The ideal use of NFT in Metaverse - A Systematic literature review

Khalil Al-Towhi

Department of Computer
And System Sciences
Degree Project 30 HE credits
Computer and System Sciences
Degree project at the master level
Spring term 2023
Supervisor: Rahim Rahmani
Reviewer: Lars Asker

Abstract

It has become possible to say that the metaverse is a great opportunity for investment and trade, as it provides massive financial returns. The metaverse is the next evolution in social connection and the successor to the mobile internet. Non-fungible tokens represent the ownership of unique items in the metaverse and allow the creator to tokenize things like art, real estate, and collectibles. Trading NFT in the metaverse faces challenges, including security, fraud, and scams. Those challenges have negatively affected the stability of this market. “How can NFT trading in metaverse be improved?” is the main question of this thesis to overcome the challenges. The author performed a systematic literature review to survey and explore the possibility of using technologies to reach the ideal use of NFT in the metaverse. The systematic literature review will guide the researcher to gain more information to evaluate it in the research area. Furthermore, Pointing and identifying the gaps and knowledge needed between the research elements. Three main challenges are presented (identity verification, fraud, and ownership) in areas in which technologies that can provide (flexibility, reliability, accuracy, and performance) can apply. Three dominant solutions, smart contracts, oracle nodes, and blockchain are the study and analysis results to realize the research question and identified problem. The elected technologies show an ability to address challenges in different ways and thus maintain the security and effectiveness of trading operations. Also, the result section mentions other solutions not counting on the dominant solutions. Open issues which provide a ground for future research with practical implementations are also discussed.

Keywords: metaverse, scams, fraud, NFT, smart contract, oracle nodes, blockchain, systematic literature review

Synopsis

BACKGROUND: The term metaverse has become common nowadays. The largest technology companies invest in the metaverse because of its importance and promising financial returns. One of the main components of the metaverse is NFT. Trading NFT in the metaverse is a great attraction but also has noticeable challenges. This thesis examines the possibility of safe NFT user trading by finding appropriate solutions to these challenges.

PROBLEM: NFT use in the metaverse has challenges. Among these challenges are Cybersecurity, fraud, and scams. These problems are met by most NFT traders, especially those with little experience in information security. Implementing a proper solution for those challenges, NFT use in the metaverse becomes more secure.

RESEARCH QUESTION: The research question answered in this thesis is “How can NFT be used to improve its use in the metaverse?” The current solutions can be considered ineffective towards the challenges faced by the NFT users in the metaverse, and therefore this question can be considered appropriate to answer. Mainly, this thesis helps to find better ways to trade NFT safely and effectively.

METHOD: The thesis conducted a systematic literature review to examine and discover the technological landscape on how NFT will be used and improve its use in the metaverse. A survey is a strategy chosen. A systematic literature review is the research method selected. The research method is conducted by following a review protocol that shows how the literature is gathered and narrowed down to the targeted scope of articles.

RESULT: Three main challenges have been identified from the research papers obtained from the databases to answer the research questions. Three challenges cover different areas where their solutions can be applied to ensure a secure NFT trading environment in the metaverse. The results show how each challenge can be addressed in different ways and techniques.

DISCUSSION: A discussion is made to evaluate the results based on the results drawn from performing a systematic literature review. Smart Contracts and Oracle Contracts with blockchain are the mainstream solutions to NFT metaverse challenges. Practical implementations are also discussed together with open issues, validity, reliability, limitations, and future work.

Acknowledgment

I would like to acknowledge the Department of Computer and System Sciences at Stockholm University and especially Professor Rahim Rahmani for guiding and providing knowledge in the field of research and in the area of the thesis topic.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

1- SLR: Systematic literature review.

2- EVM: Ethereum Virtual Machine.

3- SLOC: Solidity compiler.

4- NFTM: Non-fungible marketplace.

5- DAC: Decentralized access control.

6- DONs: Oracle decentralized network.

7- EOA: Externally Owned Account.

8- KYC: Know Your Customer.

9- AML: Anti-Money Laundering.

10- CFT: Combating Financing of Terrorism.

11- NFT: Non-Fungible Token.

12- DeFi: Decentralized Finance.

13- ZKP: Zero-Knowledge Proof.

14- KELP: KEy-Loss Protection Logic.

15- POW: Proof Of Work.

16- KYB: Know-Your-Business.

17- dNFT: Dynamic Non-Fungible Token.

18- ZTA: Zero Trust Architecture.

19- IOT: Internet Of Things.

20- PKI: Public key infrastructure.

21- AI: Artificial Intelligence.

22- MCNN: Multiple Convolutional Neural Network.

23- PCA: Principal Component Analysis.

24- NFTM: Non-Fungible Token Marketplace.

25- POS: Proof Of Stake

1 Introduction

1.1 Background

Technology has always been a driving force behind innovation, and this is especially true today. The interest in virtual world technologies has been evident in the past years and it's increasing daily due to its importance in our world (Mathew, 2014). Recently, the metaverse became a global platform for digital content, services, and applications (*The Future of the Metaverse*, n.d.). The metaverse is the next evolution in social connection and the successor to the mobile internet. (*What Is the Metaverse?* n.d.). Information technology and the virtual world, such as metaverse and NFT, have a significant role in the economic reality that we live in today. Metaverse provides users with a unique experience combining digital and physical goods into a single ecosystem. Several companies like Microsoft (*Introducing Microsoft Mesh*, n.d.), Meta (*What Is the Metaverse?*, n.d.), and Google started enrolling in the technologies of the digital world to benefit from their market value. Products such as games, music, artwork, real estate, and domain names are considered to be NFTs (Rehman et al., 2021).

