownership to the student. It also provides hash value for verifying the authenticity of NFT-based certificates. The control over the data is only accessible to the owner who mints the NFT, in this case the University. The platform also incorporated blockchain Oracle to add an online payment gateway for the necessary payment to retrieve the certificate. In terms of the technical implementation, NFTCert defines its own digital certificate data format and incorporates the students' personal information and certificate information along with their signatures. These certificates are then issued to the students and stored in their digital wallets. To facilitate the minting process, NFTCert introduces an online payment gateway, allowing participants to make necessary payments for certificate issuance without relying on cryptocurrency transactions. However, in NFTCert [40], only the educational institution has the right to mint the NFT. From the student point of view, this approach is time consuming as it involves more interactions with the institution. Unfortunately, the paper [40] does not clearly state whether the ownership or the right to access the NFT is transferred to the student; this makes the student completely dependent upon the institute. Also, similar to other existing systems, here too the student cannot create purpose-based views of their full data as certificates. For example, if a student is applying for a software developer job, not all subjects or credits that he studied might be relevant to that particular job, and it would have been convenient if the student could provide the potential employer with only a selection of the grades for the relevant subjects. This should not compromise the authenticity of the credential issued by the university. Furthermore, this platform focuses on NFT certificate management rather than sharing the NFT certificate and is centered towards private network implementation. This may limit the scope of the system and may not meet the needs of all stakeholders.

In summary, the showcased blockchain-based systems, such as EduCTX, Blockchain for Education, VE-

Cefblock, Eternal Digital Certificate, and NFTCert, have demonstrated their potential to tackle issues related to education credential management and verification. These systems harness blockchain technology and, in some instances, NFTs to enhance security, transparency, and trust within the certification process. However, they all share certain limitations. Firstly, many of these systems do not fully capitalize on the capabilities of NFTs, resulting in a lack of unique ownership and detailed tracking of certificates by students, thereby limiting their ability to offer comprehensive credential management solutions. Additionally, some are confined to closed platforms or specific regions, curtailing scalability and inclusivity, while open and public blockchain platforms like Ethereum offer broader participation and transparency. Moreover, none of the existing systems empower students to tailor their certificates for various purposes, potentially impeding adaptability to diverse employment opportunities or academic pursuits. Another notable gap in all of these systems is the absence of usability and user acceptance evaluations, creating a significant knowledge void regarding their real-world performance and user perceptions.

To address these limitations I propose to design an open certificate sharing system that is student-centered, giving the student ownership and control over the generation and management of their certificate and to evaluate its usability in a study. I will deploy Blockchain and the Interplanetary File system to ensure openness and security, and NFTs to ensure student ownership and control. Finally I will conduct a comprehensive usability and user acceptance evaluation of the proposed framework based on the Technology Acceptance Model. In the next two sections, I provide an overview of the Interplanetary File System and TAM - a well-established and widely-utilized methodology for evaluating interactive systems, underscoring its relevance in assessing the proposed NFT-based blockchain credential management solutions.

2.5 InterPlanetary File System

The InterPlanetary File System (IPFS) was developed by Benet in 2014 [3] as a peer-to-peer distributed file system with the aim of connecting all computer devices. It operates on the principle of content addressing, where the address of a file stored in IPFS corresponds to its content. This means that if the content of a file changes, the address for retrieving the current version of the file also changes, rendering the old address invalid. This unique feature ensures that any modifications to the file's content in IPFS will result in a new address, preserving data integrity.

IPFS offers an innovative solution for storing and distributing files on the public blockchain. Instead of storing the complete file on the blockchain, only the IPFS address (Content Identifier or CID) of the file is stored. This approach significantly reduces the size of data stored on the blockchain, resulting in cost savings. Importantly, this method does not compromise the transparency and traceability of the file. The CID of an IPFS file is generated using a hashing algorithm, such as SHA256. The file content is hashed into a hash value, which is then packaged into a Multihash string. This string includes the hash algorithm code, the length of the hash value, and the hash value itself. The Multihash string is then encoded using the Base58 Encoding

Scheme [26] to form the CID or IPFS address of the file. By default, IPFS files start with "1220" in their Multihash strings, and the resulting CID is a 46-character string starting with "Qm" (Qm is the code for 1220 in Base58). IPFS has a rich history and technical foundation. It leverages distributed hash tables (DHTs) and a BitSwap protocol for efficient file distribution and retrieval. Files in IPFS are chunked into smaller blocks, each assigned a unique hash. These blocks are distributed across the IPFS network, promoting fault tolerance and resilience. IPFS also supports versioning and deduplication mechanisms, optimizing storage and bandwidth usage.

2.6 Technology Acceptance Model

The Technology Acceptance Model (TAM) has been extensively used to explain users' adoption of information systems across various domains such as health, business, and education. TAM was derived from the Theory of Reasoned Action (TRA) by Ajzen and Fishbein [18], which emphasizes that behavioral intention is a strong predictor of actual behavior. TAM itself is rooted in social psychology and has been employed as a conceptual framework in the information systems literature to study users' behavioral intention to use a specific technology.

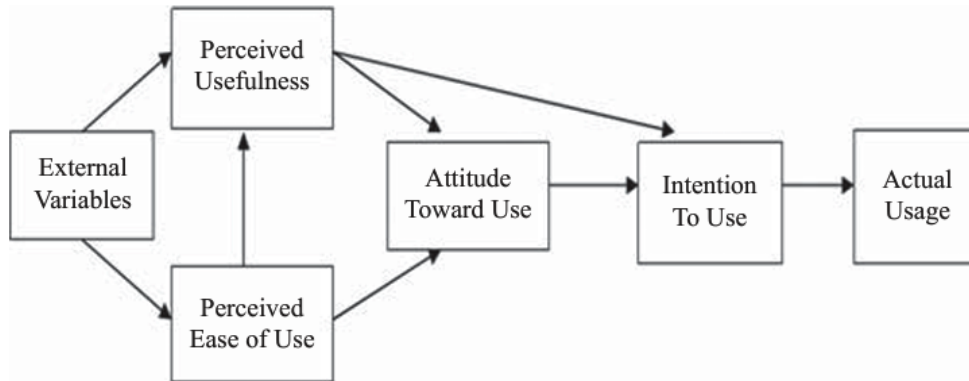


Figure 2.2: A classical TAM model [12] [13][14]

However, while there have been studies applying TAM in the context of blockchain and smart contract applications [35], there is currently a significant knowledge gap in terms of its application to Non-Fungible Tokens (NFTs). NFTs are a unique form of digital assets that are indivisible and cannot be exchanged on a one-to-one basis like cryptocurrencies. They have gained significant attention in recent years, particularly in the art and collectibles market, as they enable the ownership and verification of digital assets using blockchain technology.

In relation to TAM, it is important to note that the model holds that the actual usage (AU) of a system is dependent on the user's intention to use (ITU). In other words, the user's intention to adopt and use a technology plays a crucial role in determining their actual usage behavior. Factors such as perceived

usefulness and perceived ease of use influence the user's intention to use the system. While TAM has been widely applied in various technology adoption studies, including blockchain and smart contract applications, the specific application of TAM to NFTs is an area that lacks sufficient literature and research. Therefore, exploring the factors that influence users' acceptance and adoption of NFTs within the TAM framework would contribute to filling this knowledge gap and understanding the dynamics of NFT adoption.

Many researchers have extend TAM by adding extended constructs such as Perceived Privacy, Perceived Security, Quality of the System, and Trust and they have been recognized as influential factors in determine user acceptance of information technology.

Perceived privacy [4] is a crucial factor to consider when studying privacy concerns and user attitudes towards privacy in the context of a certificate sharing system based on Non-Fungible Tokens (NFTs). Perceived privacy reflects an individual's subjective perception or attitude regarding the control and protection of their personal information. In this regard, previous research by Buchanan et al. (2007) has validated constructs related to privacy concerns and user behavior models, including behavioral items such as general caution and technical protection of privacy, as well as an attitudinal item focused on privacy concern. This research highlighted the significant correlation between privacy concern and general caution, underscoring the importance of user attitudes in influencing privacy-related behaviors. In the specific context of an NFT-based certificate sharing system, perceived privacy plays a critical role in users' acceptance of the technology. Users need assurance that their personal and sensitive information stored within the NFT certificates will be securely protected from unauthorized access. Addressing users' perceived privacy concerns becomes essential in order to foster trust, enhance user satisfaction, and encourage the widespread adoption of NFT-based certificate sharing systems across various domains.

Perceived security [33] is the degree to which a user believes that the online service has no predisposition to risk [39]. The protected personal information may get compromised by theft and fraudulent activities, leading to vulnerability on the internet. Because of this, a sense of security becomes a major concern for users to hand out their details on the network . Perceived security here does not only mean technical security but also the user's subjective feeling of being secured in the network [31] and the lack of subjective security in the user's mind will create hesitation to use systems.

Trust is a crucial factor that influences users' willingness to engage in tasks where they may be vulnerable and rely on the service provider to comply with established protocols [16]. It plays a significant role in building new relationships and developing a sense of reliability in virtual environments [11][21][29]. In sharing information, when users disclose information, their trust in the service provider increases, leading to a reduced sense of doubt and a greater likelihood of engagement. Trust has been found to have a positive and significant impact on users' attitudes and intentions to use systems [29]. It enables users to question the authenticity of online services less frequently, fostering a sense of confidence and reliance.

2.7 Summary

This chapter provided an overview of key topics in blockchain technology, including decentralization, immutability, and transparency. It explained how blockchain ensures data security and integrity through cryptographic linking of blocks, and introduces consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) that maintain the reliability of blockchain networks. Previous works suggesting the integration of blockchain in education, emphasizing its potential to enhance credential verification, data integrity, and decentralized learning platforms were presented. Ethereum was introduced as a prominent blockchain platform that enables the execution of smart contracts. Smart contracts - executable code triggered by specific events, written in languages such as Solidity - were introduced along with their applications in ensuring appropriate data access and modification on blockchain.

Also, the chapter also discussed non-fungible tokens (NFTs) as unique pieces of data stored on a blockchain that certify the uniqueness of an asset. NFTs have gained significant attention and find applications in various domains beyond digital arts, including physical arts, virtual worlds, and research domains. The commonly used ERC-721 standard for creating NFTs was mentioned. Asymmetric cryptography was highlighted as a crucial component of blockchain technology, where pairs of public and private keys are used for secure communication and digital signatures. This cryptographic mechanism ensures data confidentiality, integrity, and authentication within blockchain systems.

Additionally, the chapter highlighted the significance of models in assessing user acceptance and adoption of new technologies and presents the Technology Acceptance Model (TAM), privacy model and trust model. TAM evaluates factors such as perceived usefulness, ease of use, and subjective norms to understand users' attitudes towards technology adoption. The chapter acknowledged that other relevant models may also be considered based on the specific research focus and context. Finally, the chapter reviewed existing solutions and research on blockchain based system with and without NFT implementation focused in academic data storage and sharing. It also discussed the benefits and challenges faced by these systems. The next chapter introduces the design and architecture of a new certificate sharing framework for decentralized ownership and sharing with Ethereum blockchain.

3 Proposed Design and Architecture

The chapter presents the overall architecture of the NFT based certificate sharing system, including an explanation of how the system was designed to solve the problem previously discussed and implementation of an actual certificate sharing application with the purpose of measuring and investigate the performance of the implemented framework for final user study to evaluate its usability.

3.1 System Overview

The system overview outlines a decentralized solution framework for certificate issuance and ownership, prioritizing the ownership rights of students and their control over the data. The workflow supported by the system begins with university administrators registering their institutions and creating profiles that include essential metadata such as the issuer address and signature. This metadata is crucial for verification purposes, ensuring the authenticity and credibility of the certificates issued by the universities. Once registered, students can create their accounts within the system, providing necessary personal information and linking their MetaMask wallets for decentralized authentication. This process guarantees that only legitimate students can access and interact with the system, adding an extra layer of security and trust. In the certificate issuance process, the University begins by generating a hash of the metadata and creating a digital signature using its private key. This signature is then added to the metadata alongside the original information. Additionally, the university generates NFT metadata, mints the NFT, and transfers it to the student's wallet, granting full ownership to the student.

A notable feature of this framework is the flexibility it offers to students. They can choose to mint multiple viewNFTs from their original certificate, which are NFTs created by students themselves. These viewNFTs have a flag that allows students to filter courses while preserving the integrity of other credential information.

Students can include relevant courses as a view transcript with their degree completion certificate and mint them as viewNFT certificates. As the owner, the student can then share and grant access to these certificates and credentials whenever necessary. Importantly, the student retains ownership even after sharing, thanks to the rules established in the smart contract. By sharing the NFT through the receiver's wallet address, students can retrieve the NFT back to their dashboard by adjusting the access rights.

Upon receiving a viewNFT, the recipient is notified that it is a viewNFT and that the student chose to hide certain subjects. Using the university's public key, the receiver can decrypt the digital signature attached to the viewNFT. The resulting hash represents the original NFT from which the viewNFT was derived. To

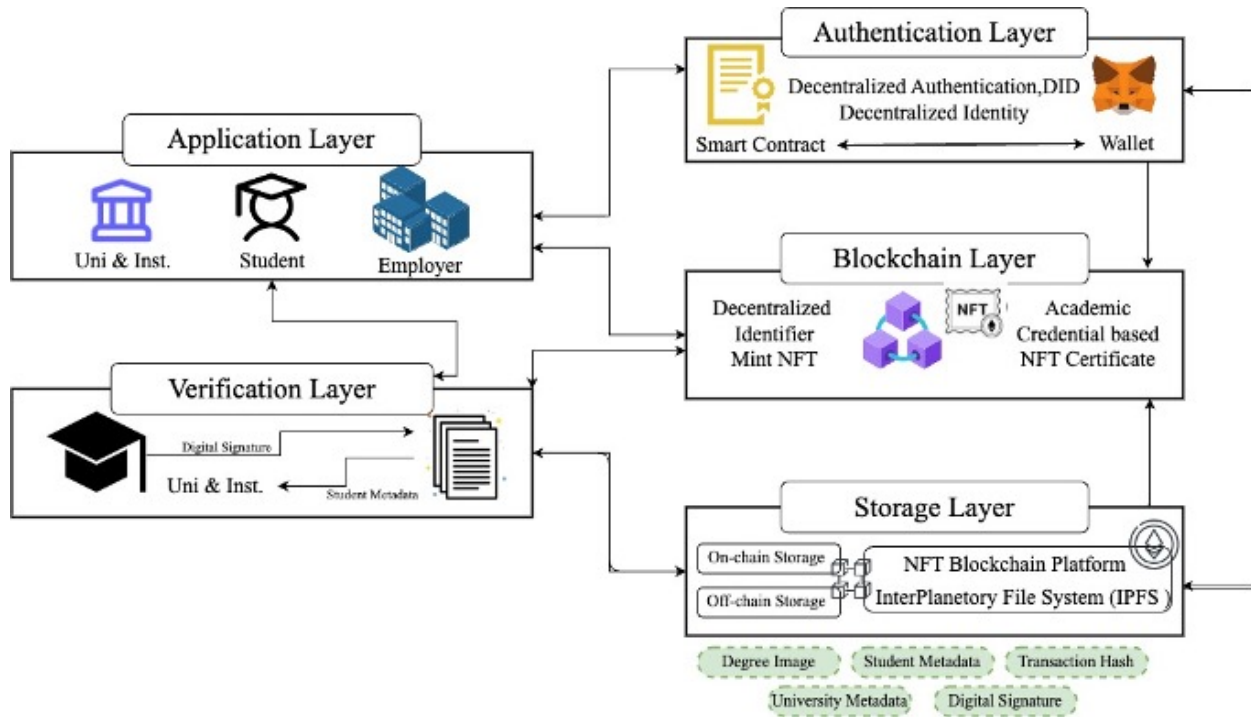


Figure 3.1: A general NFT certificate sharing system overview

verify ownership and authenticity, the function compares the hashes of the original data attached to the viewNFT with other supporting elements in the metadata.

In summary, this solution framework empowers students with full ownership of their certificates, streamlines transactions, provides extensive control and customization options, and enhances security to ensure that student data remains under their control. The decentralized authentication utilized in this framework enables students to access their profile information without relying on a centralized authority. University administrators play a pivotal role in institution registration and student profile creation, while employers can view and verify certificates issued to potential employees.

The system overview figure 3.1 depicts the architecture of the system, which consists of five key layers: the application layer, verification layer, authentication layer, blockchain layer, and storage layer. Each layer serves a distinct purpose in the system's overall operation.

3.1.1 Application Layer

The application layer represents the users of the system, which include students, university administration staff, employers and other relevant stakeholders. It encompasses the user interface, enabling users to interact with the system. The user experience design is based on the use cases and functionalities provided to the users, such as issuing and sharing certificates.

University :- In this context, the university has two main roles. Firstly, the university can establish its own profile through the administration of the university. The university administrators have the ability

to register their institution and generate certificates as NFTs for their students. These NFT certificates are then sent to the individual students' wallet addresses. The smart contract, created by the platform administrator, facilitates the transfer of ownership of the NFT certificate to the student's address provided during the creation of the certificate. Additionally, the university can also issue certificates upon request from third parties for verification purposes. They can verify and validate certificates and their associated metadata when receiving certificates from other students.

Student :- When students log in with their Metamask wallet, they can view the certificates issued to them by their respective universities. They have the option to create additional viewable NFT certificates based on the original one. Since the student owns the issued certificate, they can choose to filter the subjects and create a dedicated certificate for their specific purposes. They can also choose to create a copy of the original NFT without any changes to the appearance of the certificate.

In the designed system, the certificate data and its metadata are no longer stored in a centralized database. Instead, they are hashed and transferred to a distributed data system, with the hash being stored in the NFT certificate on the blockchain. The student has the access rights to transfer the certificate by selecting the recipient institution from a list of those that have enrolled in the system. Before transferring it, the student can set rules and conditions. Despite transferring the certificate, the ownership still remains with the student. If needed, the student can regain possession by calling the smart contract to revoke access rights to the transferred NFT. This ensures that data is not lost even after sharing it. The platform is designed to give students control over their credentials even after sharing the certificate.

Employer:- In the proposed system, employers have the ability to receive viewing rights, allowing them to access and review the student's certificate data. They can verify the certificate without requiring technical knowledge of comparing hash values, as they can simply interact with the system. Additionally, employers have access to the ledger viewer, which displays the data provenance of the certificate. This includes information such as the university that issued the certificate and the current owner of the certificate. This enables employers to easily verify the authenticity and ownership of the certificate.

3.1.2 Authentication Layer

The authentication layer incorporates decentralized authentication through the inclusion of the "Sign in with Ethereum" functionality. This feature utilizes the MetaMask wallet for user authentication, offering a secure and decentralized solution. MetaMask serves as a reliable wallet for managing Ethereum accounts and facilitating signIn transactions. By adopting this approach, the system ensures that only authorized users can access the platform and engage in activities related to certificate issuance and sharing. Decentralized authentication operates by utilizing the Ethereum account for authentication purposes with an off-chain service. In this case, the system has integrated Google Firebase authentication with a MetaMask extension to establish a standardized message format. This format includes essential parameters such as nonce, scope, session details, and security mechanisms, enabling effective authentication. This decentralized authentication

approach holds significant importance, especially in the context of NFT certificate and credential sharing systems. It grants ownership rights to students while implementing robust access control measures to ensure secure and controlled access to certificates.

By adopting a decentralized authentication model, the platform enables students to retain ownership of their certificates, assigning it to their individual wallet addresses rather than a centralized system. This ensures that the access and control over certificates remain independent of the platform, enhancing security and empowering students with full ownership and control over their credentials.

3.1.3 Verification Layer

The verification layer consists of the university admin and the transaction history stored in the blockchain through smart contracts. The blockchain maintains a record of all transactions related to issuing certificates, transferring ownership to students, creating new certificate transactions, and granting or revoking viewing rights between different institutions. Prior to certificate issuance, the certificate metadata undergoes hashing, which would result in a different hash if any data is altered. When a student creates a new viewNFT, they are only able to access filtered subjects, and the corresponding information is specified in the certificate. The student cannot modify this information, ensuring the preservation of unaltered data. When a certificate is issued, its metadata, including the certificate hash, is stored on the blockchain. During the verification process, the university compares the certificate's hash with the stored metadata to verify the certificate's integrity and authenticity. This layer guarantees the authenticity of the certificates and ensures they have not been tampered with.

Furthermore, the university retains the ability to verify the authenticity of the certificate without needing to possess ownership rights. This efficient verification process offers significant advantages to third parties such as employers or educational institutions. They can securely and conveniently validate certificates by accessing the stored metadata directly within the platform, without the need to navigate away from it. The metadata contains the university's signature and hash, both of which are linked to the original certificate. Additionally, the original certificate is connected to the newly created viewNFT, providing indisputable evidence of unalterable data provenance backed by the blockchain and distributed database.

3.1.4 Blockchain Layer

The blockchain layer involves the Ethereum blockchain, which serves as the underlying infrastructure for the system. The Ethereum blockchain stores the smart contracts that define the logic and behavior of the certificate issuance and ownership processes. methods such as creating or minting the NFT certificate, transferring ownership, creating new viewNFT and setup access rules to send or revoke are all methods in the smart contract. This smart contract is deployed by the admin of the platform. It also maintains the details of NFT ownership, ensuring transparency and immutability. The blockchain layer provides a secure and decentralized environment for managing certificates and their ownership.

By leveraging the Ethereum blockchain, the system achieves a distributed consensus mechanism, ensuring that the certificates and their associated NFTs are tamper-proof and resistant to unauthorized modifications. Before creating NFT the metadata related to the certificate data are stored in a distributed database cryptographically hashed to form a unique content identifier (CID) and assigned with the NFTs. In order to deploy the smart contract and utilize the functionalities of the deployed blockchain, the system necessitates users to utilize the native token of the Ethereum blockchain, known as ETH. This requires users to have the same wallet for both logging in and accessing the system, providing a convenient experience. By utilizing ETH, users can seamlessly interact with the smart contract and leverage the various features offered by the blockchain network. The design of the smart contract is especially convenient for students, as the low transaction cost of less than 30 cents per transaction makes it affordable for them to engage with the system. This affordability factor ensures that students can easily participate in various activities and utilize the functionalities of the smart contract without worrying about high transaction expenses. The cost-efficient design of the smart contract prioritizes accessibility and convenience for students, enabling them to seamlessly interact with the system and benefit from its features.

3.1.5 Storage Layer

The storage layer is responsible for preserving the data associated with certificates. There are two types of data storage: on-chain and off-chain. On-chain data refers to information stored directly within the blockchain itself, which can be costly if there is a large volume of data. On the other hand, off-chain data is stored in centralized or distributed databases. In my system, I implemented a hybrid approach that combines both methods.

Initially, the certificate content is stored in Firebase, a cloud-based storage solution provided by Google known for its scalability and flexibility. However, to ensure improved security and durability, the content is subsequently transferred to IPFS (InterPlanetary File System) before the certificate is minted as an NFT. In this approach, the IPFS serves as a distributed and decentralized file system that enables the storage and retrieval of files based on their content's hash. The hash of the certificate is stored on-chain and linked to the smart contract responsible for minting the NFT, while all other data are stored in IPFS. By utilizing IPFS, the system guarantees the secure storage of certificate contents and enables reliable and efficient access to them. When a new version of a file is uploaded to IPFS, it undergoes a cryptographic hashing process that generates a unique identifier called a CID (Content Identifier). This ensures that any modifications made to a file will result in a different CID. The use of IPFS offers several advantages. Firstly, it spreads the certificate data across multiple nodes, minimizing the risk of data loss or unavailability. Secondly, IPFS employs content addressing, referencing certificates by their unique hash to guarantee integrity. Lastly, it allows for efficient file retrieval by enabling fetching from any node within the network, improving system performance.

A notable benefit of this approach is that modifications to a file do not overwrite the original version. Instead, each modified version receives its own distinct CID, preserving the integrity and historical record

of the file. Additionally, IPFS utilizes an intelligent mechanism that efficiently reuses common data chunks shared among multiple files, reducing overall storage costs. This optimization optimizes storage resources and enhances the efficiency of the IPFS network.

3.2 System Architecture

This section presented the detailed system architecture of the NFT based certificate sharing system. This section has the content from my framework paper published at the 2023 Blockchain congress conference [23](in print).

The proposed solution framework, depicted in figure 3.1 , introduces a decentralized approach to certificate issuance and ownership, prioritizing students' maximum ownership of their certificates employing *Firebase*, *IPFS* and *ReactJS* as the main building technology, that allows user to interact with the system using wallet *Metamask* and currency *ether* with all the transactions stored in the blockchain eliminating the trust issues. The system uses *Firebase* as the backend for authentication seamlessly with *MetaMask* using the *Moralis SDK's*¹ authentication API. This integration enables users to authenticate themselves using their *MetaMask* wallets, taking advantage of the secure and convenient decentralized authentication. Furthermore, I have leveraged *Firebase's* database for centralized storage, ensuring efficient and reliable management of data. *Firebase* primarily offers a NoSQL database. As shown in the figure, the component is both a flexible and scalable database, storing information as collections related to the user's role.

It allows user data to be pushed and retrieved from the cloud through an Internet connection. Additionally, *Firebase* keeps user data in sync and supports offline capability. The screenshot of the database is shown in figure 3.2. *Firebase* enhances data security through multiple measures. Firstly, it encrypts data during transit using the secure Hypertext Transfer Protocol (HTTPS), ensuring that information remains protected while being transferred over networks. Additionally, *Firebase* applies encryption to the data at rest, meaning that even when stored, the data remains encrypted and safeguarded. Furthermore, the chosen database service for this project holds certifications in accordance with prominent privacy and security standards, including ISO 27001, 27017, 27018, and SOC 1, 2, and 3. These certifications attest to the database's compliance with internationally recognized regulations, further solidifying the system's robust security framework

The framework, as illustrated in the figure 3.3, primarily focuses on creating and sharing certificates as NFTs, emphasizing certificate ownership. To support the creation and management of NFTs, the system has integrated *Hardhat*, a popular development environment for Ethereum smart contracts. Additionally, it utilizes an *IPFS* database. When a NFT certificate is generated, the system operates as a decentralized application (dApp), running on a decentralized network. Similarly storing the metadata associated with NFTs in a distributed database is crucial for decentralized applications (dApps). Distributed databases offer several advantages, including data availability, resilience, and transparency. With data distributed across

¹<https://docs.moralis.io/web3-data-api/evm/moralis-sdk>

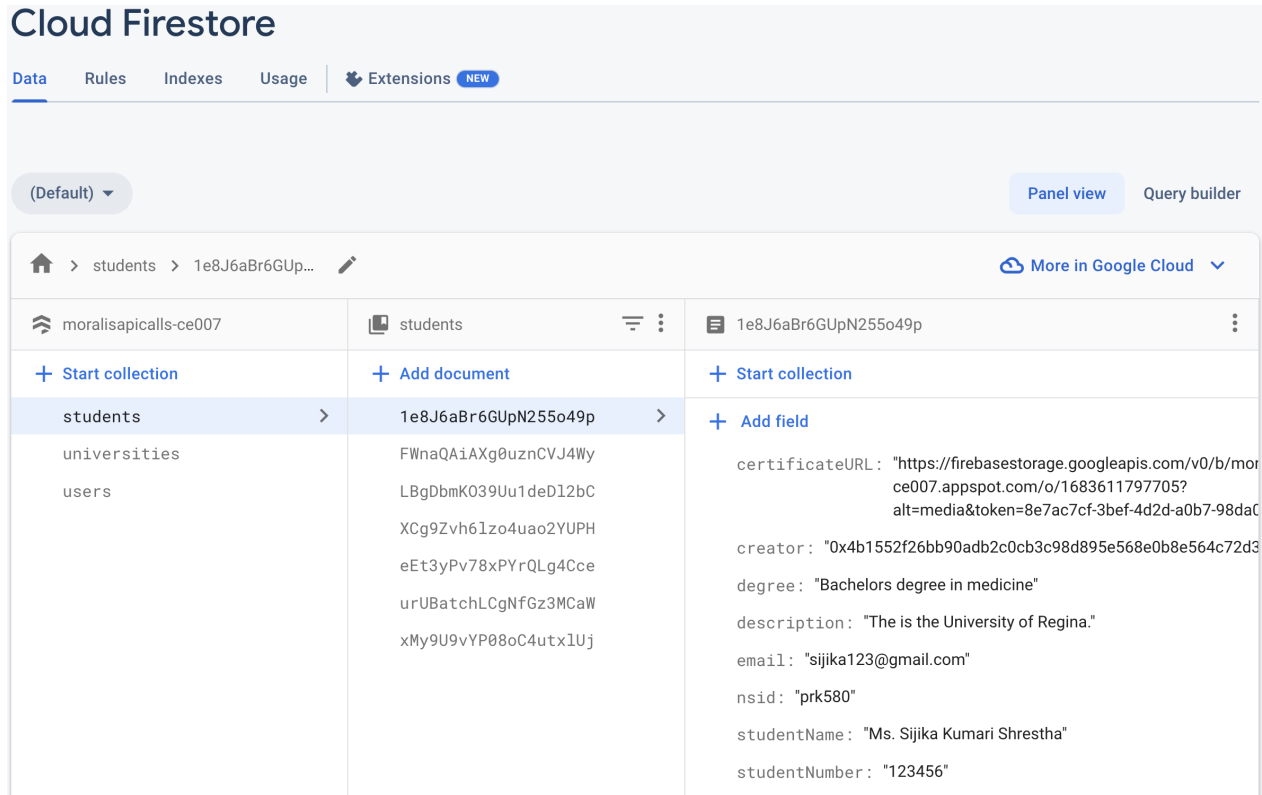


Figure 3.2: Sample Data on Google Firestore Database

multiple nodes or servers, the system ensures uninterrupted access to metadata even if some nodes fail or are compromised. This distribution also enhances resilience to failures and attacks. Transparency is facilitated as each participant in the distributed system has a copy of the database, aligning with the principles of trust and transparency in dApps. Additionally, distributed databases, such as IPFS or decentralized storage systems, provide decentralized and immutable storage solutions, mitigating the risk of data manipulation or censorship. By leveraging distributed databases, dApps can ensure data integrity, security, and reliability, while adhering to the decentralized principles they are built upon. To connect the front-end with the Ethereum blockchain, I utilized Hardhat, a development toolset. Hardhat provides integration with Ethers.js through the package '@nomiclabs/hardhat-ethers'. This package allows seamless usage of Ethers.js within the Hardhat project, enabling interaction with smart contracts and the Ethereum network. Additionally, I used the package '@nomiclabs/hardhat-waffle', which integrates Hardhat with the Waffle testing framework. This package provides a set of utilities and APIs for writing thorough and expressive tests for Ethereum smart contracts.

For the front-end development, I utilized ReactJS as the primary technology. To set up the project, I used Node.js, a runtime environment based on the V8 JavaScript engine. The project skeleton of the ReactJS application was created using the 'create-react-app' command in the command line. By running 'npm start', the project was loaded in the browser. In the setup process, Node.js installed 'create-react-app' to establish a development environment with Java features and tools for project initialization and production optimization.

Babel, operating under the hood, converted ES6 JavaScript code into ES5 to ensure compatibility with most browsers that do not fully support ES6 yet. Webpack, an asset bundler, collected all the project's assets (codes and files) and created a bundle that could be efficiently delivered from the server to the client's browser. To create a new ReactJS application, the command line instruction 'npm create-react-app appName' was utilized.

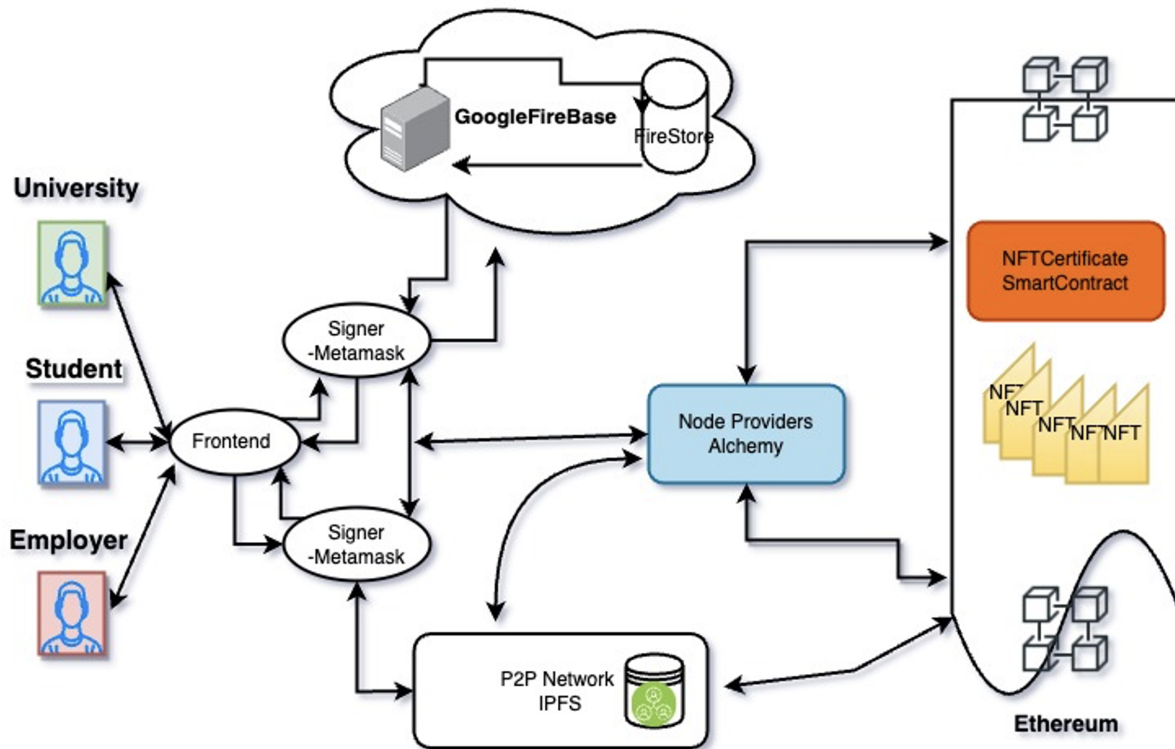


Figure 3.3: System Architecture

To establish connection of ipfs to the frontend I used Axios library, a popular promise-based HTTP client that facilitates making asynchronous HTTP requests in both browsers and Node.js environments. I can interact with REST endpoints and perform CRUD (Create, Read, Update, Delete) operations. Axios automatically parses JSON response data, simplifying the process of working with JSON-based APIs. It also provides the ability to send JSON data in request payloads with ease. To connect with the IPFS API, I used Axios to send requests to the desired endpoints. IPFS provides an API that enables interaction with the decentralized file system and its functionalities. With Axios, I can send requests to upload files, retrieve files, manage directories, and perform other operations supported by the IPFS API. In my implementation, I utilized a service called Pinata², a popular IPFS infrastructure. Pinning is a key feature provided by Pinata, allowing users to ensure the availability of their files on the IPFS network. By pinning files, users can prevent them from being removed or garbage collected from IPFS, even if they are not frequently accessed. This is

²<https://www.pinata.cloud/>

beneficial in preserving important files and preventing them from being lost due to lack of popularity or usage. Additionally, Pinata enables efficient metadata management for files stored on IPFS. Users can store custom metadata, perform searches and filters based on metadata, and retrieve metadata alongside the files. Pinata also simplifies the integration process with well-documented APIs, making it easy to incorporate features like file uploading, management, and retrieval from IPFS into applications using tools like Axios.

For the purpose of communicating with the Ethereum network, the system architecture includes an Ethereum query gateway, which acts as an interface to exchange data with the blockchain. In the context of my architecture, I have used a popular Ethereum API, Alchemy, which is explained in details in the section 3.2.2. How users interact with the front-end is explained in details in section 3.3.1.

3.2.1 SignIn with Ethereum

Sign-In with Ethereum is a proposed Ethereum Improvement Proposal (EIP-4361) that introduces a standardized method for off-chain authentication using Ethereum accounts. This section aims to explore the motivation behind Sign-In with Ethereum, its specifications, and its potential benefits in terms of self-custodial identity management, interoperability, and user experience enhancement.[8]. Traditional authentication systems often rely on centralized identity providers (IdPs), which possess ultimate control over users' identifiers. In contrast, Sign-In with Ethereum offers a self-custodial alternative, empowering users to assume greater control and responsibility over their digital identities. By leveraging Ethereum accounts and message signing, this authentication method seeks to align incentives between users and service providers, promoting privacy, security, and user autonomy. Sign-In with Ethereum follows a structured workflow wherein the user's Ethereum wallet presents a plaintext message to be signed, incorporating essential parameters such as the Ethereum address, requesting domain, message version, chain identifier, scoping URI, nonce, and issued-at timestamp as shown in figure 3.4 The resulting signature is then verified by the service or application, which can also fetch additional data associated with the Ethereum address from sources like the Ethereum blockchain or other permissioned databases.

```
service.invalid wants you to sign in with your Ethereum account:
0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2

I accept the ServiceOrg Terms of Service: https://service.invalid/tos

URI: https://service.invalid/login
Version: 1
Chain ID: 1
Nonce: 32891756
Issued At: 2021-09-30T16:25:24Z
Resources:
- ipfs://bafybeiemxf5abjwjbikoz4mc3a3dla6ual3jsgpdr4cjr3oz3evfyavhwq/
- https://example.com/my-web2-claim.json
```

Figure 3.4: Example Message of SignIn with Ethereum

Several technical decisions and considerations are outlined in the Sign-In with Ethereum proposal ³. These include the prevention of replay attacks through the use of randomized nonces, the verification of domain binding, channel security, session invalidation mechanisms, and the establishment of maximum lengths for ABNF terms. Backwards and forwards compatibility are also discussed to ensure smooth integration and evolution of the authentication method. The utilization of the Ethereum blockchain in the Sign-In with Ethereum process offers additional benefits. Users can authenticate their data associated with their Ethereum addresses, such as ERC-721⁴ assets with data sharing platforms. This becomes particularly significant in the context of academic certificates, where the issuance, verification, and sharing of credentials can be revolutionized.

A Student user is able to establish direct link between their accounts and their certificates. Students gain complete control over their academic achievements and can easily share them with employers, academic institutions, or any other relevant parties. By utilizing self-custodial authentication methods, students maintain ownership of their Ethereum accounts and the associated NFT certificates. They no longer need to rely on third-party identity providers or centralized systems to verify their credentials. This decentralized approach empowers students to manage their digital identities autonomously, ensuring data privacy and reducing the risk of unauthorized access or misuse.

The Sign-In with Ethereum process commences with the user's wallet presenting a structured plain text message or an interface designed for signing. As shown in the figure 3.4, the message follows the ERC-191 standard ⁵ signed data format and is prefixed with "`\x19Ethereum Signed Message:\n<length of message>`" to adhere to ERC-191 standards. Within this message, crucial components are included, such as the user's Ethereum address, the requesting domain, message version, chain identifier (chain-id), URI for scoping, nonce for preventing replay attacks, and issued-at timestamp. The user's wallet is then used to sign the message, generating a unique signature. This signature is shared with the relying party, which is the service seeking authentication. The relying party verifies the validity of the signature and examines the content of the signed message to ensure its integrity, protecting against tampering or unauthorized alterations.

3.2.2 Ethereum Query Gateway

The Ethereum gateway in the proposed architecture serves two main purposes: handling queries and transactions. Queries are used to retrieve data from the Ethereum blockchain without incurring any charges or confirmation requirements. For instance, a query can be made to retrieve the hash value associated with an NFT in order to identify its owner. This retrieved information can then be displayed on the frontend of the application. On the other hand, transactions involve writing data to the blockchain and require fees and network confirmation. These transactions perform actions such as creating a new NFT or calling a method

³<https://eips.ethereum.org/EIPS/eip-4361>

⁴<https://eips.ethereum.org/EIPS/eip-721>

⁵<https://eips.ethereum.org/EIPS/eip-191>

to transfer the viewing rights of an existing NFT to another user.

Functioning as a client in the Ethereum network, the gateway enables applications to communicate with the blockchain. It serves as an interface that facilitates the submission of transactions for data modification and enables the querying of stored blockchain data. To address concerns related to trust and centralization, the gateway utilizes multiple Ethereum API providers. This approach distributes trust among the providers and introduces redundancy, minimizing reliance on a single point of failure. By adopting this decentralized approach, potential risks are mitigated, and the gateway's reliability is enhanced. For my specific project, I have opted to utilize the Alchemy gateway as the Ethereum API provider. Alchemy offers infrastructure as a service, streamlining the process of interacting with the Ethereum network through their API. With their reliable and scalable infrastructure, my application can efficiently communicate with the Ethereum blockchain. Alchemy manages the complexities associated with Ethereum network interaction, encompassing transaction signing, fee estimation, and network communication.

3.2.3 Ethereum Wallet

An Ethereum wallet is a software application designed for storing and managing Ethereum accounts and tokens. It enables users to securely sign transactions using their private keys and interact with the Ethereum network and decentralized applications (DApps). Integrating an existing wallet into the system architecture offers the benefit of familiarity for Ethereum users. Various wallet options are available to cater to different needs, including desktop or mobile usage, browser add-ons, hardware wallets, multi-token support, and robust security features.