NFTs (non-fungible tokens) represent physical assets in the digital world with distinct properties like uniqueness, immutability, and non-interchangeability. These properties are difficult to exchange with other assets (Rehman et al., 2021). NFT's importance lies in creating new markets and investments. NFT aspects must be authenticated, namely who invented it, who owns it, and whether it's unique or similar to the same NFT. The trading value of NFT in the first quarter of 2022 amounted to 16,45 billion USD. It's an increase of 13.25% over the fourth quarter of 2021, amounting to 14,5 billion USD. (Our NFT Market Report Q1 2022 Is Published, 2022).

Using NFTs in the metaverse will make it easier for users to trade and change ownership of digital assets like avatars, digital land, or other virtual objects in a secure environment using users' digital wallets. Until August 2022, 245 NFT marketplaces were listed with over 1000 blockchains including 68 million digital wallets. Many metaverse platforms like decentraland, Efinit are available today and provide various services. Also, NFT platforms like OpenSea, for example, provide services like minting (Publishing NFT certificates of ownership on blockchain for trading) (*What Is Minting an NFT? How to Mint Using OpenSea*, n.d.) and advertising.

Some NFT challenges in the metaverse have been highlighted by experts and specialists in terms of cybersecurity, fraud “any deliberate act intended to deceive the victims and lead to the loss of their properties (Omair & Alturki, 2020, 1)”, and scams ”gaining personal information illegally”. In 2021, $14 billion is the total value earned by scammers. In 2020, 79% of losses were related to crypto crimes. 72% of the value of $ 3.2 billion is the rate of increase in cryptocurrency theft obtained from DeFi protocols. (Sigalos, 2022).

The challenges generated using metaverse trading platforms without controls and mechanisms limiting to fraud, theft, and scams. Moreover, many NFT's malicious pop-ups are available on social media platforms like Telegram and Discord (Tomkevičiūtė, 2023). One common challenge is that the scammer aims to access the victim's digital wallet using several types of phishing. With the key to the wallet in hand, the scammer drains it before the victim knows. As NFTs continue to grow and expand into different use cases, NFT technologies, and tools to improve NFT properties should be capable of adapting. To overcome these challenges, experts have started to create solutions that address these issues. Using tools and mechanisms that address the challenges, authentication mechanisms as an example, which in turn, leads to positive and effective results to reduce this phenomenon (Choi et al., 2022).

Many proposed solutions are used to overcome challenges, one of many using NFT records (Rehman et al., 2021, 3). Since NFT records are built based on decentralized blockchain technology and those

records are immutable, thus, they can be used, as an authenticator, to ensure information like the originality and ownership history of NFTs.

But why do we consider these solutions critical? Maybe due every NFT has its metadata, but it does not prevent the scammers from faking the NFT and using the work of other people to gain financial benefit, depending on the limited knowledge and lure of quick profit to the platform users, and this, of course, without the permission of the owner (Tambe Ebot, 2023).

The metaverse and NFT are something relatively new. There is no clear ground to control the use of digital assets(Christodoulou et al., 2022, 143). Scammers can bypass traditional methods(*The Largest NFT/Metaverse Hacks of 2021/2022*, 2022). Therefore, it's essential to use efficient methods and techniques to overcome the challenges. It becomes clear for NFT traders in the metaverse to verify the validity of trading operations and the transfer and disposition of property rights before starting any critical process.

1.2 Problem Statement

As discussed earlier, the NFT market's capitalization is around 61.8 billion USD dollars and seems to rise to 426.9 by 2027 (*Meta Market*, n.d.). NFT in the metaverse has a great impact because it contributes to circling all kinds of digital assets. However, the risk of cybersecurity, fraud, theft, scams, and deception continues because there are no mechanisms to prevent them (Rehman et al., 2021) (Christodoulou et al., 2022, 143). Regarding the scientific community and digital scientific libraries, there is a severe lack of scientific research papers for NFT use in the metaverse to suggest solutions (Ali et al., 2022, 2). It's challenging to find a solid ground for compliance in NFTs. Fraud sales are the most common technique to sell non-real NFTs through a type of NFT fraud scenario named, Sleep minting. The hacker exploits security flaws within smart contracts or publishes an NFT contract designed to assist mining operations rather than users. The user of this technology can sell the NFT using another username. This technique was used to sell 69 million unreal copies of Beeple's NFT. (Barber, 2022)

Nowadays, many platforms are available for users to trade with NFTs in the metaverse like Ertha, and Sandbox. The challenges generated by using these platforms are more critical for people with less knowledge of information security experiences. Clarifying the basis of the problems does not mean focusing on a specific category of users but taking it in general for all users to reduce this phenomenon, which is the trade and use of fake NFTs.