Ethereum wallets typically provide APIs that connect to the blockchain, allowing interaction with it, similar to the Ethereum query gateway discussed earlier. Popular software libraries like Web3.js facilitate the development of software for Ethereum interaction and can be used with different wallet providers. However, trust is a crucial aspect when using wallets since a malicious wallet could potentially access a user's private key and take control of their account. Wallet providers address this concern in various ways, such as open-sourcing their code or involving the community in the wallet's development, which reinforces trust through peer review. To address trust risks, my proposed architecture prioritizes security and privacy by encrypting and locally storing users' private keys within their browser's extension. It also offers users the option to set up a password or use hardware wallets for enhanced security. In my architecture, I have chosen Metamask as the primary wallet for my web-based application. Metamask is a popular Ethereum wallet browser extension that serves as a bridge between the web browser and the Ethereum blockchain. When a user accesses a web application requiring Ethereum interaction, such as sending a transaction or signing a message, the application can seek permission from Metamask to access the user's Ethereum account. Metamask then prompts the user to review and authorize the requested action. Upon approval, Metamask securely signs the transaction using the user's private key, ensuring that the private key remains protected and never leaves the wallet. Furthermore, Metamask provides APIs that enable developers to make RPC (Remote Procedure

Call)⁶ calls to interact with the Ethereum blockchain. RPC calls allow applications to query the Ethereum network and send commands. These calls provide access to information such as account balances, transaction history, smart contract data, and more.

3.3 System Development

The System Development section focuses on the process and implementation of the architecture discussed in the previous section. It outlines the steps involved in bringing the proposed system to life and provides a detailed discussion on the relevant aspects of its implementation. The section begins by presenting the chosen stack of technologies used in building the system. It highlights the various components and tools employed, such as programming languages, frameworks, databases, and other necessary infrastructure. The rationale behind the selection of each technology is explained, considering factors such as compatibility, scalability, security, and ease of development.

A significant part of the section is dedicated to the deployment and execution of smart contracts. It elucidates the process of writing smart contracts that govern the system's logic and behavior. The smart contract development framework used is described and the essential considerations when designing and deploying smart contracts on the Ethereum network are discussed. Moreover, the section addresses the execution of smart contracts and how they interact with the other components of the system. It explores various scenarios and use cases, providing insights into the functionalities and capabilities of the deployed smart contracts. Throughout the section, relevant discussions on challenges encountered during the development process, design decisions made, and optimizations implemented are included. The emphasis is placed on ensuring the robustness, efficiency, and security of the system.

a. Visual Studio(VS) Code

Visual Studio Code (often referred to as VS Code) is a highly popular code editor developed by Microsoft. It has gained immense popularity among developers and software engineers, primarily due to its versatility, extensibility, and user-friendly interface. VS Code is renowned for its broad support for numerous programming languages, making it a versatile choice for developers. It offers comprehensive syntax highlighting, code completion, and debugging capabilities for languages like JavaScript, Python, Java, C, Ruby, Solidity and many others. Additionally, it provides developers with an integrated terminal, allowing them to execute commands and run code seamlessly within the editor. One of the standout features of VS Code figure3.5 is its seamless integration with Git, a widely used version control system. This built-in Git integration simplifies the process of tracking changes to codebases. Developers can conveniently manage repositories, commit changes, switch between branches, and perform various other Git-related tasks without having to

⁶https://en.wikipedia.org/wiki/Remote_procedure_call

leave the editor. This powerful integration streamlines the development workflow, enhancing productivity and collaboration.

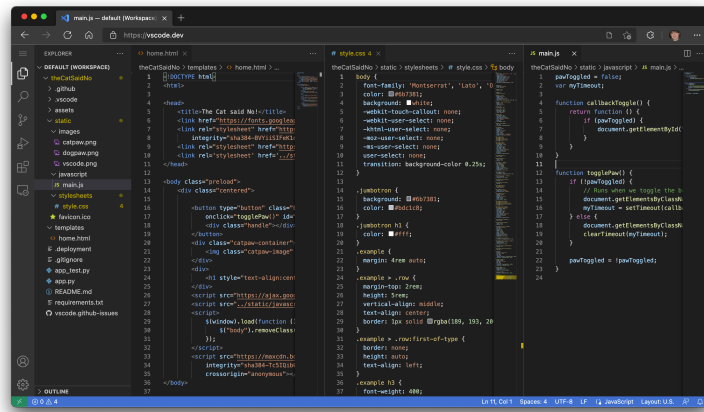


Figure 3.5: A Screenshot showing VS Code Setup

b. GitHub

GitHub is an online service that offers hosting for software development version control. It serves as a platform for developers and teams to collaborate on projects, track code changes, and manage their source code repositories. Developers can create repositories on GitHub to store their code and related files. Each repository represents a project and contains all the files, folders, and version history associated with that project. GitHub provides a web-based interface as well as a command-line interface (CLI) to interact with repositories. One of the key features of GitHub is its support for distributed version control systems, primarily Git. Git allows developers to track changes to their codebase, create branches for different features or experiments, and merge changes back into the main codebase. GitHub provides a seamless integration with Git, making it easy to manage and collaborate on code changes.

c. Google Firebase Services

For the NFT-based certificate sharing system, Google Firebase offers a comprehensive suite of cloud-based services that enhance functionality and user experience. Firebase Authentication, integrated with the Moralis SDK, ensures secure authentication and wallet connectivity. Cloud Firestore Database provides a scalable NoSQL document database to store and retrieve real-time certificate data, including details, metadata, and ownership information. Firebase Cloud Storage enables secure storage and retrieval of user-uploaded NFT certificate files. Leveraging these Firebase services allows developers to prioritize user experience while offloading backend infrastructure, server-side logic, and data storage to Firebase's reliable and scalable cloud-based tools. This results in the development of a secure and scalable NFT certificate sharing system tailored to user needs.

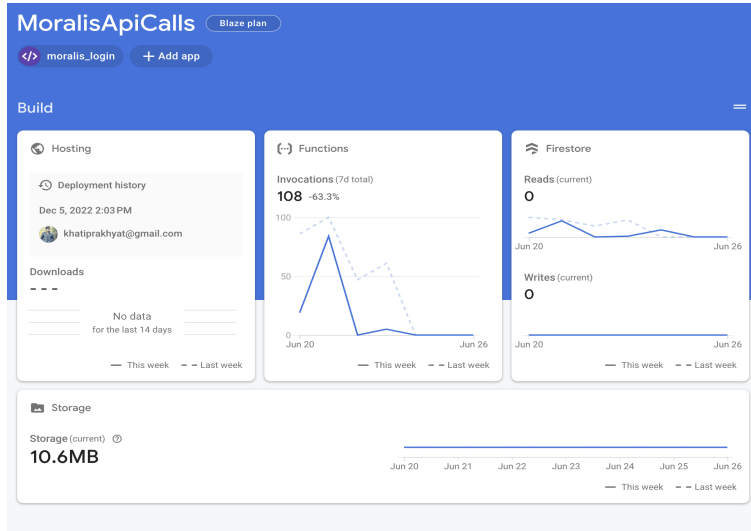


Figure 3.6: Google Firebase Console Interface

3.3.1 User Interface

The user interface of framework, which is a web-based application, caters to three distinct access roles, ensuring different functionalities for each user category. To achieve system independence and establish a unique identifier, the system integrates a universal wallet and utilizes the wallet address as a global identifier. When signing in to the system, users are directed to a single login button, simplifying the authentication process. Upon successful login, the web app dynamically adjusts the navigation buttons based on the user's assigned role, as identified by their Metamask address. By default the role is assigned as general user as student.

For students, the interface provides convenient access to tabs such as Profile, NFT Certificate, and Transferred NFT, allowing them to manage their profile information, view their NFT certificates, and monitor any NFT transfers. Universities, on the other hand, have access to additional tabs including Profile, Collection, NFT Certificate, and Transferred NFT, empowering them to manage their profile, curate NFT collections, and track NFT certificates and transfers. Similarly, Employers can leverage the platform by accessing tabs specifically designed for them, such as Profile and Employer NFT. By tailoring the user interface and functionality based on the respective roles, the system delivers a personalized experience, catering to the unique requirements and permissions of each user category.

Dashboard: The landing page of the system is displayed in figure 3.7. Upon clicking the "Connect Wallet" button, the wallet sign-in process is initiated. This process utilizes the Metamask wallet, as shown in the sign-in message provided to the user in figure 3.8. The message generated by Metamask informs the user about their logged-in status and the blockchain they are connected to. To authenticate the user, Firebase and Moralis SDK are integrated, leveraging Firebase for authentication purposes. Referencing figure 3.8, I can observe the context of the sign-in message in MetaMask.

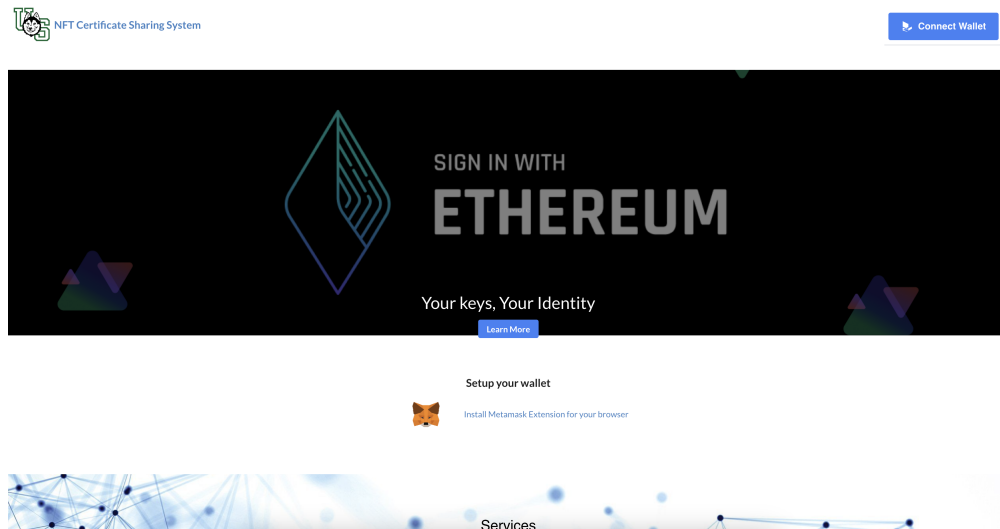


Figure 3.7: NFT certificate sharing dashboard

In the authentication process, there are several parameters involved. The "statement" parameter, which is optional, represents a user's human-readable assertion in ASCII format that will be signed. It's important to note that the statement should not contain newline characters (0x0a). The "URI" parameter is an RFC 3986-compliant URI that points to the specific resource being signed. In my case, I was locally hosting the page using react to https://localhost/. The "version" parameter is required and denotes the current version of the message, which should be set as 1 according to the specification. The "chain-id" parameter refers to the EIP-155 Chain ID, binding the session to a specific network where Contract Accounts must be resolved. Here I am using Sepolia test network having chainId 11155111.

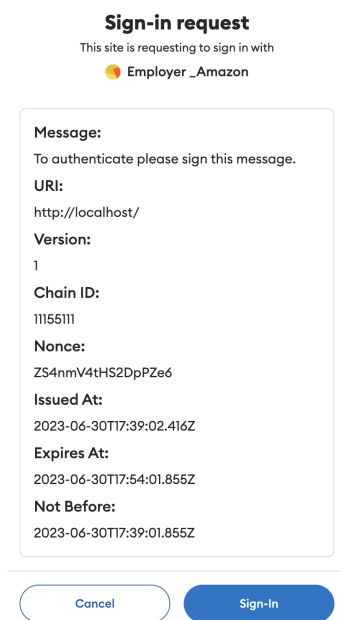


Figure 3.8: NFTcertificate SigIn Using Metamask

Additional parameters include the "Nonce," a randomly generated token chosen by the relying party to prevent replay attacks. The nonce should be at least 8 alphanumeric characters in length. The "Issued-at" parameter represents the current time in ISO 8601 datetime string format. Optionally, the "Expiration-time" parameter can be provided as an ISO 8601 datetime string indicating the point at which the signed authentication message is no longer considered valid. Similarly, the "not-before" parameter, also optional, is an ISO 8601 datetime string indicating the time when the signed authentication message will become valid.

Profile: The landing page of the application will default to the profile tab when a user logs in. Upon logging in, users can view general details related to their profile. For instance, if a university admin logs in, they will see the profile of the university, as shown in figure 3.9. The same applies to employers, with the only difference being that students, particularly those who have received NFTs from their respective institutes, will see their own profile. figure 3.10 illustrates an example where a student can observe that they have received a certificate from the University of Regina, specifically a Bachelor's degree certificate.

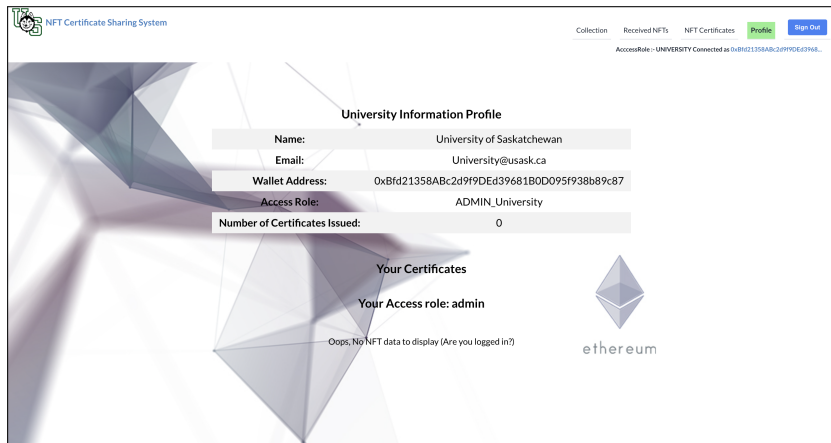


Figure 3.9: Student Original NFT certificate Dashboard

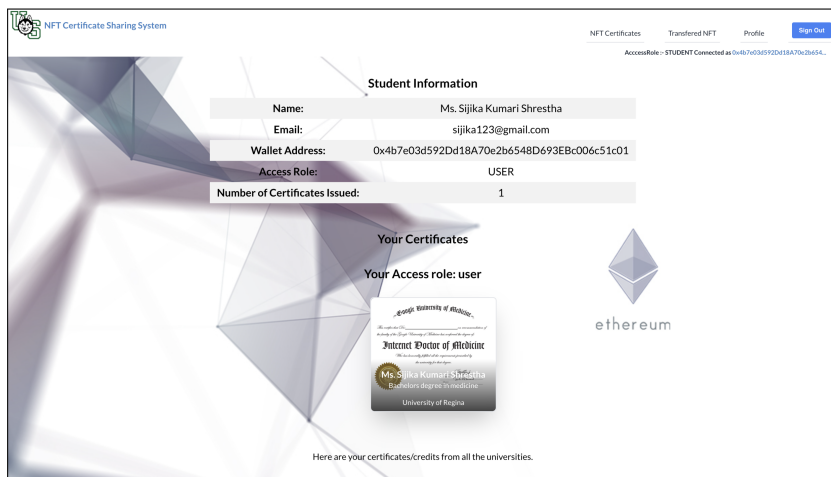


Figure 3.10: Student Dashboard After Certificate Issued

Similarly, all certificates issued to the student will be present in the profile section of the application, along with a count of the total number of certificates issued. Students have the capability to create and share their own viewNFTs, which enable them to tailor a personalized version of their certificates by including only selected subjects and grades from the original certificate while preserving all the attributes of the original NFT. Moreover, these viewNFTs incorporate a link to the university-issued original NFT, as illustrated in figure 3.11. During the creation of a viewNFT, students have the choice to filter out subjects they consider irrelevant for their sharing needs and mint their customized NFT certificate. It's essential to note that students can exclusively filter subjects and relevant grades when generating a viewNFT. The sole distinction between the original NFT generated by the university and the currently produced viewNFT is the number of subjects displayed in the transcript. Students cannot modify other credentials such as personal information, the institute's certificate name, hash value, etc. The resulting NFT will be explicitly labeled as a "viewNFT" certificate, clearly indicating that it is not a complete certificate. Essentially, a viewNFT functions as a verified yet incomplete copy of the certificate, facilitating easy accessibility and sharing. Figure 3.12 provides an example in which a student filters specific subjects and clicks the "Create NewNFT" button, initiating a blockchain transaction using Metamask. Typically, this transaction involves the minting or creation of a new NFT based on the student's specified filtering criteria.

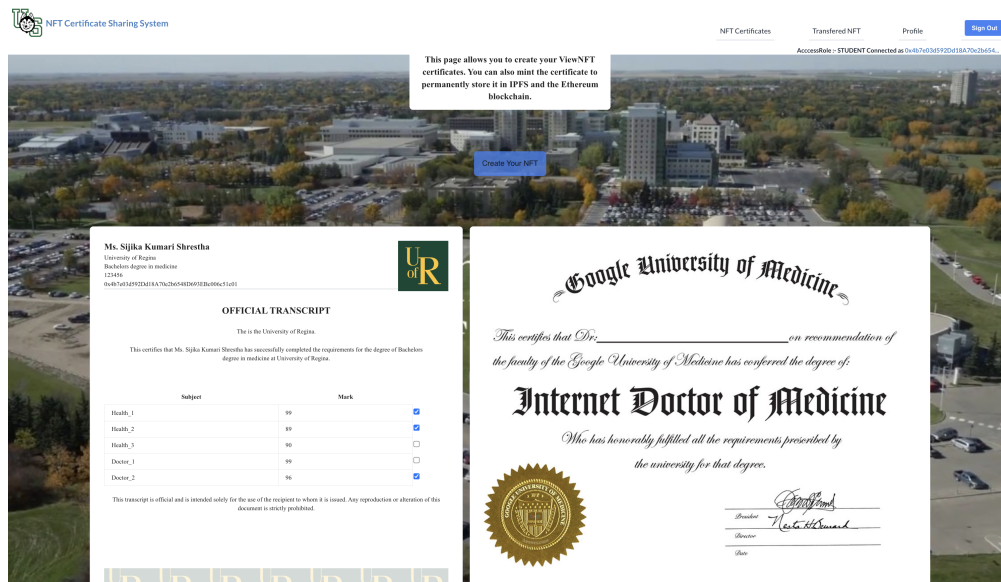


Figure 3.11: Student ViewNFT Minting Dashboard

Here after minting the data is store in IPFS linked to the address and transactions are securely recorded on the blockchain as shown in figure 3.13, the process of minting an NFT (Non-Fungible Token) involves creating a distinct digital asset on a blockchain network. Here is a basic overview of the steps required for minting an NFT. Once the smart contract is deployed, the student can initiate the minting process by invoking a designated function within the smart contract. This function typically requires supplying essential information and metadata for the NFT, including its name, description of the certificate, metadata related

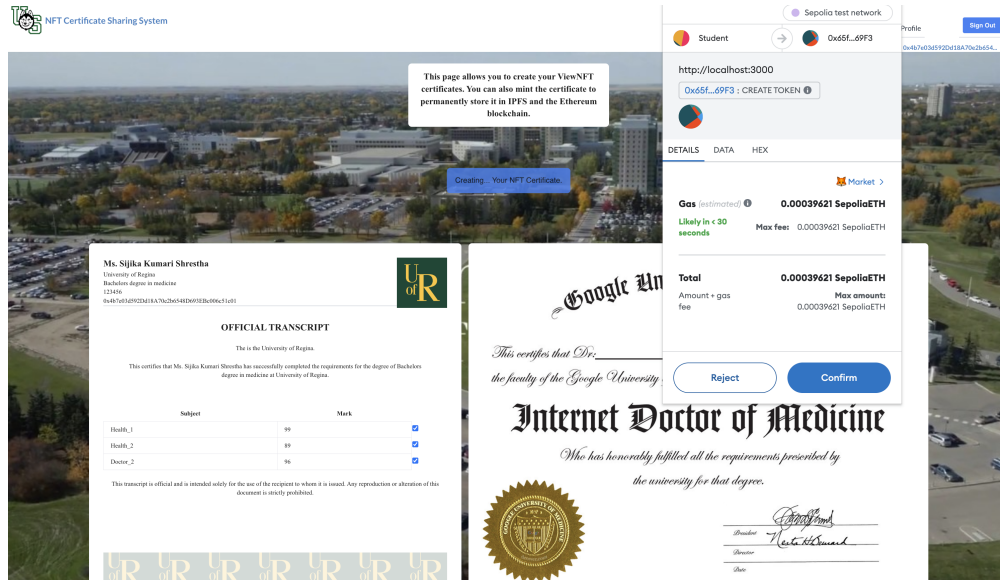


Figure 3.12: Student Triggering Minting Transaction

to the subject and link to the original NFT that was used to create this new viewNFT.

NFT Certificate: After the student creates a viewNFT, the website will direct them to the NFT Certificate tab, where the student can view their recently created viewNFTs along with general information of their profile. The dashboard of the student, depicted in figure 3.13, displays the options available after minting some viewNFTs. The student can choose to send the NFT by opening the certificate and selecting the registered institute or employer in the network.

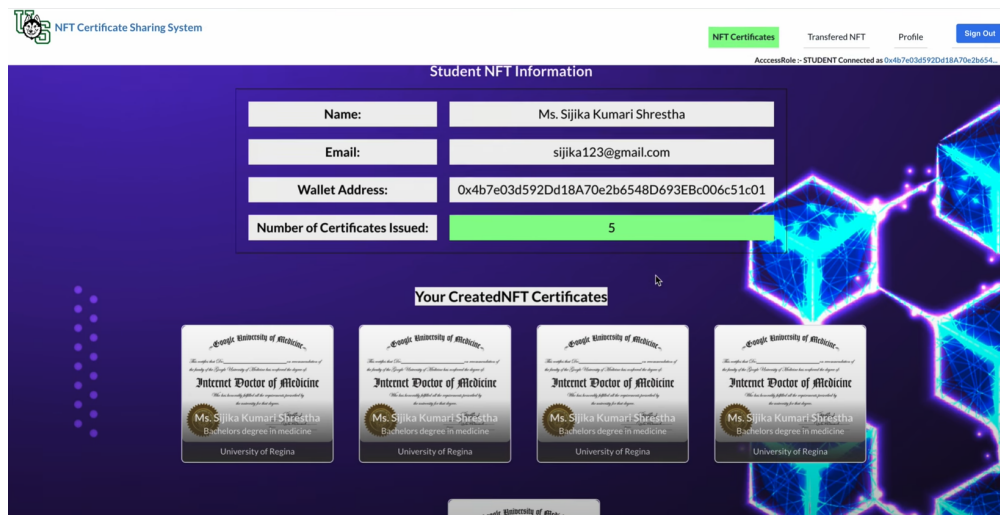


Figure 3.13: Student ViewNFT Dashboard For All Certificate

Additionally, the student can specify their preferred time frame for the receipt to access the certificate as shown in figure 3.14, after which the smart contract will revoke the access rights. Alternatively, the student can retrieve the certificate by navigating to the TransferNFT tab.

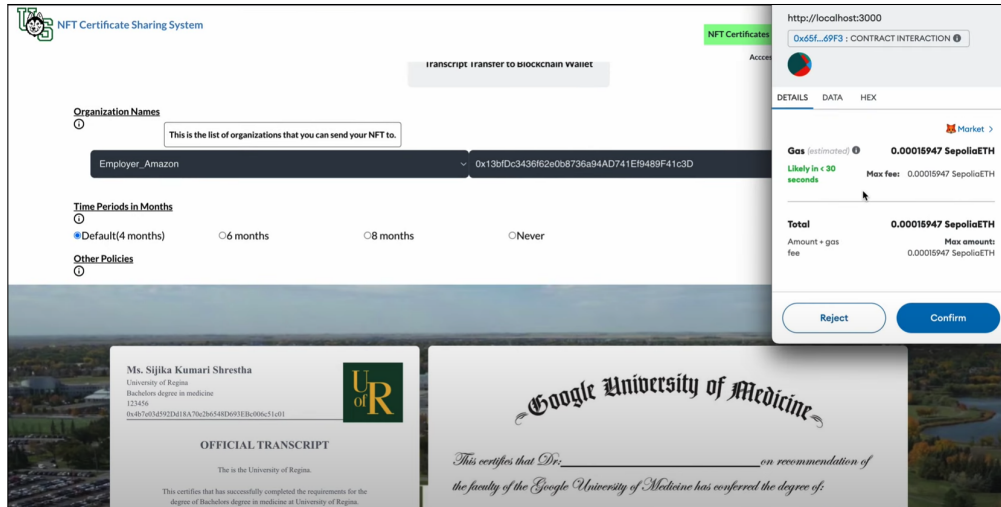


Figure 3.14: Student Transferring Viewing Rights to ViewNFTs

Transferred NFT: The TransferNFT tab as shown in figure 3.15 contains the viewNFTs that have been transferred by the user. Even after transferring the viewing rights, the student, as the owner of the viewNFT, retains access to their data. This tab displays all the transferred NFTs, including information about the institute or employer to which they were transferred. As mentioned earlier, the student can easily revoke the viewing rights for a specific user by clicking a button. This action initiates a blockchain transaction, which can only be executed by the NFT owner, as it involves changing the viewing rights.

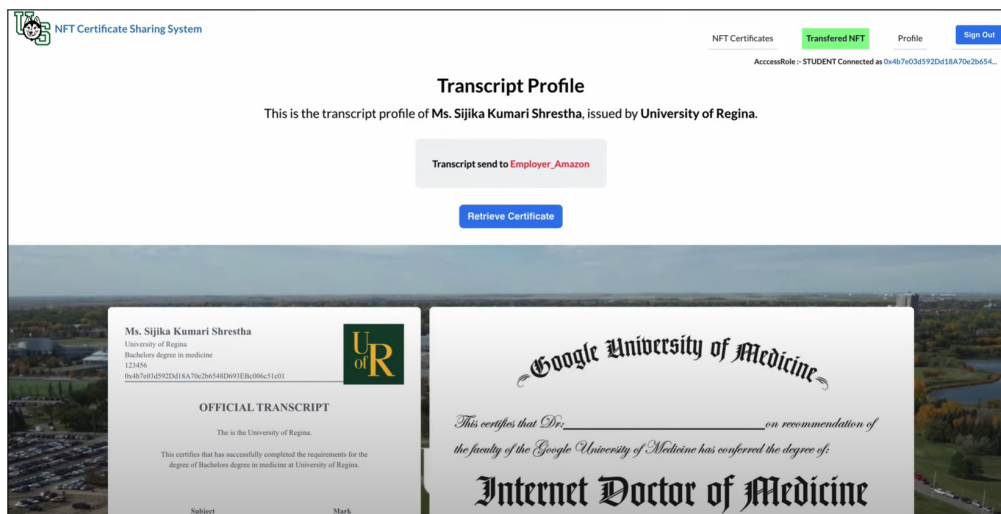


Figure 3.15: Student Retrieving ViewNFT

Collection: The Collection tab serves as an exclusive feature available solely to administrators who serve as the original issuers of the NFTs, specifically registered certificate issuers such as universities. In the event that an Ethereum address corresponds to a registered employer, the university’s dashboard will be displayed. As part of the initial setup, the university is required to register itself and establish its dedicated

university profile. Upon successfully completing the registration process, the university gains access to a range of powerful functionalities within its profile. Figure 3.16 provides an example representation of the University of Regina’s dashboard subsequent to its registration and profile activation. This dashboard acts as a centralized hub for the university’s management of student profiles, transcript issuance, and attachment of verified degree completion certificates or PDFs. To enhance administrative efficiency, the Collection tab includes a user-friendly feature demonstrated in figure 3.17, allowing seamless creation of profiles for students. Importantly, the "Create Student Profile" button enables the university to efficiently generate additional student profiles as needed. Furthermore, as part of the certificate issuance process, the university ensures that the same certificate is transferred to the student’s wallet address as an NFT. This ensures that students have direct ownership and control over their certificates, securely stored within their personal digital wallets. This transfer of certificates as NFTs guarantees the authenticity and integrity of the documents, as they are immutably recorded on the blockchain.

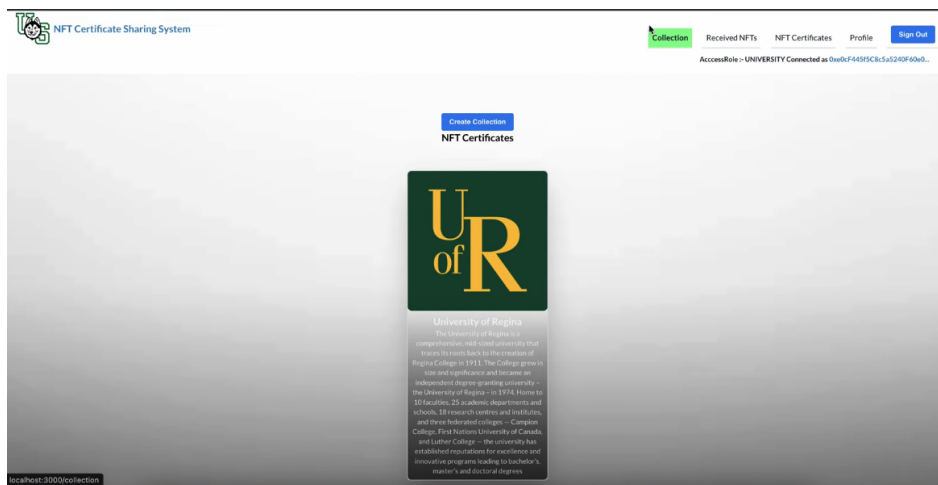


Figure 3.16: University Collection

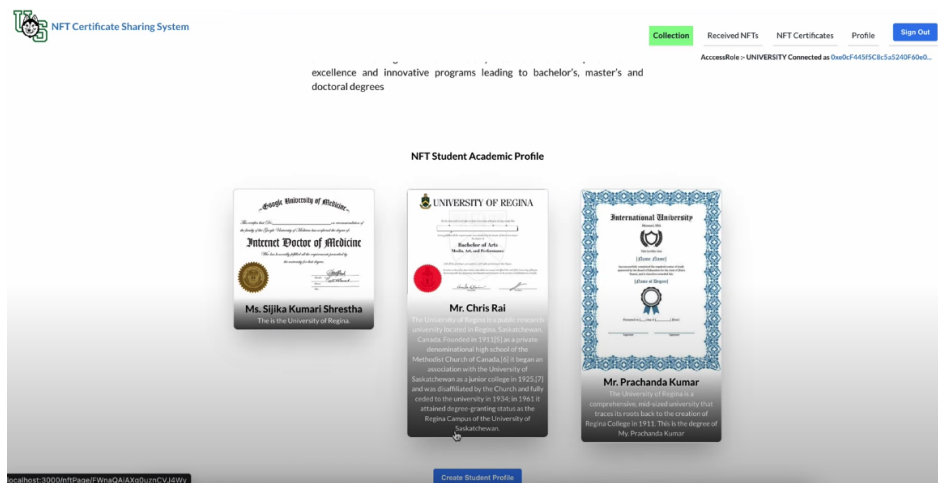


Figure 3.17: University Student profile

Validation and Verification: When a user logs in as an admin of the university or an employer, they are granted access to received NFTs from students or other universities. Within the system, these users have the ability to effortlessly open certificates, which are in the form of viewNFTs. By simply clicking a button, they can validate the authenticity of the certificate. The intricate process of checking the hash value and the signature is handled in the backend, ensuring a seamless and straightforward experience for the institute or employers. This user-friendly approach streamlines the verification process, allowing administrators to efficiently verify the legitimacy of the certificates.

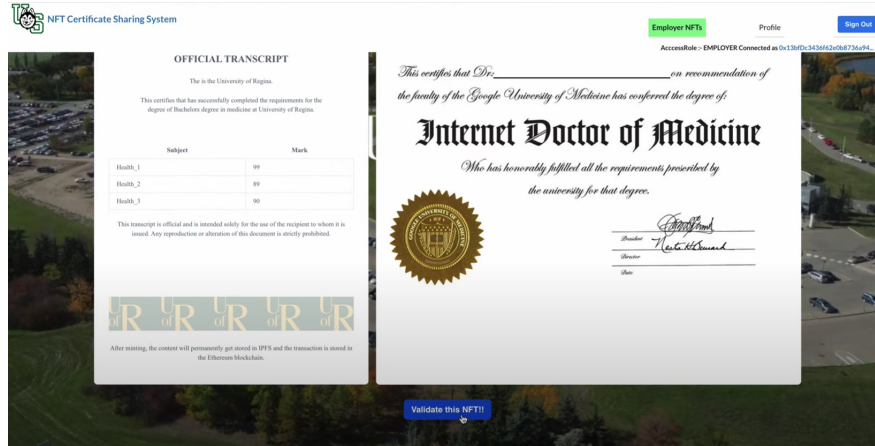


Figure 3.18: University Student NFTs description

3.3.2 NFT Smart Contracts Deployment

As discussed in section 3.2.2 a direct connection to the testnet⁷ was possible using Alchemy⁸ API. The Ethereum Query Gateway and the reasons to use Alchemy as primary gateway were also presented there. The smart contracts can easily be deployed on the testnet via Alchemy. In my case, I created the project and obtained the associated project secrets. Here the project secrets are set of confidential and secure authentication credentials such as API keys and authentications tokens. This serve as a secure way to identify and verify the authenticity of the user or application when connecting to Alchemy's services.

I first deployed the system in Gorilla testnet but due to system traffic I had to switch and redeploy my smart contract in Sepolia testnet. For the Sepolia endpoint, the associated URL was <https://eth-sepolia.g.alchemy.com/v2/secret>. I initialized a Hardhat project in a directory and installed the necessary packages using npm. Hardhat provides a local Ethereum network for development and testing purposes. In the 'hardhat.config.js' file, the following lines were added as shown in figure 3.19 and this configuration will be triggered using the migration command.

The initial smart contract templates were developed using the Solidity language. Migration files were

⁷<https://sepolia.etherscan.io/>

⁸<https://www.alchemy.com/>


```

module.exports = {
  defaultNetwork: "hardhat",
  networks: {
    hardhat: {
      chainId: 1337,
    },
    sepolia: {
      url: "https://eth-sepolia.g.alchemy.com/v2/HFriUW9vbAxx_9vzNs_2JYGtYyvWyA-t",
      // url: "https://eth-goerli.g.alchemy.com/v2/AFg44fwI4dzYHzJ-Cy40li-y9-Ds50oQ",
      accounts: [
        "0b031d356319dc3308ed6b6580df3f3bdc9db8efbce35c81b9a3f62b3b26f596",
      ],
    },
  },
  solidity: {
    version: "0.8.4",
    settings: {
      optimizer: {
        enabled: true,
        runs: 200,
      },
    },
  },
};

```

Figure 3.19: Hardhat Configure

created for the smart contracts, and then they were deployed onto the Sepolia testnet blockchain using the migration command: `'npx hardhat run scripts/deploy.js --network sepolia'`. I added the following lines as shown in figure 3.19 to configure my system with the network. The successful deployment resulted in JSON files in the build directory containing network information such as the contract address, transaction hash, and events to access the smart contract. This information was used to establish the connection between the application and the smart contracts deployed on the blockchain. By leveraging Alchemy and Hardhat, the deployment of NFT smart contracts becomes more streamlined and efficient, allowing developers to focus on building the desired functionality while relying on the infrastructure provided by these tools.

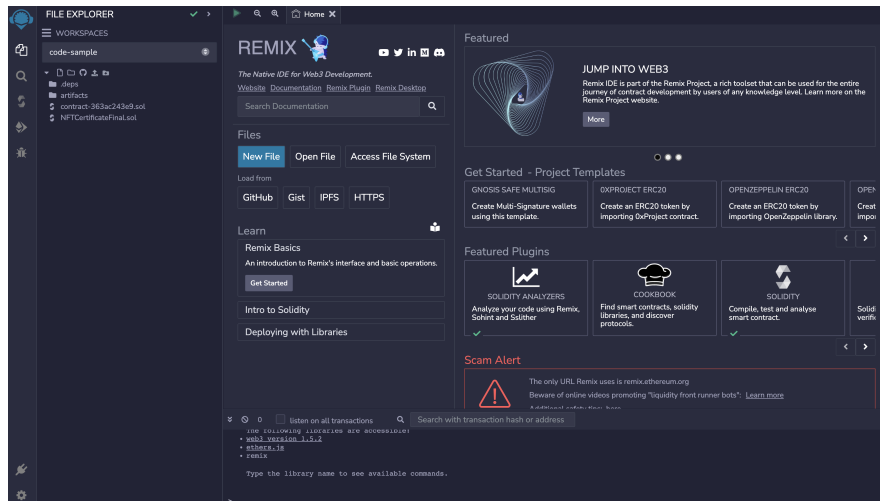


Figure 3.20: Remix IDE

I used Remix online IDE to deployed and test run the smart contract before I added it to the system. Remix shown in figure 3.20 offers a built in compiler that can compile solidity code into bytecode, which can

be executed in the ethereum virtual machine(EVM). Also it provides us with a powerful testing environment, enabling developers to write and run unit tests for the smart contracts.

3.3.3 NFT Smart Contracts Execution

According to the ERC721 standard, I define the metadata JSON schema to represent the certificate as shown below. It includes institute details, degree details, student details, course issued to the students, and the respective wallet address details as shown in figure 3.21. The shown JSON is of viewNFT where there is data related to the originalToken as well as the data related to viewNFT.

```
{
  "Title": "Certificate Metadata",
  "Description": {
    "Creator": "String",
    "Owner": "String",
    "StudentID": "String",
    "StudentWalletAddr": "String",
    "StudentName": "String",
    "StudentDescription": "String",
    "OriginalHash": "String"
    "OriginalNFT": {
      "TokenId": "uint256",
      "TokenURI": "String",
      "Subjects": [
        {"mark": "String", "subject": "String"},
        {"mark": "String", "subject": "String"}
      ]
    }
  },
  "ViewNFT": {
    "TokenId": "uint256",
    "TokenURI": "String",
    "ViewSubjects": [
      {"mark": "String", "subject": "String"},
      {"mark": "String", "subject": "String"}
    ]
  }
},
"UniversityName": "String",
"UniversityID": "String",
"UniversityAddress": "String",
"UniversityMetadata": "String",
"Degree": "String",
"CertificateHash": "String"
}
```

Figure 3.21: ViewNFT Certificate Metadata JSON

Here, the course in the schema is dynamically set by the university/institute that is creating the profile for the student. The viewSubjects are the subjects that students filtered from the original list of subject to create a viewNFT. The smart contract is deployed just once for each node on the Ethereum blockchain which stores the access control and tokenID to identify the user who minted their certificate issued to them by

their University/Institute. The receiver can view the course subjects that the student has set, and the smart contract keeps track of the changes made by the student. If the receiver wants to verify the authenticity of the academic credential, the receiver can view the original metadata validated by the university and decrypt the signature using the university public key to get access to the hash. After receiving the hash, the receiver can verify the authenticity of the data by comparing the hash value. Since the NFT allows verification of its history regarding ownership, it is easier to verify the owner's address. I used OpenZeppelin smart contracts to create my NFTCertificate sharing smart contract. The smart contract developed with Solidity contains the following functions as shown in figure 3.22.

```

{
contract NFTCertificate is ERC721URIStorage {
    struct ListedToken {
        uint256 tokenId;
        address payable owner;
        address payable viewer;
        uint256 transferBackTime;
        bool currentlyListed;
        bool currentViewer;
    }
    struct TokenTransferScheduler {
        uint256 transferBackTime;
        address transferBackTo;
    }
    event TokenListSuccess(
        uint256 indexed tokenId,
        address owner,
        address viewer,
        uint256 transferBackTime,
        bool currentlyListed,
        bool currentViewer
    );

    function createToken(string memory, address )public payable returns (uint)
    function createListedToken(uint256 ) private()
    function getAllNFTs() public view returns (ListedToken[] memory)
    function getMyNFTs() public view returns (ListedToken[] memory) {
    function getTransferredNFTs() public view returns (ListedToken[] memory)
    function executeTransfer(uint256 , address , uint256 ) onlyOwner ()
    function transferOwnership(uint256 ) onlyOwner()
}

```

Figure 3.22: Smart contract of NFT based certificate sharing system

The `createToken()` method as shown in figure 3.22 and in the sequence diagram figure 3.23 takes the `tokenURI` as a parameter, which is a hash value generated after uploading the metadata to IPFS. The data from the firestore is given in JSON format with all the necessary metadata. The metadata is first uploaded to IPFS using the Pinata API. This function mints an NFT and assigns ownership to the student wallet address. The `createListedToken()` function is used solely to keep track of the number of NFTs issued via the smart contract. To display data on the frontend of the application, I needed to create additional

methods, such as `getAllNFTs()`, which lists all NFTs issued using the smart contract, and `viewNFT()`, which displays a particular NFT. Similarly, the `getMyNFTs()` method returns a list of all the `viewNFTs` owned by the current user, while the `getTransferredNFTs()` method retrieves a list of `viewNFTs` that have been transferred to universities and employers. The `executeTransfer()` method in the smart contract is used to transfer view rights to an Ethereum address. The owner can set a default time period after which the `transferOwnership()` function is executable to reclaim the viewing rights of the NFTs. The owner can revoke view rights by calling the `transferOwnership()` method from the application frontend.