Therefore, the problem that this thesis addresses is the challenges arising around the use of NFTs in the metaverse in terms of cybersecurity, fraud, and scams.

With the significance and generality of the challenges, reaching technologies that address problems and challenges for each NFT that can be dealt with in metaverse, in turn, leads to achieving an extensive degree of reliability for the user and also works to reveal all the required information which can contain transaction records, ownership, etc. It clearly confirms that the person who sells this NFT is the official and correct owner and not a scammer.

1.3 Aim and research question

1.3.1 Aim

This thesis effort aims to discover the existing literature and research to assess the possibility of using NFT in a metaverse environment in a safe manner so that users can remain confident and reassured. The research identifies challenges and issues with NFT in the metaverse by investigating the metaverse with NFT research to assess if new technology could be implemented and fitted as a solution.

1.3.2 Research question

The main research question that this thesis aims to answer is:

“How can NFT trading in Metaverse be improved?”

Subsequently, two sub-research questions are further defined to guide the author in answers to the main research question:

RQ1- What are the NFT challenges in Metaverse in terms of cybersecurity, fraud, and scams?

This sub-question helps in searching for challenges of Non-fungible tokens in the metaverse.

RQ2- How can modern solutions overcome the challenges of NFT use in the metaverse in terms of cybersecurity, fraud, and scams?

This sub-question helps search for expected answers through research papers to overcome the challenges of using NFT in the metaverse.

1.3.3 Delimitation

As mentioned in the research question, this thesis aims to find appropriate solutions to the challenges of using NFT in the metaverse. Solutions to the challenges of using NFT in areas other than metaverse were proposed in scientific articles. Therefore, there is a chance to take advantage of these solutions if they can be applied to the challenges we have. Moreover, due to only one author for this thesis work, the scope of reviewing the literature is limited to 160 research-published papers.

1.3.4 Contribution

In general, This research can contribute to the knowledge base of the research field of information security. The research paper also provides valuable opinions and ideas for anyone whose experience in the field of NFT. These insights will inform the development of new paradigms to address the challenges of NFT in the metaverse. As it is clear, NFT is an emerging technology, which, in turn, shows the circulation and use of NFT did not exist in the past. Therefore, relying on the available literature is a practical method with great returns and contributes to contemporary efforts.

1.4 Related works

Through research in scientific libraries, some aspects related to the challenges that NFT faces were found, but not within the metaverse. These challenges can be classified in the same category as the challenges met in the metaverse. A current solution to challenges including (security standards for smart contracts, intellectual property rights, and fraud) is to adopt the use of zero-knowledge proof (ZKP). Other solutions are non-browser wallets including digital asset protection. These solutions are being adopted on

a small scale in the NFT communities, with the majority of Platforms providing traditional solutions. For this, effective solutions must be adopted. (Rehman et al., 2021).

A kind of recommendation Musamih et al(2022) stated that platforms dealing with NFT should be regulated in a way that minimizes scams and Cybersecurity challenges. These proposals can be applied by developers, but they need studies, in-depth knowledge, and efforts to achieve this regulation. Also, urging the application of appropriate standards and frameworks to properly monitor and manage NFT. For monitoring NFT platforms, this solution can create a privacy issue for users. To address fake and malicious assets, Verifying the unique contract address of the NFT is recommended. Another solution was suggested by Wang et al (2021) regarding NFT cybersecurity issues like spoofing. This solution recommends the official approval of the NFT smart contract and the use of a cold wallet (a type of encrypted electronic wallet that is characterized by not being connected to the Internet) to ensure the chance that the user's private key will not be leaked. Regarding tampering, Wang et al(2021) also suggested sending both the original and hash information using the blockchain due the information outside the blockchain may be manipulated. To prevent counterfeit copies which is a type of fraud, Gagliardoni (2021) suggests encouraging users to store their wallets in their personal computers rather than in central databases. This solution is currently being implemented in CryptoKitties (an NFT application on the Ethereum blockchain). Working to assert the self-sovereignty of users' data, we guarantee the assets and continued stability of the metaverse.

A new smart contract method named KELP was suggested by Foteini Valeonti et al (2021) that helps to regain access to lost cryptocurrency wallets but it has not been tested widely. These articles have been chosen because they demonstrate the capabilities of NFT in trading platforms. These potentials represent great potentials that have an impact on market economies. However, these solutions partially address the challenges that NFTs face in the digital world. The need for more research addressing the challenges of NFT in the metaverse is critical because it contributes to improving the quality and its use.

2 Extended Background

2.1 Blockchain

Blockchains can be defined as digital protocols that store record transactions in an unalterable and decentralized ledger. shared, immutable ledger through which all parties record activities and track businesses and their assets in all fields. These works or assets can be tangible or intangible things such as cars, artwork, copyrights, and trademarks. Providing opportunities for all parties to trace the assets and reducing the costs of tracking products and risks of fraud. Blockchain keeps all information available on the ledger for all users as a type of transparency. Each transaction doesn't take place in the ledger until it's confirmed by network users to ensure the security of information (*How Does Blockchain Work?* | *Stanford Online*, n.d.). Specific algorithms are used to encrypt information and put it on the block, and hash algorithms are used to impose another layer of protection. Hash codes are included in each block and refer to previous and next block information. It's almost impossible to change the information in any specific block to hackers. The reason for this is that each block is linked as a chain of the previous and subsequent blocks, and any change to any specific block leads, in turn, to change in the information of the previous, and subsequent block as well(*How Does Blockchain Work?* | *Stanford Online*, n.d.).

There are two types of blockchain: public and private. If we talk about the public: any user can use it like Bitcoin. Since everyone can participate, the data amount is huge, and processing this data requires great effort. The privacy of the information is relatively low. In terms of performance: relying on POW protocols that use competitive tools to confirm transactions, these protocols are very power consuming and inefficient. Bitcoin can process seven data transfers per second. On average, users must wait 10 minutes to ensure the information is written to the block. Conversely, POS protocols use random tools to confirm transactions and form new blocks (*How Does Blockchain Work?* | *Stanford Online*, n.d.).

As for the private blockchain, this type is managed by private companies or institutions that allow specific users to use this block based on Know-Your-Business (KYB) and Know-Your-Customer (KYC). One of the advantages of this type is per to per technique, the operator can maintain data security in a better way by using firewall applications as an example. (*What Is Blockchain Technology? - IBM Blockchain*, n.d.).

In general, one of the risks facing our society is the misuse of decentralized feature of blockchain and the automatic execution of smart contracts(a program stored on the blockchain and is run when certain pre-conditions are met without wasting time and is available to all users.), which in turn can be exploited for money laundering and extortion. Each country has a different vision of decentralization in blockchain, and there is no specific view agreed upon by all countries in this field. Focusing on efficiency and regulation is a major aspect of blockchain and needs more research. (Deng et al., 2022).

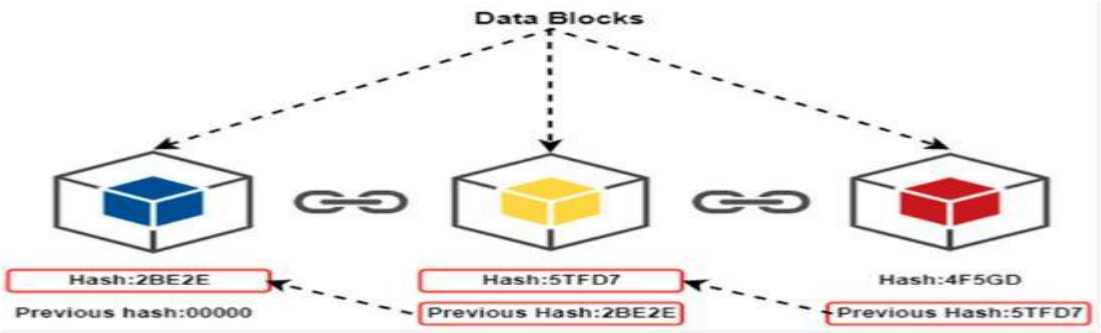

figure 1: Blockchain (Kitsantas, 2022)

2.2 Metaverse

If we look at the word metaverse, it's made up of two basic words: meta, which means in Greek “transcendence,” and verse, which means “the universe.” The term was first used in 1992 by American science fiction writer Neil Stevenson. This term refers to the possibility of using three-dimensional objects in a virtual reality that is appropriate and compatible with real reality. (Smart et al., 2007).

Four types of metaverses are described by Han et al (2021) as follows: mirror reality, augmented reality, lifelogging, and virtual reality. We can discuss each:

A- augmented reality: The meaning referred to by augmented reality indicates that this technology can add new functions and services that can be used and realized in the current reality. In addition, it works to build a smart environment using technologies that operate using locations like Pokémon Go and textbooks.

B- Lifelogging: an augmented reality image of the inner world. Let’s imagine a person who uses his smart devices to access many applications like Facebook, Snapchat, Instagram, and Twitter to follow his content on the Internet daily. This is lifelogging. Moreover, another example of ‘if we skip the security issue’ some devices have sensors that record information to be used in all fields, especially the medical ones(Han et al., 2021).

C- Mirror reality: There is the possibility of reproducing all the activities of reality to the virtual world when transferring these activities using technologies that have been developed, such as smart applications, and adding some improvements, which leads to a virtual world with a more comfortable environment. An example of this reality is the Google Earth application and the Airbnb application for real estate rental(Han et al., 2021).

D- virtual reality: Virtual reality is a new world that has nothing to do with the reality in which we live, and it represents a kind of idea that was imagined to achieve a certain idea. All characters in the virtual world have forms that represent them in a fictional environment and can communicate with each other as well as access the virtual world at the same time. Using NFT is the most significant feature. Big tech companies are now starting to invest in the metaverse to control this world which has promising financial returns. Roblox, Zepeto as an example(Han et al., 2021).

Metaverse attracts users due to its providing many services and advantages including effectiveness and accuracy of training and experimentation, collaboration and co-creation, and more accurate description of physical objects in the virtual world.

Metaverse proponents argue that the metaverse will be able to change many concepts in the near and foreseeable time and in all aspects in which we live (Hughes, 2022). Likewise, all economic, cultural, and social activities will soon move to take their place in the metaverse. Thus, the metaverse will become the most comprehensive virtual world for all users. With all this, the percentage of challenges and risks will increase, and determinants and regulations must be put in place to regulate its use.