3.4 Conclusion

In my proposed solution framework, I aim to revolutionize certificate issuance and ownership by adopting a decentralized approach. By granting students control over distributing views of their academic credentials, this approach empowers them in a unique way. Additionally, my framework leverages Ethereum cryptocurrency for transactions, ensuring streamlined processes and transparency throughout. An important feature of my solution is the ability for students to mint `viewNFTs` (Non-Fungible Tokens) from their certificate credentials. This functionality offers a higher level of customization and control over academic certificates. By harnessing the capabilities of NFTs and blockchain technology, I can effectively address the limitations of traditional certificate systems. To provide further guidance in designing a similar system for the intended purpose, this chapter presents an illustration of the conceptual framework architecture. This visual representation shown in figure3.3 will aid in the development of a robust and efficient solution. The next chapter presents a user study, which evaluates the framework on a real-life blockchain-based system using the TAM method, augmented with a trust model. This comprehensive evaluation will provide valuable insights into the effectiveness and practicality of the proposed solution.

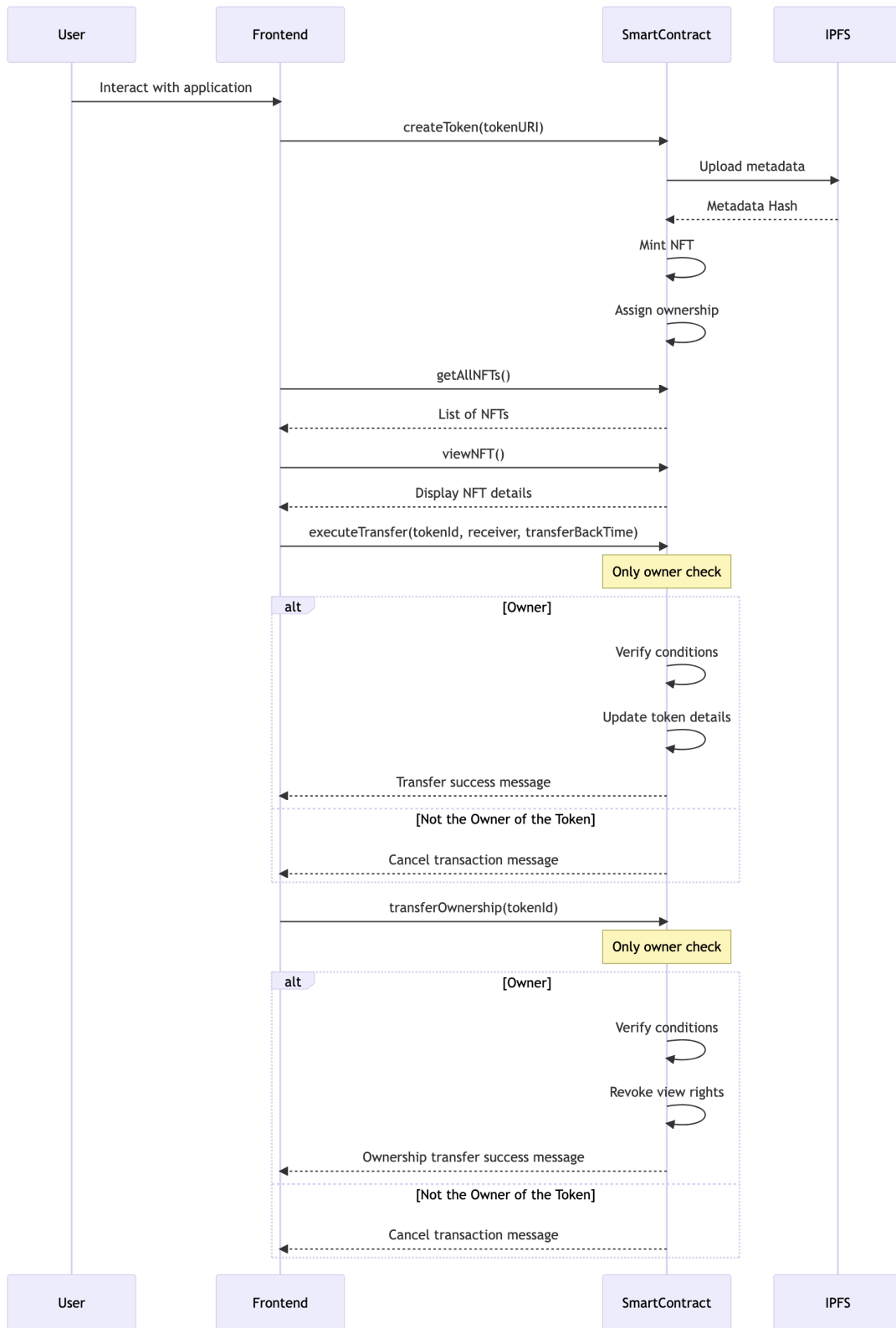


Figure 3.23: Smart Contract Execution Sequence diagram

4 System Evaluation: Methodology, Experiment Design, and Result

As described in the previous chapter, I have developed a comprehensive blockchain-based prototype model that grants students ownership of their certificates in the form of NFTs. Based on the findings from previous chapters, blockchain technology, specifically non-fungible tokens (NFTs), has emerged as a promising solution for transforming data management models across various domains such as healthcare, agriculture, supply chain, and education. In simple terms, an NFT-based system enables users to: 1) Establish proof of uniqueness, ownership, and origin of activities conducted, 2) Share data, such as certificates, without relinquishing control or ownership, and 3) Maintain control over data access. However, due to the general public's limited familiarity with blockchain and NFTs, it remains uncertain whether users will adopt a system that is implemented with these technologies. Therefore, it is crucial to investigate user acceptance and trust in the blockchain-based application. There exist studies in the literature that have evaluated the performance of blockchain based systems used for sharing data such as user credentials, user owned research findings, etc., but to my best knowledge, there have been no users studies specifically dedicated to examining user acceptance of NFT-based blockchain systems. The closest work to mine is that of Shrestha et al. [35] who conducted a user acceptance study of a blockchain system, which did not include NFTs. The application evaluated in that work was for sharing user profile data and user owned scientific data. To bridge this gap and advance research on user acceptance of NFT in a blockchain based system, I adopted the Technology Acceptance Model (TAM) as a theoretical framework [12] [13][14]. TAM is one the most influential models used to examine the indicators that affect the user's acceptance of interactive systems [37].

This chapter provides an overview of the methodology, research questions and hypotheses, experimental design and procedure, participant demographics, as well as participant consent forms with tools used in the study.

4.1 Methodology

The Technology Acceptance Model (TAM) is an information systems theory that explains how to encourage users to accept and utilise new technology [12]. TAM stipulates that the attitude and intention to use an application is determined by an evaluation of the trade-off between the perceived usefulness of the system and the perceived difficulty of using it. Perceived usefulness is defined as the individual's perception of the

extent to which the use of a given technology improves performance and perceived ease of use - as the degree to which a person believes that using a particular system is free of effort. TAM-based frameworks have been widely used to evaluate the likelihood that an application would be accepted by users.

The four TAM constructs are shown in table 4.1. A validated survey consisting of items related to the four TAM constructs was used as a research instrument. Based on the findings from previous studies conducted by Davis in 1989, Davis and colleagues in 1992 [13][14], I initiated a similar research endeavor. The corresponding extended TAM is shown in figure 4.1.

In my case, my study is centered around examining user attitudes regarding the acceptance of applications based on blockchain technology. Similar studies, such as the one conducted by Shrestha et al. (2021) [35], serve as examples.

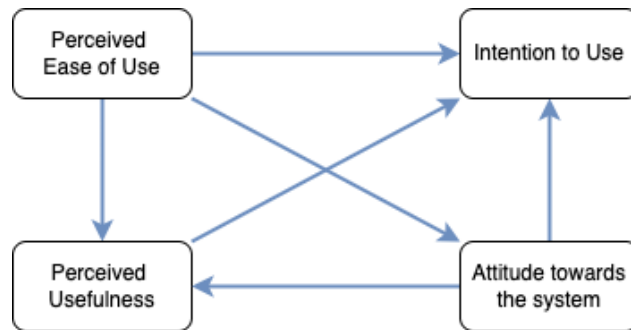


Figure 4.1: An extended TAM model for my study

The survey instrument included questions (here-forth called "items") related to the four TAM model constructs to measure participants' perceptions and attitudes. The set of TAM constructs comprised perceived ease of use (6 items), perceived usefulness (5 items), intention to use (2 items), perceived security (3 items), trust (9 items), attitudinal privacy (4 items), behavioral privacy-general caution (3 items), and attitude towards the system (2 items). The list of the items related to each of the four TAM constructs is shown in table 4.2. Participants rate their responses on a 7-point Likert scale ranging from strongly disagree (1) to strongly agree (7).

4.2 Research Hypotheses

In this section, I present my research hypothesis, research question, measurement instrument and the demographic of participants. I set several hypotheses, based on the literature review, to investigate the relationships between TAM constructs as given in table 4.1, which are as follows. For brevity below I use "the system" to refer to the proposed the certificate sharing system using NFT and blockchain framework.

H1: The *perceived ease of use* will significantly influence the *perceived usefulness* of the system.

H2: The *attitude towards the system* will significantly influence the *perceived usefulness* of the system.

H3: The *perceived ease of use* will significantly influence the intention to use system.

H4: The *perceived usefulness* will significantly influence the intention to use the system.

H5: The *attitude towards the system* will significantly influence the intention to use the system.

H6: The *perceived ease of use* will significantly influence the attitude to use the system.

H7: The combined effect of *perceived ease of use*, *perceived usefulness* and *attitude towards the system* will significantly influence the intention to use the system.

Construct	Definition
Perceived Ease of Use (PEOU)	The degree to which a person believes that using a particular system would be free of effort.
Perceived Usefulness (PU)	The degree to which a person believes that using a particular system would enhance his or her job performance.
Attitude towards the system (ATS)	The degree to which a person is favourable or unfavourable evaluation of a system or technology
Intention to use (ITU)	The degree to which a person has a behavioral intention to adopt the technology.

Table 4.1: Definitions of Constructs

4.3 Experiment Design

I conducted an experiment to evaluate user acceptance and usage of my blockchain-based prototype model for academic data sharing. The participants in the experiment used a fully deployed prototype platform of the NFT based certificate sharing system. To evaluate the likelihood of users adopting the proposed system I had to investigate (based on the study participants' answers to the respective survey questions) the influence of the perceived usefulness and perceived ease of use on the user's attitude towards the system and intention to use the system.

To recruit participants for my survey, I posted an advertisement on the university portal "Paws," targeting current students of the university. Eligible and interested participants were invited to provide their consent to participate in the study. The study itself took place in a controlled computer lab setting. Before commencing the survey, participants were equipped with essential context through a concise overview video on blockchain technology and non-fungible tokens (NFTs). This video served to familiarize participants with the framework. Participants were then given the opportunity to engage with the system actively. This hands-on experience allowed participants to interact with the system from various user perspectives, offering a comprehensive

Construct	Items
Perceived Ease of Use (PEOU)	<p>peou1 - Learning to operate this system is easy.</p> <p>peou2 - I find it easy to get this system to do what I want it to do.</p> <p>peou3 - My interaction with this system is clear and understandable.</p> <p>peou4 - I find this system to be flexible to interact with.</p> <p>peou5 - I feel it is easy to become skillful at using this system.</p> <p>peou6 - I find this system easy to use.</p>
Perceived Usefulness (PU)	<p>pu1 - Using the system would improve performance in certificate sharing with transparency and privacy.</p> <p>pu2 - Using this system would increase effectiveness in privacy policy formulation.</p> <p>pu3 - Using this system would make it easier for me to set certificate sharing preferences.</p> <p>pu4 - Using the system would increase productivity in certificate sharing with more control over privacy.</p> <p>pu5 - I find this system useful for setting my certificate sharing preferences.</p>
Attitude towards the system (ATS)	<p>ats1 - I believe that using the blockchain-based system would be beneficial for me.</p> <p>ats2 - In my opinion, it would be desirable for me to use the blockchain-based system.</p> <p>ats3 - It would be good for me to use the blockchain-based system.</p>
Intention to Use (ITU)	<p>itu1 - I would like to use this system to set certificate sharing preferences.</p> <p>itu2 - I would enjoy using this system when I need to use it.</p> <p>itu3 - It is worthwhile to use this system to set certificate sharing preferences.</p> <p>itu4 - I will use this system to decide how my data is shared.</p>

Table 4.2: Construct and items

evaluation. To be able to interact with the blockchain, the participants had to sign up with a wallet into the system. Then the participants were then presented with another short video. This video specifically clarified the roles and functionalities associated with different user types within the system (University, Student, Employer). Participants were given the freedom to watch this video at their own discretion, gaining insights into what each user type could achieve within the system. Following this video presentation, participants could select any user role (University, Student, or Employer), and explore the corresponding functionalities. They were actively encouraged to assess the system from multiple user viewpoints.

The participants were able to not only view their issued certificates but also create additional certificates, filter subjects, and share them with other institutions. This allowed us to comprehensively assess the system's usability and effectiveness in meeting the diverse needs of its users.

After interacting with the system, the participants proceeded to complete the survey, which was administered via SurveyMonkey. The survey's questions were designed to gauge various aspects of participants' attitudes and intentions related to the blockchain-based prototype model for academic certificate sharing. Specifically, these questions aimed to measure perceived usefulness, perceived ease of use, attitude towards the system, and intention to use the system. This data was gathered to assess user acceptance and usage comprehensively.

To conclude the survey, participants were invited to share comments, providing their qualitative feedback. This provided them with the opportunity to report any observed issues or suggest areas for improvement. This qualitative feedback was subjected to analysis to pinpoint specific challenges and opportunities for enhancement. The combined dataset, comprising both quantitative survey data and qualitative feedback, forms the basis for my comprehensive evaluation of user acceptance and usage of the prototype model for academic data sharing.

To refine my experiment design and survey questionnaire, I conducted an initial pilot study involving five quantitative research experts from the University of Saskatchewan. This pilot study aimed to evaluate the study's feasibility and duration and to enhance the overall study design. Participants in the pilot study provided valuable feedback on the survey, which I considered alongside input from research experts to modify and restructure the final survey questionnaires.

My research protocol received ethical approval from the University of Saskatchewan's Behavioral Research Ethics Board (Beh-REB) through a delegated review process (Beh ID 4046).

I chose structural equation modeling (SEM) as the primary statistical technique for analysing the quantitative data collected in the study because of its capacity to concurrently analyze multiple variables and their relationships. SEM provides a comprehensive modeling approach that allows examining the interplay between the variables measured in my study: perceived usefulness, perceived ease of use, attitude towards the system, and intention to use.

In the next section, I present the data collected and the statistical analysis results obtained using SEM. Specifically, I will scrutinize the path coefficients (β), assess significance levels (p), and evaluate the coefficient

of determination (R^2). Moreover, I will elucidate the effects observed in perceived usefulness, perceived ease of use, and the combined impact of all antecedents on intention to use. I will provide explanations for the significance or insignificance of these effects. This structured approach ensures the presentation of my statistical analysis and results in a clear and logical sequence.

4.3.1 Data Collection

To ensure ethical compliance for privacy according to my study approval by the Beh-REB, I did not record the participants' actions on the system during their tasks. However, I took note of their comments and points of confusion during their interaction with the system. A total of 40 participants took part in the study. Around 33.3% of the participants were somewhat familiar and 63% of the participant were very familiar with the blockchain and smart contract technology. Similarly, 28.21% were somewhat familiar with the concept of NFT and 62% were highly familiar with the concept of NFT but not in the context of applications related to academic certificates. The participant demography is shown in table 4.3. As mentioned above, the study was advertised within the University and participation was done in person, so almost all participants were students. All the data were complete data even after the first phase of data cleaning.

Respondent Characteristics	Criteria	Percentage
Highest Education Level	Grad-High School	12.82%
	Bachelors	25.64%
	Masters	38.46%
	PhD	23.08%
Requested academic credits transfer between universities	Yes	76.92%
	No	23.08%
What medium was used for the credits transfer	Post/mail(paper-based)	30.0%
	Electronic(sent by university via email)	43.33%
	Both using email and post	20.0%
	Using certificate/credit sharing platform	6.67%
Familiar with blockchain technologies and smart contract	Extremely familiar	17.95%
	Very familiar	46.15%
	Somewhat familiar	33.33%
	Not so familiar	2.56%
Familiar with the concept of Non fungible token	Extremely familiar	23.08%
	Very familiar	38.46%
	Somewhat familiar	28.21%
	Not so familiar	10.25%

Table 4.3: Participants' demographics

4.4 Result

In this section, I first present and briefly analyze the collected data with descriptive statistics. Then I present the result of the structural equation model(SEM), which includes the measurement model (internal consistency, composite reliability and average variance extracted, structural models (exploratory factor analysis, regression analysis and brief analysis of results). I have used Ms excel and SmartPls software to calculate the descriptive statistics and pls-sem.

4.4.1 Descriptive Statistic

Since I measured the responses to the items on a 7-level Likert scale, I categorized the scale in seven score ranges to analyze the score for each item and overall impression of the construct. Table 4.4 provides the category of the different score ranges of the 7-scale Likert scale. Tables 4.5 to table 4.8 summarize the data collected for the items in each of the four TAM constructs: perceived ease of use, perceived usefulness, attitude towards the system and intention to use.

Score Range	Category
$6 < x \leq 7$	Extremely High
$5 < x \leq 6$	Quite High
$4 < x \leq 5$	Slightly High
$3 < x \leq 4$	Neither
$2 < x \leq 3$	Slightly Low
$1 < x \leq 2$	Quite Low
$0 < x \leq 1$	Extremely Low

Table 4.4: Score Ranges and Categories

The obtained scores for different selected constructs indicate that user perceptions on the benefits of using the proposed system should be maintained or enhanced by making improvements in order to achieve a higher level of score category. The preliminary descriptive statistic of the obtained data shows that all the constructs provide a significant impression in the context of user acceptance of the usable certificate sharing system using NFT and blockchain prototype. Figure 4.2 shows the average results obtained for each of the constructs, which are in the quite high and extremely high category.

Perceived Ease of Use (PEOU)		
Indicators	Score	Std. Deviation
Ease of Learning	5.718	1.218
Controllable	5.795	1.304
Understandable	5.974	1.000
Flexible	5.923	0.917
Effort to Skillful	6.103	1.008
Easy to Use	5.923	1.047
Total Average	5.906	
Category	Quite High	

Table 4.5: Analysis of Perceived Ease of Use (PEOU)

Perceived Usefulness (PU)		
Indicators	Score	Std. Deviation
Job Performance	6.590	0.741
Effectiveness	6.205	1.090
Makes Job Easier	6.308	1.244
Increase Productivity	6.333	1.117
Useful	6.205	0.992
Total Average	6.3282	
Category	Extremely High	

Table 4.6: Analysis of Perceived Usefulness(PU)

Intention to Use (ITU)		
Indicators	Score	Std. Deviation
Worthwhile to use	6.077	1.328
Use for sharing certificate data	5.923	1.289
Intend to use for sharing certificate data in future	6.051	1.218
Necessary to use to share certificate data	5.974	1.459
Total Average	6.006	
Category	Extremely High	

Table 4.7: Analysis of Intention to Use (ITU)

Attitude towards the System (ATS)		
Indicators	Score	Std. Deviation
Beneficial System to use	5.949	1.319
Desirable to use	5.795	1.399
Good system to use	5.795	1.417
Total Average	5.846	
Category	Quite High	

Table 4.8: Analysis of Attitude towards the System (ATS)

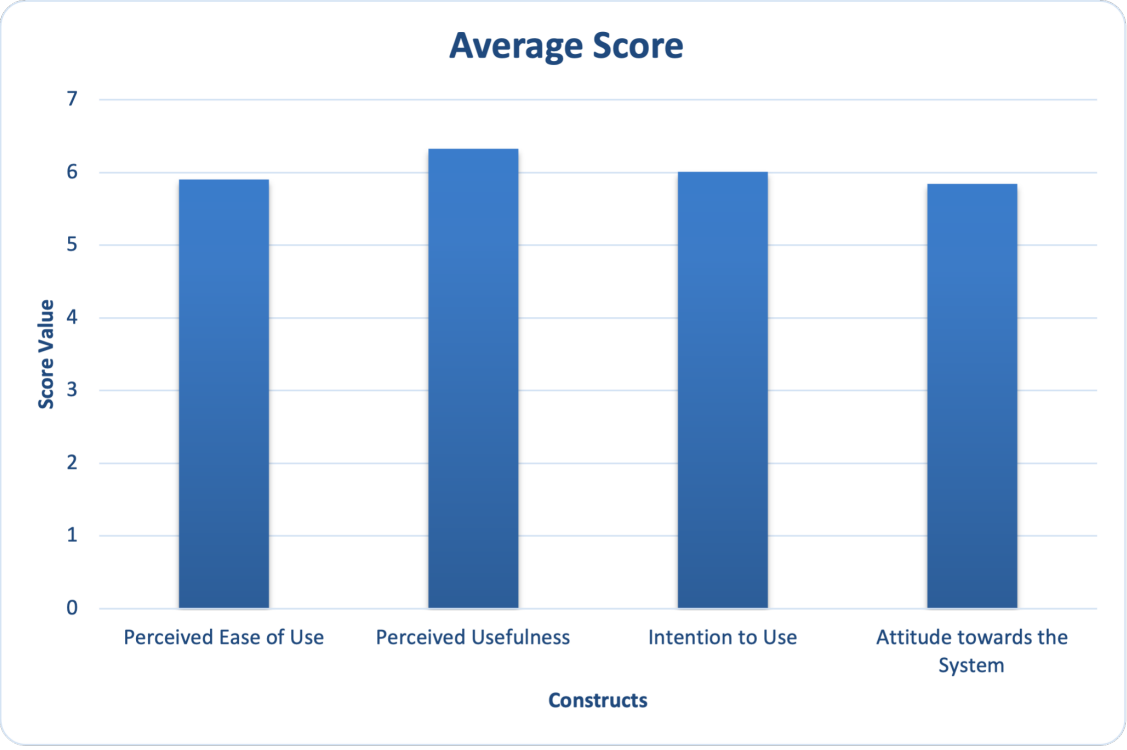


Figure 4.2: Analysis of all the constructs

4.4.2 Measurement Models

I checked the measurement model with exploratory factor analysis by testing the internal data consistency, reliability, and validity of the constructs. Here I assess the relationship between the observed variable(items) and the latent constructs.

a. Factor Loading

The measurement model's crucial parameter is factor loading, which indicates the strength of relationships between observed variables(items) and their underlying latent constructs. It determines whether items within each variable are more closely associated with their own construct rather than with other constructs. According to [20], factor loading's greater than 0.50 are considered significant. In table 4.9 the factor loadings for each construct and their respective items are presented. The table reveals that the "ATS" construct (ats1, ats2, ats3) exhibits high factor loadings, ranging from 0.938 to 0.952, suggesting a strong association between the observed variables (items) and the latent construct they represent. Similarly, the "ITU" construct (itu1, itu2, itu3, itu4) also shows strong factor loadings, ranging from 0.881 to 0.950, indicating a reliable measurement of this latent constructs. The same applies for the observed variables(items) related to "PEOU" (peou1 to peou6) and "PU" (pu1 to pu5) constructs, which demonstrate substantial factor loadings, ranging from 0.772 to 0.925 for PEOU and from 0.722 to 0.934 for PU.