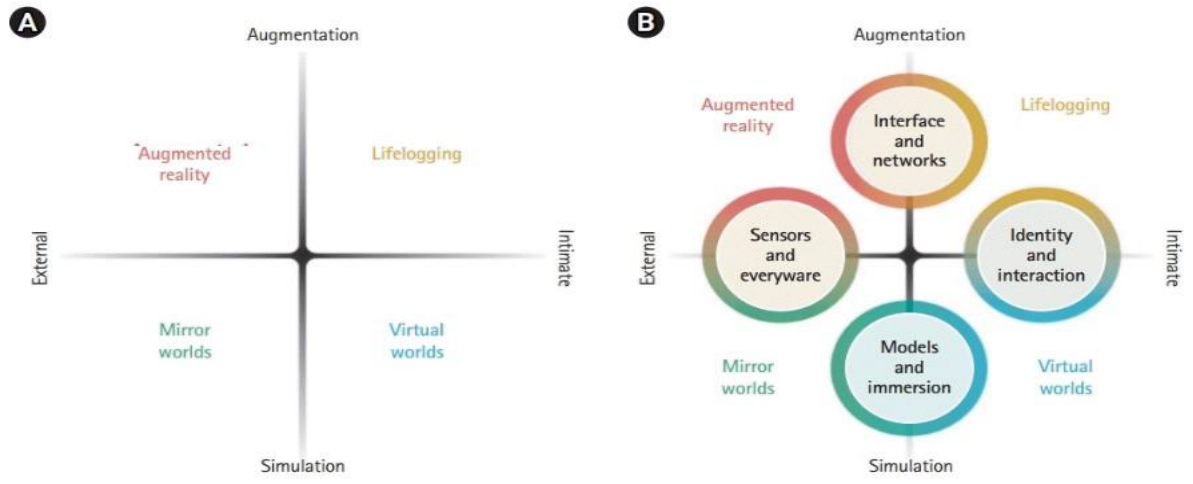

Figure 2: Metaverse (Han et al., 2021)

2.3 NFT (NON-FUNGIBLE TOKEN)

A general definition: NFT is a type of digital asset in the virtual world through which the user can own artwork or any other kind of work and has the right to buy and sell it with all related rights (Valeonti et al., 2021). An NFT can be represented as music, artwork, domain names, cartoon characters, or real life with original records of their respective owners. When NFT transactions take place in the virtual world, NFT records must include smart contracts. Generally, most of the NFTs are generated using the Ethereum blockchain. As mentioned in 1.1-second block, NFT has unique features that distinguish it from other NFTs and provide ownership rights and other services for the owner. In 2017, the first NFT was introduced on the Ethereum ERC-721. Smart contracts are included in the Ethereum Block to enhance the transparency of the information. Smart contracts are small programs that are spread over the block and include the buying and selling terms of each NFT. When it is agreed to trade, these programs are activated automatically and without the intervention of users (Kumar Mohanta et al.,2018). The information which is merged in the smart contract is tamper-proof. In virtual reality, cryptocurrency is

traded and has properties. One of the most important characteristics of digital currencies is the ability to exchange them for a similar currency. For NFT, one of its advantages is that it must be unique, distinguishable from anything else, and verifiable. (Valeonti et al., 2021).

Some of the challenges facing NFT:

1- Intellectual Property Right: It is critical to emphasize ownership rights when buying and selling NFTs. Some conditions in the smart contract sales guarantee the buyer the right to use NFT only. As well as resale rights and percentages for each transaction to the previous owner.

2- Cyber Security: With the increase in the number of NFT transactions, the phenomenon of counterfeit NFT has become increasingly noticeable. scammers can use NFT they do not own as bait to sell it on trading platforms and get financial benefits. This is due to the lack of security and information awareness among users.

3- Security and privacy: Security and privacy remain a concern for every new technology. When trading NFT in platforms, every transaction is recorded and added to the Ethereum Block. This information shall be available to all users to view and confirm that it is correct. This ledger ensures that the x-identities used for NFT owners are hidden, but if these x-identities are compared with what is used in Web 3, this can lead to revealing the real identities of NFT owners.

4- Environmental Impact: The increasing use of NFT, in turn, leads to severe damage to the environment. When an NFT transaction is made, a process called minting is created. It is a process to create NFT and add it to the blockchain. This process requires a lot of energy and computing capabilities. 44.94 terawatt-hours of electricity per year is the amount that Ethereum needs, which is roughly equivalent to the annual energy consumption of countries like Qatar and Hungary (Popescu, 2021).

2.4 Ethereum

Ethereum is a type of blockchain that depends mainly on decentralization in its work. Its idea was formed by Vitalik Buterin in 2014. The Ethereum idea came to put some required improvements to Bitcoin script languages including all kinds of computations, loops, and improvements to the structure of the blockchain. As a kind of improvement to Ethereum, any user, in the abstract layer, can add their conditional text to guarantee ownership rights or sales transactions by using smart contracts that are automatically executed when requirements are met without any intervention by users. Using SOLC smart contract processor to compile the smart contract code to EVM bytecode, Then the smart contract is created by a single transaction process (Deng et al., 2022). Ethereum platforms enable many apps to be built and deployed in a decentralized manner with the ability to add smart contracts. The main driver of the Ethereum platform is the Ether currency. It is considered one of the cryptocurrencies on this platform. Ether can be used in NFT trading operations and sending money to parties to benefit from certain operations. EOA and the contract accounts are included in Ethereum. The EOA can be controlled by a private key while the contract account is controlled by the code (Rehman et al., 2021).