These noteworthy factor loadings provide evidence of the measurement model's adequacy and accuracy in capturing the underlying constructs. Overall, the results derived from the factor loadings support the construct validity of the measurement model, indicating that the observed variables(items) effectively represent their respective latent constructs.

b. Reliability

Reliability refers to the consistency and stability of measurements obtained from a scale or instrument. In the context of the measurement model, it is an essential aspect that ensures the indicators are measuring the latent construct accurately and precisely.

Cronbach's Alpha

Cronbach's Alpha, represented by the symbol α (alpha), is a widely used metric for evaluating the internal consistency reliability of a measurement scale or a set of indicators. It plays a crucial role in assessing how well the items within each construct interrelate and consistently measure the underlying concepts. Ranging from 0 to 1, where 0 indicates no internal consistency and 1 indicates perfect internal consistency, a higher Cronbach's Alpha value indicates greater internal consistency and reliability of the measurement scale. Looking at the table 4.10, I can observe the Cronbach's Alpha values for each construct in the system acceptance evaluation. The "Attitude towards the System" construct demonstrates a high Cronbach's Alpha value of 0.936, suggesting excellent reliability. Similarly, the "Intention to Use" construct also exhibits a

	ATS	ITU	PEOU	PU
ats1	0.938	-	-	-
ats2	0.935	-	-	-
ats3	0.952	-	-	-
itu1	-	0.950	-	-
itu2	-	0.906	-	-
itu3	-	0.931	-	-
itu4	-	0.881	-	-
peou1	-	-	0.925	-
peou2	-	-	0.874	-
peou3	-	-	0.812	-
peou4	-	-	0.775	-
peou5	-	-	0.785	-
peou6	-	-	0.854	-
pu1	-	-	-	0.801
pu2	-	-	-	0.722
pu3	-	-	-	0.934
pu4	-	-	-	0.871
pu5	-	-	-	0.808

Table 4.9: Exploratory factor loading

strong Cronbach’s Alpha value of 0.937, indicating excellent reliability as well.

For the constructs ”Perceived Ease of Use” and ”Perceived Usefulness,” the Cronbach’s Alpha values are 0.915 and 0.885, respectively. These values fall within the range of 0.80 to 0.89, indicating good reliability for both constructs. In summary, the Cronbach’s Alpha values provide valuable insights into the consistency and reliability of the measurement scales used to assess users’ attitudes, intentions, and perceptions regarding the system acceptance. With high Cronbach’s Alpha values, I can have confidence in the internal consistency of the measurement model, which enhances the credibility and trustworthiness of the study’s findings and conclusions.

Composite Reliability

Composite Reliability, denoted as CR, is an essential metric used to evaluate the internal consistency and reliability of a measurement model in structural equation modeling (SEM). Similar to Cronbach’s Alpha, Composite Reliability assesses how well the indicators within each construct consistently measure the underlying concepts. It also ranges from 0 to 1, with higher values indicating greater internal consistency and reliability. The Composite Reliability of each construct is shown in the rightmost column in table 4.10.

The "Attitude towards the System" construct demonstrates excellent internal consistency with a Composite Reliability value of 0.959, reflecting its robust reliability. Similarly, the "Intention to Use" construct also exhibits high internal consistency with a Composite Reliability value of 0.955, indicating its dependable measurement. For the constructs "Perceived Ease of Use" and "Perceived Usefulness," the Composite Reliability values are 0.934 and 0.917, respectively. These values fall within the range of 0.80 to 0.89, signifying good reliability for both constructs.

It is recommended that CR should be above 0.75. In my study, CR for each construct was above 0.80, demonstrating a high level of internal consistency and reliability in the measurement model. These robust CR values reinforce the credibility of my findings and support the trustworthiness of the study's conclusions. The results affirm that the measurement scales used to assess users' attitudes, intentions, and perceptions regarding system acceptance are dependable and suitable for analysis, providing valuable insights into the research domain.

Construct	Cronbach's Alpha (α)	Composite Reliability (CR)
Attitude towards the System	0.936	0.959
Intention to Use	0.937	0.955
Perceived Ease of Use	0.915	0.934
Perceived Usefulness	0.885	0.917

Table 4.10: Reliability Measures

c. Construct Validity

Construct validity is a crucial aspect of a measurement model and refers to the extent to which a set of items or observed variables accurately measures the underlying construct they are intended to represent.

Convergent Validity

Convergent validity is a critical aspect of a measurement model that evaluates the extent to which different indicators, expected to measure the same underlying construct, are closely related. It aims to determine whether the items collectively and accurately capture the intended latent construct. In this assessment, higher factor loadings indicate stronger convergent validity, indicating that the indicators are indeed measuring the same construct as expected. In my study, I utilized the Average Variance Extracted (AVE) value to identify the convergent validity of the measurement model. The AVE represents the average amount of variance captured by the indicators in relation to their corresponding latent construct. AVE values should ideally be greater than 0.50 to establish convergent validity. From table 4.11, we can observe the AVE values for each construct in the system acceptance evaluation. The "Attitude towards the System" construct has an AVE of 0.886, the "Intention to Use" construct has an AVE of 0.842, "Perceived Ease of Use" has an AVE of 0.704, and "Perceived Usefulness" has an AVE of 0.69.

Since all AVE values are greater than the recommended threshold of 0.50, this indicates that my measurement model has successfully established convergent validity. The indicators within each construct are closely related, demonstrating that they collectively measure the underlying constructs as intended.

Construct	Average Variance Extracted (AVE)
Attitude towards the System	0.886
Intention to Use	0.842
Perceived Ease of Use	0.704
Perceived Usefulness	0.690

Table 4.11: Reliability and Validity Measures

Discriminant Validity

Discriminant validity is a crucial aspect of a measurement model that ensures each construct maintains its distinct identity, and there is minimal overlap or shared variance between constructs. It aims to assess whether the indicators within each construct are more strongly related to their own construct than to other constructs. One commonly used criterion to evaluate discriminant validity is the Fornell-Larcker criterion.

In the Fornell-Larcker criterion, I compared the square root of the Average Variance Extracted (AVE) for each construct ($\sqrt{AVE_i}$) to the correlation values between constructs ($\text{Correlation}(i, j)$). The square root of AVE represents a construct's unique variance, while the correlation values indicate the shared variance between constructs. To establish discriminant validity, the square root of AVE for each construct should exceed the correlation values with other constructs.

$$\sqrt{AVE_i} > \text{Correlation}(i, j)$$

Where:

- $\sqrt{AVE_i}$ represents the square root of AVE for Construct i .
- $\text{Correlation}(i, j)$ represents the correlation between Construct i and Construct j .

In table 4.12, we can observe the Fornell-Larcker criterion matrix, which presents the correlation values between constructs and the square root of AVE for each construct. The matrix confirms that the square root of AVE for each construct (diagonal elements) is higher than any value in the same column (off-diagonal elements). This indicates that the construct's unique variance is indeed greater than the shared variance with other constructs. As a result, my measurement model successfully demonstrates discriminant validity. The indicators within each construct are more strongly related to their own construct than to other constructs, confirming that each construct has its own distinct identity.

	Attitude towards the System	Intention to Use	Perceived Ease of Use	Perceived Usefulness
ATS	0.942			
ITU	0.830	0.917		
PEOU	0.668	0.761	0.839	
PU	0.776	0.865	0.784	0.831

Table 4.12: Fornell-Lacker criterion Matrix

4.4.3 Structural Model

I built a structural model with the four constructs (perceived ease of use, perceived usefulness, attitude towards the system, and intention to use) that potentially influence the user adoption of the proposed certificate sharing framework using NFT and blockchain, which was presented in figure 4.3.

I conducted Structural Equation Modeling (SEM) analysis to assess the strength of the relationships and the variance explained by antecedents, by calculating coefficients of determination (R^2) and path coefficients (β). Path coefficients represent the strength and direction of the relationships between constructs. while (R^2) determines the proportion of variance of the constructs. A higher (R^2) value indicates that a significant portion of the variance observed in the dependent variable can be attributed to or explained by the inclusion of the independent variables in the model.

The results of the analysis are summarized in tables 4.13, 4.14, and 4.15. According to Chin's guidelines [9], a path coefficient should be ≥ 0.2 to be deemed relevant. Regarding statistical significance, a model is considered somewhat significant if the p-value is < 0.1 , quite significant if $p < 0.01$, and highly significant if $p < 0.001$ [10]. In my study, the direct path coefficient analysis (table 4.13) showed that the attitude towards the system (ATS) has a statistically significant influence on the intention to use (ITU) the certificate sharing system ($\beta = 0.374$, $p = 0.023$), as well as on the perceived usefulness (PU) of the system ($\beta = 0.457$, $p = 0.006$). Furthermore, perceived usefulness (PU) significantly influences the intention to use (ITU) the system ($\beta = 0.452$, $p = 0.030$). Additionally, perceived ease of use (PEOU) significantly influences the perceived usefulness (PU) of the certificate sharing system ($\beta = 0.478$, $p < 0.001$). However, PEOU's direct effect on the intention to use (ITU) was not statistically significant ($\beta = 0.156$, $p = 0.165$). Importantly, PEOU also has a significant direct effect on the attitude towards the system (ATS) ($\beta = 0.668$, $p < 0.001$).

Moving on to the indirect path coefficient analysis (table 4.14), In my indirect path coefficient analysis, I found several significant findings. First, there is a statistically significant indirect effect of perceived ease of use (PEOU) on perceived usefulness (PU) through the attitude towards the system (ATS) ($\beta = 0.305$, $p = 0.012$). This result suggests that PEOU significantly influences PU through its impact on ATS. Second, I identified a significant indirect effect of PEOU on the intention to use (ITU) through perceived usefulness (PU) ($\beta = 0.216$, $p = 0.036$). This implies that PEOU indirectly affects ITU by way of its impact on PU. Furthermore, I observed another significant indirect effect where PEOU influences ITU through attitude

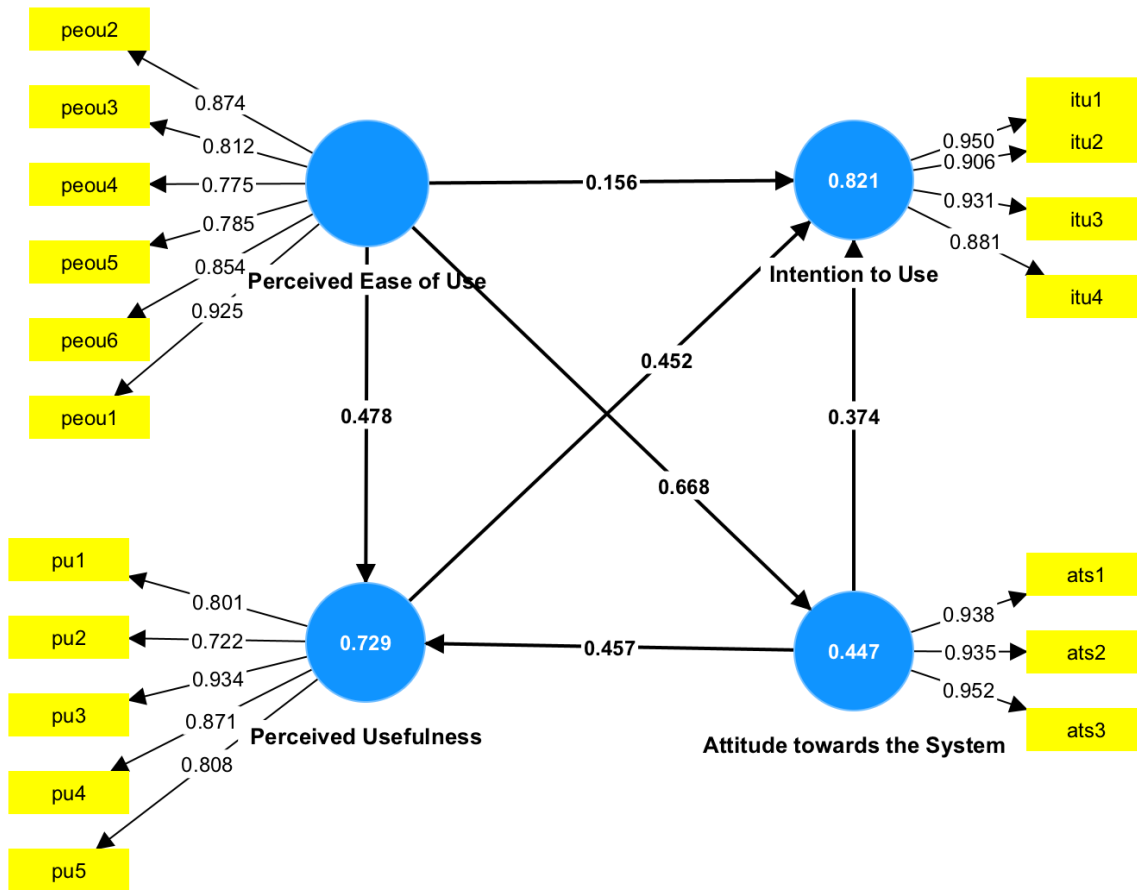


Figure 4.3: Analysis of all the constructs

towards the system(ATS)($\beta = 0.250, p = 0.032$). This indicates that PEOU indirectly shapes ITU through its influence on ATS. On a different note, the indirect effect of ATS on ITU through PU, while showing promise, is not statistically significant ($\beta = 0.206, p = 0.094$). This suggests that ATS directly influence PU and ITU as shown in 4.13, but its effect on ITU through PU does not meet the criteria for statistical significance. Finally, the indirect effect of PEOU on PU, subsequently affecting ITU through ATS, is also not statistically significant ($\beta = 0.138, p = 0.110$). This points to a complex relationship where PEOU's impact on ITU through ATS and PU does not reach the level of statistical significance.

The total effect path coefficient analysis (table 4.15) combines both the direct and indirect effects. This table presents standardized path coefficients (β), standard deviations, t-statistics, p-values, and (R^2) values for various constructs related to the intention to use the system. I found that the combined effects of perceived ease of use (PEOU), perceived usefulness (PU), and attitude towards the system (ATS) on the intention to use (ITU) were statistically significant ($p < 0.05$) and the path coefficients ranged from approximately 0.452 to 0.784.

Now, let's discuss the support for the hypotheses:

- Hypothesis H1 (The perceived ease of use will significantly influence the perceived usefulness) was supported, as evidenced by the significant direct path coefficient ($\beta = 0.478, p < 0.001$) and indirect path coefficient ($\beta = 0.305, p = 0.012$).

- Hypothesis H2 (The attitude towards the system will significantly influence the perceived usefulness) was supported, as evidenced by the significant direct path coefficient ($\beta = 0.457, p = 0.006$) and the indirect path coefficient ($\beta = 0.202, p = 0.094$).

- Hypothesis H3 (The perceived ease of use will significantly influence the intention to use) was not supported, as the direct path coefficient ($\beta = 0.156, p = 0.165$) was not statistically significant.

- Hypothesis H4 (The perceived usefulness will significantly influence the intention to use) was supported, as evidenced by the significant direct path coefficient ($\beta = 0.452, p = 0.030$).

- Hypothesis H5 (The attitude towards the system will significantly influence the intention to use) was supported, as evidenced by the significant direct path coefficient ($\beta = 0.374, p = 0.023$).

- Hypothesis H6 (The perceived ease of use will significantly influence the attitude to use the system) was supported, as evidenced by the significant direct path coefficient ($\beta = 0.668, p < 0.001$).

- Hypothesis H7 (The combined effect of perceived ease of use, perceived usefulness, and attitude towards the system will significantly influence the intention to use) was supported. as evidence by the significant p-value ($p < 0.05$) and ($R^2 = 0.821$).

	Path Coefficient	Standard Dev	T Statistics	P Value
ATS → ITU	0.374	0.187	2.002	0.023
ATS → PU	0.457	0.180	2.543	0.006
PEOU → ATS	0.668	0.133	5.042	0.000
PEOU → ITU	0.156	0.161	0.972	0.165
PEOU → PU	0.478	0.142	3.364	0.000
PU → ITU	0.452	0.241	1.876	0.030

Table 4.13: Direct Path Coefficient Analysis

	Path Coefficient	Standard Dev	T Statistics	P Value
PEOU → ATS → PU	0.305	0.135	2.263	0.012
PEOU → PU → ITU	0.216	0.122	1.777	0.036
PEOU → ATS → ITU	0.250	0.135	1.847	0.032
ATS → PU → ITU	0.206	0.157	1.314	0.094
PEOU → ATS → PU → ITU	0.138	0.113	1.226	0.110

Table 4.14: Indirect path coefficient analysis

	Path Coefficient	Standard Dev	T Statistics	P Value	R^2
ATS → ITU	0.581	0.149	3.897	0.000	0.821
PU → ITU	0.452	0.241	1.876	0.030	
PEOU → ITU	0.761	0.108	7.046	0.000	
ATS → PU	0.457	0.180	2.543	0.006	0.729
PEOU → PU	0.784	0.098	7.993	0.000	
PEOU → ATS	0.668	0.133	5.042	0.000	0.447

Table 4.15: Total effect path coefficient analysis

H	Hypothesis	Result
H1	The perceived ease of use will significantly influence the perceived usefulness.	✓
H2	The attitude towards the system will significantly influence the perceived usefulness.	✓
H3	The perceived ease of use will significantly influence the intention to use.	×
H4	The perceived usefulness will significantly influence the intention to use.	✓
H5	The attitude towards the system will significantly influence the intention to use.	✓
H6	The perceived ease of use will significantly influence the attitude towards the system.	✓
H7	The combined effect of perceived ease of use, perceived usefulness, and attitude towards the system will significantly influence the intention to use.	✓

Table 4.16: Summary of Hypotheses Results

4.4.4 Participants Comments

Table 4.17 shows the comments from the participants related to the adoption of the NFT based certificate sharing system . Most of the participants did not provide any comments, but those who provided the comments are focused mostly on the system’s potential to enhance security, confidentiality and transparency in sharing academic certificates. However, concerns were raised about the initial complexity of using the crypto wallet which is part of the system and the need for improved user-friendliness, especially for less tech-savvy individuals. Cultural and educational biases were also highlighted, emphasizing the importance of ensuring equal access for all users. Integrating NFT certificates with platforms like LinkedIn for validation and addressing scalability and performance issues were suggested for future improvements. While users recognized the system’s benefits, it was advised to focus on refining security measures, user experience, and cultural inclusivity to foster widespread adoption.

No.	Important Comments
1	"I still think that this system would be a learning curve for employers, university staff, and students. The old way of mailing transcripts was more expensive, but easier. I like how you can select which classes can be added to the transcript. I also like how there is privacy."
2	"I like the idea of using NFTs and blockchain to transfer university credentials, it would save money and time for future students. However, I think most people will need to take a while to learn how this whole system works and may take them a while to understand and get used to navigating it."
3	"The only concern I have is its security. This is a good system that helps certificate sharing process. I think it's smart, time, and money could be saved while ensuring the validity of certificates."
4	"NFT Certificates should be integrated with platforms such as LinkedIn for proper authentication and validation."
5	"Considering both privacy and convenience, I find it to be extremely helpful."
6	"I really enjoyed learning about this application. It is very much needed in every university. It is confidential and cannot let other organization to misuse your information."
7	"The elimination of an intermediate is a massive selling point for this system; hopefully this makes all future transactions like this more convenient."

Table 4.17: Important Comments from User Study

4.5 Discussion

I successfully accomplished the research objective of assessing user experience through the application of the Technology Acceptance Model (TAM) while incorporating an external construct into the conventional TAM framework. This investigation was conducted within the context of certificate sharing facilitated by Non-Fungible Tokens (NFTs) and blockchain technology.

My study also delved into users' willingness to embrace this novel system. The results have confirmed the majority of the proposed hypotheses. Specifically, I observed a noteworthy relationship between user's attitude toward the system and their perception of its usefulness, as well as their intention to utilize the system.

When users have a positive attitude to the system (after being informed about the system's security, privacy and trust while sharing their certificate thanks to the blockchain-based framework, and the ability to set permissions for data sharing thanks to smart-contracts and having ownership and control over the certificate even after sharing it thanks to NFT and smart-contracts), the system's perceived usefulness is high as well as the users' intention to use the system.

Here previous research by [32],[24] shows that the UI design is the most significant external construct that

affects perceived ease of use, and since my study used a prototype with limited functionality, the perceived ease of use may not have influenced the participants intention to use the system, which explains my result on not supporting H3.

This chapter argued for the importance of evaluating through a user study the design of platforms based on NFT and blockchain. These platforms are hard to evaluate because building a working application requires a lot of resources and a number of adopting organizations. Partial / layered evaluation using a prototype that mimics the functionality is the only feasible way to gain insight into the factors influencing the system's adoption. The main limitation of this study therefore is that the findings are based on a small sample size with a prototype system and participants were students who had less knowledge with the concept of blockchain. Some of the main challenges regarding the acceptance of distributed ledger-based such as NFT based certificate sharing system are skill gap, insufficient organizational awareness and lack of trust on the security of the underlying blockchain technology itself, which may be a result of stereotype beliefs regarding the volatility of cryptocurrencies and NFT markets.

4.6 Conclusion

User studies are much needed to evaluate technological solutions and observe the effects of different variables using theory-backed models. In this chapter, I presented an extended TAM based model to measure the relationship between perceived usefulness, perceived ease of use, attitude towards the system and intention to use constructs for a prototype certificate sharing system based on NFT and blockchain.

I implemented the descriptive statistic, measurement models, a structural model to present the results and used SEM analysis to find predictors of the users' acceptance of the proposed system. Although TAM constructs have been investigated previously as antecedents to user acceptance of different technologies in various domains, this work was the first to investigate the use of TAM for analyzing the factors influencing user acceptance of NFT academic certificate system, based on blockchain technology for certificate sharing and access control. Using the methodology of theory-based model building and evaluation through a user study and statistical analysis, it was possible to discover the factors that influence the intention to use, and the adoption of a platform. This has opened more directions to study application areas of NFT and blockchain from the user behaviour modeling prospective. It also demonstrates the use of theory informed modeling and simulated use cases study to gauge the adoption chances of new technologies that are too large and complex to evaluate directly with users.

5 Conclusion and Future work

This thesis proposes, implements and evaluates a student-centered certificate sharing framework using NFT and ethereum blockchain. The system allows students to have control over their academic certificate after receiving full ownership of the certificate. Beside defining ownership of credentials, students can set preferences and also create multiple versions (viewNFTs) that are copies of the original certificate without compromising the authenticity of the data. The students can create tailored viewNFTs for particular purposes or recipients as per their specific needs, and can share them by using ethereum address. Students can also revoke access right after the sharing purpose is accomplished or expired, because the student's ownership is defined in the blockchain with smart contract and the student is only sharing viewing rights to the viewNFT with the recipient.

The proposed framework allows more students and universities more flexibility and convenience in sharing student credentials among institutions and employers. Currently, many universities are already offering life-long learning opportunities through micro-credentials. The proposed viewNFT certificates allow students to generate versions of their full certificates by selecting only the credits and/or micro-credentials that are relevant to specific educational or employment opportunities, keeping irrelevant grades private.

Thus, my thesis proposes a new concept of student centered privacy preserving certificate sharing encoded in smart contract. The smart contracts are constructed when issuing the certificate as NFT and they define the student's ownership of the credentials. The thesis presents also an implementation of the framework that allows sharing the certificate in a decentralized fashion to other institutions and employers in much cheaper cost when I compared it with existing system cost. For instance, in my survey, I found that the total amount of ETH used by students was approximately 0.0002 ETH. To put this into perspective, when converted to the current exchange rate (1 ETH = 2238.5 CAD), it still amounts to less than 50 Canadian cents. This cost is considerably lower when compared to the fees associated with existing systems, such as MyCreds, which charges 10 CAD per certificate, and the traditional physical sharing method, which costs around 250 CAD. This highlights the cost-efficiency of utilizing NFTs for certificate sharing, making it an attractive and economical option for students.

The thesis also presents a usability study of a prototype application based on the proposed framework. The study with 40 University of Saskatchewan students allowed to find the relationships between different Technology Acceptance Model (TAM) constructs: ease of use, usefulness, attitude to the system and intention to use the system). The result of the study points to the important determinants that should be considered while designing and developing a blockchain and NFT-based platform for sharing certificate to increase its

acceptance by users.

5.1 Research Contributions

The significant contributions of my research include the following:

1. Conducted a systematic literature review on the application of Non-Fungible Tokens (NFTs) and their use in assets with both physical and digital value. Identified the need for a platform to enhance the current process of students sharing certificates with other universities for higher studies or employers for job applications (Chapter 2).
2. Designed and implemented a Non-Fungible Token (NFT) based certificate sharing system using blockchain and smart contracts. The system allows secure sharing of certificates while ensuring students retain control over access permissions (Chapter 3).
3. Conducted a user study and gathered quantitative and qualitative data to develop an extended Technology Acceptance Model (TAM) based on distinct constructs that influence the end user's intention to adopt the prototype certificate sharing system (Chapter 4).

5.2 Limitations

In the thesis, I have identified several issues and provided some solutions to them, with some of them remaining as limitations to be addressed in future works.

The current version of the framework is on a public blockchain, which raises concerns regarding the storage of sensitive information, such as student and personal data. While the framework currently employs hashing and digital signature encryption, using a private-public blockchain approach might be more suitable for sharing certificates securely. However, this approach may still face accessibility challenges for some users, as interacting with the blockchain and calling transactions could be complex and unfamiliar.

Another limitation lies in the use of Distributed Ledger Technology (DLT). While DLT offers tamperproof data solutions, it does not address all the privacy and security issues associated with decentralized applications and smart contracts. Past literature highlights various instances of security breaches and privacy infringements within these systems. Attempts to mitigate centralization limitations have led to the use of distributed databases like IPFS. However, the reliance on IPFS for data storage introduces a new concern as data can be regenerated using the CID hash of the IPFS.

The concept of Non-Fungible Tokens (NFTs) also presents challenges as the general public struggles to understand their context, particularly in relation to physical assets having digital footprint. This lack of understanding may hinder the broader adoption and acceptance of NFTs.

Regarding the usability study, the limited pool of participants and the lack of diversity in perspectives, as only students were involved, may affect the generalizability of the results. It would be beneficial to

include participants who are professionals in the roles of university administrators and employers to obtain a comprehensive evaluation. Furthermore, the reliability of the usability study results could be questioned because they were obtained solely from students who have never shared credentials. Thus the evaluation may not have fully grasped the issues faced by students who have never shared credentials, e.g. undergraduate students. Different circumstances and backgrounds could yield varying answers to the same questions.

Additionally, the cost associated with creating, sending, and transferring NFTs, as well as creating and viewing NFT certificates, might be a concern. The fluctuating value of ETH in CAD introduces uncertainty and may impact users differently depending on the market conditions.

In conclusion, while the current system shows promise, there are several limitations that need to be addressed to ensure its effectiveness, security, and broader user acceptance. Careful analysis and evaluation of these limitations will be essential to build a collaborative business model on top of blockchain and smart contract technologies successfully.

5.3 Future work

In my ongoing research, I plan to enhance the user experience model for the current framework based on the insights gathered from the user study regarding attitudes towards certificate sharing and students' desire for control over their certificates. Additionally, I aim to incorporate essential aspects such as privacy, trust, and security, and examine whether these factors influence user attitudes towards the system, subsequently affecting their intention to use it.

Furthermore, as part of future work, I intend to improve the existing certificate sharing framework by exploring the utilization of Ethereum Improvement Proposals (EIPs). This approach would enable certificates' ownership to remain non-transferable, in contrast to NFTs, while granting students the ability to create viewNFTs as copies of their original documents. Additionally, I plan to investigate the potential benefits of employing private blockchain or hybrid blockchain solutions to address security and data privacy concerns effectively.

To address the limitations highlighted in the previous section, I will work on implementing solutions that cater to a smaller-sized participant pool in usability studies. For example, this may include individuals with more background knowledge on the issue and sharing of credentials, such as graduate students who have faced challenges in this area, as well as people familiar with blockchain and NFTs. Moreover, I will strive to diversify the participant pool to ensure the generalizability of the results. This diversification will encompass individuals from various backgrounds and may involve university authorities responsible for managing existing certificate sharing systems, administrators, employers, and other relevant stakeholders. Additionally, I will aim to incorporate perspectives from these diverse groups to gain comprehensive insights into the system's usability and effectiveness.

References

- [1] Ali Alammary, Samah Alhazmi, Marwah Almasri, and Saira Gillani. Blockchain-based applications in education: A systematic review. *Applied Sciences*, 9(12), 2019.
- [2] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, and et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, volume 30, pages 1–15, 2018.
- [3] Juan Benet. Ipfs - content addressed, versioned, p2p file system. Retrieved June 13, 2023, from <https://arxiv.org/abs/1407.3561>, 2014.
- [4] Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2):157–165, 2007.
- [5] Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform. Retrieved June 13, 2023, from <https://blockchain-library.org/articles/ethereum-white-paper.pdf>, 2014.
- [6] Vitalik Buterin. On public and private blockchains. Retrieved June 13, 2023, from <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains>, 2015.
- [7] Fran Casino, Thomas K. Dasaklis, and Constantinos Patsakis. A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and Informatics*, 35(2):233–251, 2018.
- [8] Wayne Chang, Gregory Rocco, Brantly Millegan, and Nick Johnson. ERC-4361: Sign-In with Ethereum [draft]. Ethereum Improvement Proposals, October 2021.
- [9] Wynne W. Chin, Barbara L. Marcolin, and Peter R. Newsted. A partial least squares latent variable modeling approach for measuring interaction effects: Results from a monte carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, 14(2), 2003.
- [10] Wynne W. Chin, Robert A. Peterson, and Steven P. Brown. Structural equation modeling in marketing: Some practical reminders. *Journal of Marketing Theory and Practice*, 16(4):287–298, 2008.
- [11] Nancy Walters Coppola, Starr Roxanne Hiltz, and Naomi Rotter. Building trust in virtual teams. *IEEE Transactions on Professional Communication*, 47:95–104, 2001.
- [12] Fred D. Davis. A technology acceptance model for empirically testing new end-user information systems. 1986.
- [13] Fred D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13:983–1003, 1989.
- [14] Fred D. Davis, Richard P. Bagozzi, and Paul R. Warshaw. Extrinsic and intrinsic motivation to use computers in the workplace. *Journal of Applied Social Psychology*, 22(14):1111–1132, 1992.
- [15] Christian Delgado-von Eitzen, Luis E. Anido-Rifón, and Manuel J. Fernández-Iglesias. Blockchain applications in education: A systematic literature review. *Applied Sciences*, 11(24), 2021.

- [16] Catherine Dwyer, Starr Roxanne Hiltz, and Katia Passerini. Trust and privacy concern within social networking sites: a comparison of facebook and myspace. In *Association for Information Systems - 13th Americas Conference on Information Systems, AMCIS 2007: Reaching New Heights*, pages 1725–1735, 2007.
- [17] Ethereum. Proof of stake. Retrieved June 13, 2023, from <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>, 2021.
- [18] Martin Fishbein and Icek Ajzen. *Belief, attitude, intention and behavior: an introduction to theory and research*. Addison-Wesley, Reading, 1975.
- [19] General Data Protection Regulation (GDPR). Right to erasure ('right to be forgotten'). Retrieved June 13, 2023, from <https://bit.ly/2zMT9V1>, May 2018.
- [20] Joseph F. Hair, William C. Black, Barry J. Babin, and Rolph E. Anderson. *Multivariate Data Analysis*. Pearson, 2014.
- [21] Sirkka L. Jarvenpaa and Dorothy E. Leidner. Communication and trust in global virtual teams. *Journal of Computer-Mediated Communication*, 3(4):JCMC346, 06 1998.
- [22] Prakhyat Khati, Ajay Kumar Shrestha, and Julita Vassileva. Non-fungible tokens applications: A systematic mapping review of academic research. In *2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 0323–0330, 2022.
- [23] Prakhyat Khati, Ajay Kumar Shrestha, and Julita Vassileva. Student certificate sharing system using blockchain and nfts. In *Blockchain and Application 5th International Congress*, Guimaraes, Portugal, 2023.
- [24] I-Fan Liu, Meng Chang Chen, Yeali S. Sun, David Wible, and Chin-Hwa Kuo. Extending the TAM model to explore the factors that affect intention to use an online learning community. *Computers & Education*, 54(2):600–610, 2010.
- [25] Media Lab Learning Initiative. Digital certificates project. <http://certificates.media.mit.edu/>.
- [26] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Retrieved June 13, 2023, from <https://bitcoin.org/bitcoin.pdf>, 2008.
- [27] Binh Minh Nguyen, Thanh-Chung Dao, and Ba-Lam Do. Towards a blockchain-based certificate authentication system in vietnam. *PeerJ Computer Science*, 6, March 2020.
- [28] Sara Nikolić, Sasa Matić, Darko Čapko, Sran Vukmirović, and Nemanja Nedić. Development of a blockchain-based application for digital certificates in education. In *2022 30th Telecommunications Forum (TELFOR)*, pages 1–4, 2022.
- [29] Gabriele Piccoli and Blake Ives. Trust and the unintended effects of behavior control in virtual teams. *MIS Quarterly*, 27(3):365–395, 2003.
- [30] Wolfgang Prinz, Sabine Kolvenbach, and Rudolf Ruland. Blockchain for education: Lifelong learning passport. volume 2020, 2020.
- [31] Juan Carlos Roca, José Juan García, and José Juan de la Vega. The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security*, 17(2):96–113, 2009.
- [32] Alfred P. Rovai. A constructivist approach to online college learning. *The Internet and Higher Education*, 7(2):79–93, 2004.
- [33] Dong-Hee Shin. The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption. *Interacting with Computers*, 22(5):428–438, 2010.

- [34] Ajay Kumar Shrestha and Julita Vassileva. Towards decentralized data storage in general cloud platform for meta-products. In *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*, BDAW '16, New York, NY, USA, 2016. Association for Computing Machinery.
- [35] Ajay Kumar Shrestha, Julita Vassileva, Sandhya Joshi, and Jennifer Just. Augmenting the technology acceptance model with trust model for the initial adoption of a blockchain-based system. *PeerJ Computer Science*, 7:e502, 2021.
- [36] Muhamed Turkanović, Marko Hölbl, Kristjan Košič, Marjan Heričko, and Aida Kamišalić. Eductx: A blockchain-based higher education credit platform. *IEEE Access*, 6:5116–5127, 2018.
- [37] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3):425–478, 2003.
- [38] Gavin Wood. Ethereum: A secure decentralized generalized transaction ledger. Retrieved June 13, 2023, from <https://ethereum.org/whitepaper>, 2014.
- [39] Mehmet Murat Yenisey, A. Ant Ozok, and Gavriel Salvendy. Perceived security determinants in e-commerce among turkish university students. *Behaviour & Information Technology*, 24(4):259–274, 2005.
- [40] Xiongfei Zhao and Yain-Whar Si. Nftcert: Nft-based certificates with online payment gateway. In *2021 IEEE International Conference on Blockchain (Blockchain)*, pages 538–543, 2021.

Appendix A

NFT Solidity Contract

```
pragma solidity ^0.8.0;

import "hardhat/console.sol";
import "@openzeppelin/contracts/utils/Counters.sol";
import "@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";
import "@openzeppelin/contracts/token/ERC721/ERC721.sol";

contract NFTCertificateFinal is ERC721URIStorage {

    using Counters for Counters.Counter;
    // '_tokenIds' variable has the most recently minted tokenId
    Counters.Counter private _tokenIds;
    // Keeps track of the number of items sold
    Counters.Counter private _itemsSold;
    // 'owner' is the contract address that created the smart contract
    address payable owner;

    // The structure to store information about a listed token
    struct ListedToken {
        uint256 tokenId;
        address payable owner;
        address payable viewer;
        uint256 transferBackTime;
        bool currentlyListed;
        bool currentViewer;
    }

    // The structure to store time information about a listed token
    struct TokenTransferSchedule {
        uint256 transferBackTime;
        address transferBackTo;
    }

    // The event emitted when a token is successfully listed
    event TokenListedSuccess (
        uint256 indexed tokenId,
        address owner,
        address viewer,
        uint256 transferBackTime,
        bool currentlyListed,
        bool currentViewer
    );

    mapping(uint256 => ListedToken) private idToListedToken;

    mapping(uint256 => TokenTransferSchedule) private idToTransferSchedule;

    constructor() ERC721("NFTMarketplace", "NFTM") {
        owner = payable(msg.sender);
    }

    function updateListPrice(uint256 _listPrice) public payable {
        require(owner == msg.sender, "Only owner can update listing price");
        listPrice = _listPrice;
    }

    function getListPrice() public view returns (uint256) {
        return listPrice;
    }

    function getLatestIdToListedToken() public view returns (ListedToken memory) {
        uint256 currentTokenId = _tokenIds.current();
        return idToListedToken[currentTokenId];
    }

    function getListedTokenForId(uint256 tokenId)
        public view returns (ListedToken memory) {
        return idToListedToken[tokenId];
    }

    function getListedTokenTime(uint256 tokenId)
        public view returns (TokenTransferSchedule memory) {
```



```

        return idToTransferSchedule[tokenId];
    }
    function getCurrentToken() public view returns (uint256) {
        return _tokenIds.current();
    }
}

//The first time a token is created, it is listed here
function createToken(string memory tokenURI) public payable returns (uint) {
    //Increment the tokenId counter, which is keeping track of the number of minted NFTs
    _tokenIds.increment();
    uint256 newTokenId = _tokenIds.current();

    //Mint the NFT with tokenId newTokenId to the address who called createToken
    _safeMint(msg.sender, newTokenId);

    //Map the tokenId to the tokenURI (which is an IPFS URL with the NFT metadata)
    _setTokenURI(newTokenId, tokenURI);

    //Helper function to update Global variables and emit an event
    createListedToken(newTokenId);
    return newTokenId;
}

function createListedToken(uint256 tokenId) private {
    //Update the mapping of tokenId's to Token details, useful for retrieval functions
    idToListedToken[tokenId] = ListedToken(
        tokenId,
        payable(msg.sender),
        payable(msg.sender),
        0,
        true,
        false
    );

    //_transfer(msg.sender, address(this), tokenId);
    //Emit the event for successful transfer. The frontend parses this message and updates the end user
    emit TokenListedSuccess(
        tokenId,
        msg.sender,
        msg.sender,
        0,
        true,
        false
    );
}

//This will return all the NFTs currently listed to be sold on the marketplace
function getAllNFTs() public view returns (ListedToken[] memory) {
    uint nftCount = _tokenIds.current();
    ListedToken[] memory tokens = new ListedToken[](nftCount);
    uint currentIndex = 0;
    uint currentId;
    //at the moment currentlyListed is true for all, if it becomes false in the future we will
    //filter out currentlyListed == false over here
    for(uint i=0; i<nftCount; i++)
    {
        currentId = i + 1;
        ListedToken storage currentItem = idToListedToken[currentId];
        tokens[currentIndex] = currentItem;
        currentIndex += 1;
    }
    //the array 'tokens' has the list of all NFTs in the marketplace
    return tokens;
}

//Returns all the NFTs that the current user is owner or seller in
function getMyNFTs() public view returns (ListedToken[] memory) {
    uint totalItemCount = _tokenIds.current();
    uint itemCount = 0;
    uint currentIndex = 0;
    uint currentId;
    //Important to get a count of all the NFTs that belong to the user before we can make an array for them
    for(uint i=0; i < totalItemCount; i++)
    {
        // if(idToListedToken[i+1].owner == msg.sender || idToListedToken[i+1].seller == msg.sender){
        //     itemCount += 1;
        // }
        if(idToListedToken[i+1].viewer == msg.sender){
            itemCount += 1;
        }
    }
}