3 Methodology

Since the primary studies presented an effort in the field of research, secondary studies must follow developments in the same field of research to gain more knowledge and information. In the field of computer science, it has become common to use two types of secondary studies, namely, the observation method and SLR (Vakkalanka & Kuzniarz, 2015). Despite the advantages and disadvantages of each method stated in 3.3 and 3.4, the author chose the proper one(systematic literature review) to achieve the thesis goals.

3.1 Research Strategy

The results obtained from the research project will be accurate if a proper strategy is adopted. Different research strategies are generally considered appropriate to achieve specific research goals. Depending on the type of research strategy, an appropriate and compatible research method must be chosen. The research method is defined as a data collection mechanism such as interviews, questionnaires, observations, and documents. With that, no basic rule stipulates choosing a specific research method based on a specific strategy. A survey is chosen as a research strategy in this thesis to collect data from documents based on the Systematic Literature Review. This strategy helps to take advantage of all the information and knowledge available in this field (Denscombe, 2010). Furthermore, the availability of real experimental data and credibility of the extracted information depended on the empirical research that the survey strategy provided with a snapshot to better understand the research area and provide a basis for this thesis with debriefing on how information technology is used in this field. (Denscombe, 2010).

3.2 Alternative research strategy

The case study provides a large amount of basic knowledge of a specific situation represented by a complex situation and subtle properties. It provides a comprehensive view of the subject being researched with a description of all its parts and how they interact with each other. The results are generalized to similar cases. These are, in short, the properties of the case study that were chosen as an alternative strategy for the search strategy.

Since the main research question is an NFT with a metaverse question, it's difficult to apply the case study approach here. The difficulty comes with validating the similarities or differences to other technologies and this was pointed out by (Denscombe, 2010). Moreover, The solutions to the NFT challenges in the metaverse are of high value and are kept by the developer companies as a form of superiority and are not disclosed. The difficulty in accessing the needed solutions was mentioned (Denscombe, 2010). Many more search strategies like interviews, observation, and questionnaires can be listed, but a case study has been taken as an example.

3.3 Research Method

A systematic literature review or systematic review is a form of secondary study. It is a tool for research, evaluation, and interpretation of all relevant research in one field such as a research question, a specific phenomenon, or a specific idea in a fair way based on a specific strategy. A systematic review researcher must make a his-her offer to show research that supports/does not support research hypotheses. Many reasons are considered for taking a systematic review:

1- Identifying gaps or deficiencies in any research topic to focus on providing more efforts to fill the void. In addition, the results drawn are less biased(Kitchenham, 2007).

2- Formation of a new framework or a solid scientific research background to carry out the desired research activities.

3- Work on summarizing the proofs of technical phenomena, such as summarizing the benefits and harms of specific agile methods. It can be used to examine the extent of empirical evidence for and against theoretical hypotheses. (Kitchenham, 2007).

As a disadvantage of SRL, the selected articles, and their credibility are a kind of cons to the chosen method. Any researcher can critique research papers concerning publication date, materials, and publisher reputation. Numerous interpretations can influence what researchers think.

A systematic literature review has been chosen for this thesis to gather, analyze and evaluate information about the metaverse, Non-fungible tokens, challenges, and solutions. Moreover, it will guide the researcher to gain more information to evaluate it in the research area. Pointing and identifying the gaps and knowledge needed between the research elements. The guideline presented by Kitchenham (2007) will be followed to conduct the research protocol in this thesis.

3.4 Alternative research method

It's possible to choose the observation method as an alternative type to the primary method. In computer science, observation is closely observing the contents and how information flows and is exchanged. Since this information is not available as we mentioned earlier because it is a kind of scientific superiority, it is not appropriate to choose this method.

3.5 Sampling

Since this thesis is a single author's effort,160 scientific articles will be collected from digital scientific libraries using keywords related to the research topic. After that, these articles will be reviewed and filtered iteratively using the developed protocol to choose what is appropriate for the research topic. When the scientific saturation reaches the required level, no need to read more articles, and will continue to the data analysis stage.

3.6 Research ethics

The Nuremberg Code 1947-1949 and the "Helsinki" declaration 1964, the research ethics were extracted. Research ethics is one of the basic parts of scientific research. These determinants provide for the existence of justified limits to the acquisition of knowledge. This applies to computer science. To conduct scientific research Denscombe (2010) identifies four areas that the researcher needs to consider which are:

1- The privacy of the subscriber's interests.

2- Participants provide consent to the use of the information provided by them.

3- Providing the correct information in the search and emphasizing integrity.

4- Compatibility of scientific research with the laws of the country.

As a commitment to the laws in the country, the researcher submits the references fully in the manner of APA-7th ED. Transparency and integrity in research will be discussed in the next section. There is no need to pay attention to the points related to the participants because they do not exist. (Denscombe, 2010).