```

```

    }
}

//Once you have the count of relevant NFTs, create an array then store all the NFTs in it
ListedToken[] memory items = new ListedToken[](itemCount);
for(uint i=0; i < totalItemCount; i++) {
    // if(idToListedToken[i+1].owner == msg.sender || idToListedToken[i+1].seller == msg.sender) {
    //     currentId = i+1;
    //     ListedToken storage currentItem = idToListedToken[currentId];
    //     items[currentIndex] = currentItem;
    //     currentIndex += 1;
}
if(idToListedToken[i+1].viewer == msg.sender) {
    currentId = i+1;
    ListedToken storage currentItem = idToListedToken[currentId];
    items[currentIndex] = currentItem;
    currentIndex += 1;
}
}
return items;
}

//Returns all the NFTs that the current user is owner or seller in
function getTrasferedNFTs() public view returns (ListedToken[] memory) {

    uint totalItemCount = _tokenIdIds.current();
    uint itemCount = 0;
    uint currentIndex = 0;
    uint currentId;
    //Important to get a count of all the NFTs that belong to the user before we can make an array for them
    for(uint i=0; i < totalItemCount; i++)
    {
        // if(idToListedToken[i+1].owner == msg.sender || idToListedToken[i+1].seller == msg.sender){
        //     itemCount += 1;
        // }
        if(idToListedToken[i+1].owner == msg.sender && idToListedToken[i+1].currentViewer == true){
            itemCount += 1;
        }
    }

//Once you have the count of relevant NFTs, create an array then store all the NFTs in it
ListedToken[] memory items = new ListedToken[](itemCount);
for(uint i=0; i < totalItemCount; i++) {
    // if(idToListedToken[i+1].owner == msg.sender || idToListedToken[i+1].seller == msg.sender) {
    //     currentId = i+1;
    //     ListedToken storage currentItem = idToListedToken[currentId];
    //     items[currentIndex] = currentItem;
    //     currentIndex += 1;
    // }
    if(idToListedToken[i+1].owner == msg.sender && idToListedToken[i+1].currentViewer == true) {
        currentId = i+1;
        ListedToken storage currentItem = idToListedToken[currentId];
        items[currentIndex] = currentItem;
        currentIndex += 1;
    }
}
return items;
}

function executeTransfer(uint256 tokenId, address receiver, uint256 transferBackTime) public {
    require(idToListedToken[tokenId].owner == msg.sender, "Only token owner can transfer Viewer rights ");
    // lets converet the time into seconds for now.
    transferBackTime = transferBackTime+block.timestamp ;
    //update the details of the token
    idToListedToken[tokenId].currentlyListed = false;
    idToListedToken[tokenId].currentViewer = true;

    idToListedToken[tokenId].viewer = payable(receiver);
    //idToListedToken[tokenId].owner = payable(receiver);
    idToListedToken[tokenId].transferBackTime = transferBackTime;
    _itemsSold.increment();

    if (transferBackTime > 0) {
        TokenTransferSchedule storage schedule = idToTransferSchedule[tokenId];
        schedule.transferBackTime = transferBackTime;
        schedule.transferBackTo = idToListedToken[tokenId].owner;
    }
}

function transferOwnership(uint256 tokenId) public {
    require(idToListedToken[tokenId].owner == msg.sender, "Only token owner can transfer ownership back");
}

```

```
require(idToListedToken[tokenId].currentViewer == true, "You are not the owner just the viewer ");

TokenTransferSchedule storage scheduledTransfer = idToTransferSchedule[tokenId];
if (scheduledTransfer.transferBackTime > 0 && block.timestamp >= scheduledTransfer.transferBackTime) {
    //address viewer = scheduledTransfer.transferBackTo;
    //_transfer(receiver, seller, tokenId);
    idToListedToken[tokenId].currentlyListed = true;
    idToListedToken[tokenId].currentViewer = false;
    idToListedToken[tokenId].viewer = payable(msg.sender);
}
}
}
```

Appendix B

Ethics Approval



Behavioural Research Ethics Board (Beh-REB) 28-Apr-2023

Certificate of Approval

Application ID: 4046

Principal Investigator: Julita Vassileva

Department: Department of Computer Science

Locations Where Research

Activities are Conducted: 1. In research lab 2. Online, Canada

Student(s): Prakhyat Khati

Funder(s): Natural Sciences and Engineering Research Council of Canada

Sponsor: Natural Sciences and Engineering Research Council of Canada

Title: Student Certificate Sharing System Using Blockchain and NFTs

Approved On: 28-Apr-2023

Expiry Date: 28-Apr-2024

Approval Of:

- * Behavioural Ethics Application
- * Recruitment poster (updated 25-April)
- * Consent form (updated 28-April)
- * Survey questions (17-April version)

Acknowledgment Of:

- * TCPS2 CORE Tutorial Certificate: Prakhyat Khati

Review Type: Delegated Review

CERTIFICATION

The University of Saskatchewan Behavioural Research Ethics Board (Beh-REB) is constituted and operates in accordance with the current version of the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans TCPS 2 (2022). The University of Saskatchewan Beh-REB has reviewed the above-named project. The proposal was found to be acceptable on ethical grounds. The principal investigator has the responsibility for any other administrative or regulatory approvals that may pertain to this project, and for ensuring that the authorized project is carried out according to the conditions outlined in the current approved protocol. This Certificate of Approval is valid for the above time period provided there is no change in experimental protocol or consent process or documents.

ONGOING REVIEW REQUIREMENTS

Any significant changes to your proposed method, or your consent and recruitment procedures must be reported to the Chair through submission of an amendment for Beh-REB consideration in advance of implementation.


To remain in compliance, a status report (renewal of closure form) must be submitted to the Beh-REB Chair for consideration within one month prior to the current expiry date each year the project remains open, and upon project completion. Please refer to the Research Ethics Office website for further instructions and current forms.

Digitally Approved by Diane Martz
Vice-Chair, Behavioural Research Ethics Board
University of Saskatchewan

Appendix C

Recruitment Form

**Department of Computer Science
University of Saskatchewan**



PARTICIPANTS NEEDED FOR RESEARCH IN USABILITY STUDY OF NFT-BASED BLOCKCHAIN SYSTEM

“A Study to Assess the Use of Non-Fungible Tokens (NFTs)
and Smart Contracts on a Blockchain for Sharing Academic
Certificates and Credits”

As a participant in this study, you will be asked to respond to an online self-report questionnaire regarding Ease of use, System usefulness, Intension of use, Attitude, and Trust towards the system after a brief interaction with the system.

We don't require your NSID for personal identification.

Your participation would take about 60 minutes and participants will be compensated up to the University Survey Standard.

For more information about this study, or to volunteer for this study,
please contact:

Julita Vassileva (julita.vassileva@usask.ca)

Prakhyat Khati (prakhyat.khati@usask.ca)

Computer Science

**This study has been reviewed by, and received approval
through, the Research Ethics Office, University of Saskatchewan.**



Appendix D

Consent Form and Survey Questionnaire



Department of Computer Science
176 Thorvaldson Building
110 Science Place Saskatoon SK S7N 5C9 Canada
Telephone: (306) 966-4886 Facsimile: (306) 966-4884

Consent Form

Before proceeding, please read the following terms and conditions. You must give your consent to continue. Feel free to ask the researcher any questions you might have.

We would like to cordially invite you to take part in a survey that aims to discover efficient methods for evaluating a blockchain-based academic certificate-sharing framework that utilizes non-fungible tokens (NFTs). The framework is designed to be user-controlled and prioritizes privacy protection. Your experience will be evaluated through a survey questionnaire, and the researcher will be available to provide technical support in case you encounter any issues while using the system.

The survey will take place inside the computer science department in "**MADMUC-Lab, (Room-181)**" which is a confined space located within the Thorvaldsen building. Covid-19 safety measures will be enforced, including the provision of face masks, hand sanitizer, and cleaning of devices before and after use. The location will also adhere to all Covid-19 guidelines set forth by the University of Saskatchewan. For more details, please visit the website: <https://covid19.usask.ca/faculty-staff/index.php>.

The laboratory where the survey will be conducted is an enclosed area, and there are no obstacles or constraints that could compromise the confidentiality of the data collection process within that space.

The researcher will undertake to safeguard the confidentiality of participants but cannot guarantee that other members of the group will do so. Please respect the confidentiality of the other members of the group by not disclosing the identity of participants outside the group and be aware that others may not respect your confidentiality.

Title: - A Study to Assess the Use of Non-Fungible Tokens (NFTs) and Smart Contracts on a Blockchain for Sharing Academic Certificates and Credits.

Ethics Application Number: -

Student Researcher: -

Prakhyat Khati, Department of Computer Science (prakhyat.khati@usask.ca)



Department of Computer Science
176 Thorvaldson Building
110 Science Place Saskatoon SK S7N 5C9 Canada
Telephone: (306) 966-4886 Facsimile: (306) 966-4884

Researcher: -

Julita Vassileva, Department of Computer Science (julita.vassileva@usask.ca)

Purpose and Procedure of the Research: -

The aim of this study is to assess the effectiveness of an NFT - blockchain based system for academic certificate sharing by utilizing the Technology Acceptance Model with trust constructs. The study aims to gather feedback on Perceived Ease of use, Usefulness, Intention of Use, Attitude, Security, Trust, and Privacy. The research findings may contribute to the broader field of user acceptance of real-world NFT - blockchain based applications in education and data sharing. To achieve this, we will conduct a survey with validated questions.

- During the study, you will be shown a demonstration of the system and given a brief explanation of the underlying technology.
- You will also be able to interact with a prototype of the system.
- You will then be asked to complete a survey questionnaire to evaluate your experience. The entire process should take approximately 60 minutes.
- Data from the tasks and the questionnaires will be recorded.

During the interaction with the system, a student researcher will be available to assist with any technical barriers that you may encounter while using the system.

Potential Risks: -

There are no known risks in this study. No personal data is collected, and all data are stored in an anonymous format.

Potential Benefits: -

Findings from the study may provide more insight into whether an NFT-based, user-controlled privacy-preserving framework using smart contracts for sharing academic certificates is a viable solution from a user perspective (is it perceived usable and useful, also, is it trusted and generally acceptable).

Compensation: -

- In appreciation of your time, you will be paid CAD \$13 in cash.
- Participants will receive the full compensation even if they withdraw during data collection.



Department of Computer Science
176 Thorvaldson Building
110 Science Place Saskatoon SK S7N 5C9 Canada
Telephone: (306) 966-4886 Facsimile: (306) 966-4884

- Any personal information collected as a record of honorarium payment will be stored separately from the data by the PI and may be kept for 7 years in case the University of Saskatchewan is subjected to a financial audit.

Confidentiality: -

- The data collected from this study will be used in articles for publication in journals and conference proceedings.
- This survey is hosted on SurveyMonkey, a tool that is adopted for surveys by the University of Saskatchewan. The security and privacy of the information you provide is subject to the laws of the University of Saskatchewan and Canada.
- Your survey data will be stored in facilities hosted in Canada. Please see the following link for more information on the "[Survey Monkey Privacy Policy](#)."
- No personally identifiable information will be collected in this study, the data from the survey will be stored under system-generated ids.
- By participating in this survey, you acknowledge and agree that your answers and data from interaction with the system will be stored in the University of Saskatchewan secured storage and accessed only by the researchers involved in this study.
- Also, to ensure the accessibility, security and integrity of the data, all electronic data will be kept on the PI's University of Saskatchewan password-protected computer and will be backed up on a USASK server or cloud storage service, such as OneDrive or Datastore.
- The certificate and credentials used to create the NFT certificates are all demo and will not affect the participant's transcript, grades, or academic records.
- Aggregated results from this study will be used in the evaluation portion of MSc thesis.

Copies: -

If you would like to keep a copy of this consent form for your records, right-click this web page, click "Save Page As..." and follow the prompts provided by your web browser.

Storage of Data: -

- The Principal Investigator (Prof. Julita Vassileva) will oversee the storage of electronic data in the analysis and long-term storage phases.
- The Electronic data will only be accessed by the researchers during the time of analysis on a USask password-protected computer.



✦ Department of Computer Science
176 Thorvaldson Building
110 Science Place Saskatoon SK S7N 5C9 Canada
Telephone: (306) 966-4886 Facsimile: (306) 966-4884

- Electronic data will be stored on a password-protected computer during analyses and will be moved to the Principal Investigator's USask supported OneDrive for long-term storage.
- All data will be stored for 5 years post-publication, after which it will be destroyed beyond recovery.

Dissemination of Results: -

Aggregated results from this study will appear in a MSc thesis and articles published in peer-reviewed conferences and scientific journals. These may include quotes provided in the open-form questions (anonymized).

Right to Withdraw: -

- Participation in this survey is voluntary, and you may choose not to answer any questions you don't feel comfortable with.
- You can decide not to participate at any time, but it has to be before submitting the survey questionnaire.
- Survey responses will only be saved to the database once the student clicks the submit button at the end.
- If you decide to withdraw after that point, unfortunately, it won't be possible to identify your answers to delete them.
- The observation being made is solely aimed at assisting with technical difficulties and is not intended to collect any data or information.

Questions: -

- Contact the researcher(s) using the information at the top of page 1.
- This research project has been approved on ethical grounds by the University of Saskatchewan Behavioural Research Ethics Board. Any questions regarding your rights as a participant may be addressed to that committee through the Research Ethics Office: ethics.office@usask.ca; 306-966-2975; out of town participants may call toll free 1-888-966-2975.

Follow-Up or Debriefing: -



UNIVERSITY OF
SASKATCHEWAN

✦ Department of Computer Science

176 Thorvaldson Building

110 Science Place Saskatoon SK S7N 5C9 Canada

Telephone: (306) 966-4886 Facsimile: (306) 966-4884

If you are interested in the findings of this investigation, you can reach out to the researchers. The outcomes of the study will be provisionally obtainable within 2 months starting from the day the survey was conducted.

Consent to Participate: -

By completing and submitting this questionnaire, your free and informed consent is implied and indicates that you understand the above conditions of participation in this study.

Survey Questionnaire

The Survey involved a Hypothetical exercise where you will be asked to password provided during the survey and not any personal data. Additionally, all required documents such as a demo transcript and degree certificate will be provided. It's important to note that you won't be asked to disclose any personal passwords or share personal academic information. All the necessary resources will be given to you.

* 1. Please provide a random ID, you may generate a random ID on [this page](#)

* 2. Please indicate your highest education level

- Bachelors
- Masters
- PhD
- Others

* 3. I have requested academic certificate transfer between universities.

- Yes
- No

4. If "Yes" for Q.3, did you use for the academic certificate/credits transfer.

- Post / mail (paper-based)
- Electronic (sent by university via email)
- Both by email and post
- By using a certificate / credit sharing platform, such as MyCredits

* 5. I am familiar with blockchain and smart contracts.

- Strongly disagree
- Moderately disagree
- Slightly disagree
- Neither
- Slightly agree
- Moderately agree
- Strongly agree

* 6. I am familiar with the concept of NFT.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

We would like to introduce you to the benefits of incorporating blockchain, smart contracts, and NFT technologies into familiar applications, specifically the Academic Certificate/Credits Sharing System. We have prepared a video that provides a comprehensive explanation of these technologies on an abstract level. To ensure optimal viewing experience, please click on the following link to watch the video in HD quality and in full screen mode.

Summary:

The video provides an overview of key concepts related to blockchain, smart contracts, and non-fungible tokens (NFTs) in the context of student academic certificates.

Blockchain is a secure and decentralized system of digital ledgers that ensures the immutability of records by existing simultaneously on multiple computers. It acts as an unchangeable and distributed ledger. Smart contracts are self-executing contracts that define and enforce the agreed-upon terms for executing actions, such as accessing records. These contracts determine who has access to stored records and under what conditions.

NFTs, or non-fungible tokens, represent unique digital assets that serve as proof of ownership or authenticity. In our system, NFTs are used to represent student academic certificates. Each NFT has a distinct identifier, making it distinguishable from other certificates. This enables easy verification of certificate authenticity and ownership by employers, facilitating efficient hiring processes.

In our system, the metadata associated with certificates is stored on a distributed database called IPFs. Once issued to the university or an employer with restricted access, the metadata cannot be altered. This provides increased transparency and data protection, ensuring the integrity of student credentials.

Survey Questionnaire of NFTs based Academic Certificate Sharing System using blockchain.

* 7. I am familiar with blockchain and smart contracts.

- Strongly disagree
- Moderately disagree
- Slightly disagree
- Neither
- Slightly agree
- Moderately agree
- Strongly agree

* 8. I am familiar with the concept of NFT.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

After viewing the introduction video, please watch the framework demonstration video that explains how to use the system. This video will provide you with a step-by-step guide on navigating the system effectively and optimizing your experience. Additionally, before proceeding to complete the questionnaire, we highly recommend watching the demonstration video for a comprehensive understanding of the system's functionality. Remember to click on the provided video link above to access the demonstration video and ensure the best possible experience by watching it in HD quality and in full-screen mode.

Summary:

The video explains the features and benefits of the proposed NFT-based certificate sharing system for academic credentials. The system allows students to convert their certificates into NFTs, providing them with access control and ensuring the traceability of every transaction. Additionally, students can create viewNFTs, which allow them to selectively display relevant course credentials in their transcript.

The NFT-based certificate sharing system offers several advantages to students:

1. They can share their transcript and degree certificate with other institutions for graduate studies.
2. They can easily share their degree certificate with potential employers.
3. They have the ability to share specific class grades as transfer credits when transitioning to another institution.

Overall, the system enhances the flexibility and convenience of sharing academic credentials, enabling students to efficiently utilize their certificates in various scenarios.

Please answer the following questions after you have interacted with a prototype of the system. The system, which is an example of user-controlled privacy-preserving academic certificate sharing framework based on blockchain, smart contract and NFTs.

Perceived Ease of Use

* 9. Learning to operate this system is easy.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 10. I find it easy to get this system to do what I want it to do.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 11. My interaction with this system is clear and understandable.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 12. I find this system to be flexible to interact with.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 13. I feel it is easy to become skillful at using this system.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 14. I find this system easy to use.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

Perceived Usefulness

* 15. Using the system would improve performance in certificate sharing with transparency and privacy.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 16. Using this system would increase effectiveness in privacy policy formulation.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 17. Using this system would make it easier for me to set certificate sharing preferences.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 18. Using the system would increase productivity in certificate sharing with more control over privacy.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 19. I find this system useful for setting my certificate sharing preferences.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

Intention to use

* 20. I would like to use this system to set certificate sharing preferences.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 21. I would enjoy using this system when I need to use it.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 22. It is worthwhile to use this system to set certificate sharing preferences.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 23. I will use this system to decide how my data is shared.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

Perceived security

* 24. I believe appropriate processes will handle the information I provide with blockchain.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 25. I believe that the information I provide will be stored securely.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 26. I believe that only legitimate organizations/ authorize personal can view the information I provide to the blockchain-based system.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

Trust

* 27. I believe that this blockchain-based system is trustworthy.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 28. This system can be relied on to keep its promises.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 29. This system is dependable.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 30. This system has integrity.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 31. This system protects my privacy.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 32. This system secured my information.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 33. I am familiar with this system.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 34. I am confident in this system.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 35. I can trust this system.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 36. I am aware of which organization access information I provide during the use of this system.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 37. I am aware of the exact nature of the information that will be collected during the use of this system.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 38. I believe that the information I put on this system cannot be misused.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 39. I believe that the blockchain accounts that I use on this system cannot be intercepted by someone else.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 40. I believe that using the blockchain-based system would be beneficial for me.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 41. In my opinion, it would be desirable for me to use the blockchain-based system.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

* 42. It would be good for me to use the blockchain based system.

- Strongly disagree.
- Moderately disagree.
- Slightly disagree.
- Neither
- Slightly agree.
- Moderately agree.
- Strongly agree.

Comments

* 43. Do you have any other comments, questions, or concerns?