3.7 Applied method

The goal of this research is to gather sufficient knowledge about metaverse and NFT, their challenges, and solutions. This knowledge allows the author to answer the challenges driven by the main question

“How can NFT trading in the metaverse be improved ?” and two sub-questions for this thesis

“What are the NFT challenges in the metaverse in terms of cybersecurity, fraud, and scams?” and

“Can modern solutions overcome the challenges of NFT use in terms of cybersecurity, fraud, and scams?”.

Looking at the research papers collected from the databases, NFT in the metaverse has many challenges with negative impacts. After reading the collected papers thoroughly, three critical challenges were elected in this field, these challenges are:

3.7.1 Challenge 1: Identity Verification

Identity verification is a fundamental and critical aspect of virtual reality. It plays an effective and essential role in today's digital world and comes with the confidence of using NFT in the metaverse. This aspect includes the possibility of the NFT trader in the metaverse identifying the contract address of the collection (Olade et al., 2022). This identification facilitates secure NFT trading and reduces scams. Generally, most internet users don't have their own digital identity, but they rely heavily on authentication through well-known companies such as Facebook and Google. However, having a digital identity for a specific platform doesn't help authenticate users from the rest of the existing platforms. For that, this identity must be unique.

On NFT platforms, the NFT is uploaded and traded. NFT verification is not required like the person who created the NFT. This allows scammers to copy real NFT and re-trade it as real NFT. Part of the data related to NFT is not stored in the blockchain. A link is provided to locate this information. If scammers access this link, there is a high possibility of fraud (Aulia Mochram et al., 2022).

3.7.2 Challenge 2: Fraud

Due to the modernity of the metaverse and its components, it doesn't have many controls and regulations. Therefore, it has become an opportunity for hackers and scammers to defraud users. This unregulated nature ideally allows scammers to use metaverse platforms to trade fake NFTs. For example, 80% of the items deleted in the OpenSea platform are works of pilgrims and spam created (Aulia Mochram et al., 2022). Moreover, bad actors can mint the same NFT in multiple blockchains (Wang et al., 2022, 22).

3.7.3 Challenge 3: Ownership

In the real world, anyone can prove their identity when trading commodities. However, in the digital world, this is not the case. Proving user identity or the ownership rights of any digital assets is critical to complete the trading process safely and correctly. The mechanisms used to prove the ownership of digital assets or the identity of users don't cope with the widespread use of NFT in the metaverse (Wang et al., 2022). The identities of some people can be forged without repercussions. Therefore, scammers take advantage of this gap to promote fake NFTs and digital properties.

3.8 Systematic Literature Review Protocol

To objectively answer all the research questions, the thesis will follow the below steps iteratively to collect, screen, analyze and evaluate the research papers on metaverse, Non-fungible tokens, Challenges, and Solutions (Kitchenham, 2010).

3.8.1 Digital databases

These academic digital databases will be the main source for searching relevant research papers:

A. IEEE Xplore

B. ACM digital library

C. ScienceDirect

D. Google Scholar

3.8.2 Search strings

Keyword search strings to be used on the digital databases are:

A. Metaverse AND NFT AND challenges / IEEE Xplore

B. Challenges AND Solutions AND Metaverse AND NFT / ACM digital library

C. Metaverse AND NFT AND challenges AND solutions / ScienceDirect

D. Solutions AND Non-fungible token AND Metaverse AND challenges / Google Scholar

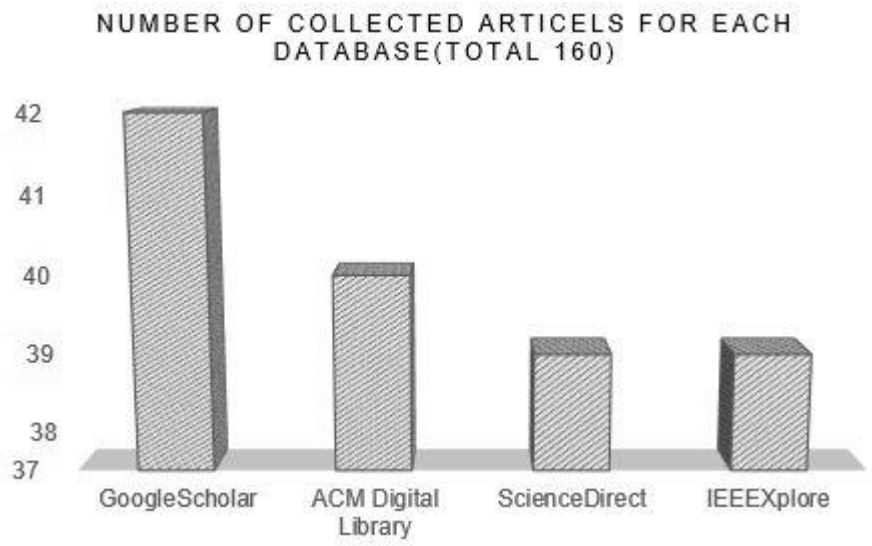

Figure 3: Data collection summary

Digital library	year	keyword	Search filed	N.article related
IEEE Xplore	2018-2023	Metaverse AND NFT AND Challenges	Anywhere	n=39
ACM Digital Library	2018-2023	Challenges AND Solutions AND Metaverse AND NFT	Anywhere	n=40
ScienceDirect	2018-2023	Metaverse AND NFT AND Challenges AND Solutions	Anywhere	n=39
GoogleScholar	2018-2023	Solutions AND Non-Fungible Tokens AND Metaverse AND Challenges	Anywhere	n=42

Table 1: Data collection keyword, research filed

3.8.3 Screening process

After collecting research articles from digital databases, it is necessary to examine them. The reason for that is these articles may be outside the research field of the research topic. The search protocol, including the inclusion and exclusion criteria applied to the articles, was relied upon repetitively.

3.8.4 Inclusion Criteria for Analysis

Inclusion criteria are the first essential part of the screening process. The desired or previously found elements will be the basis for answering the research question. The aspects of Inclusion Criteria are found below

A- The year of publication has to be between 2018 to 2023.

B- Only the English language is used.

3.8.5 Exclusion criteria for analysis:

The second essential part of the screening process to form the basis for answering the research question is the Exclusion criteria. This process ensures that the search is narrowed down to research articles that will fit the answer to the research question.

A. Papers are not academic research papers.

B. Papers is a duplicate research paper.

C. Content is partially about metaverse, Non-fungible tokens, challenges, and solutions.

D. Content is mainly about the financial, educational, healthcare, and marketing aspects of the metaverse, NFT

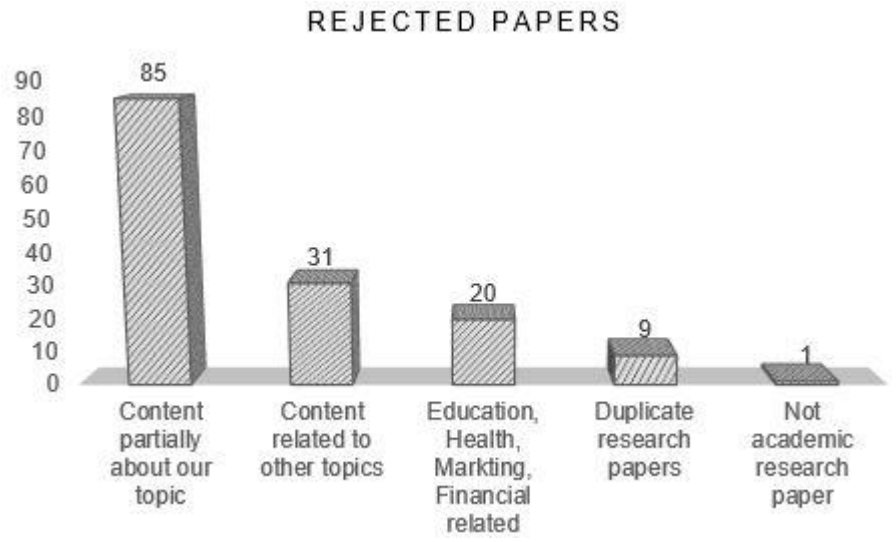

Figure 4: Data rejected summary

3.8.6 Categorization of research papers

After reading the eligible relevant research papers, categories emerged to help answer the challenges driven by the research question. The categories are presented in Figure 5 below. The numbers represent how many times each category was mentioned in the papers regarding the challenge. Each technique in the category is explained further in the result section.

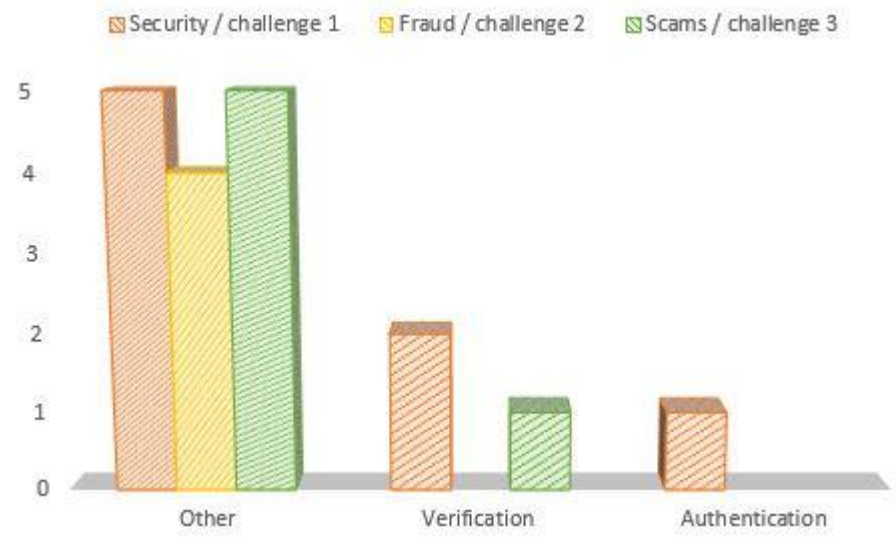

Figure 5: Categories of research papers

3.8.7 Conducting data collection

Using the digital databases provided in the protocol, the candidate research articles were collected using the specified search strings. After collecting 160 research articles from digital databases, the process of filtering began. As a first step, non-academic research articles that cannot be relied upon for solid information were excluded. After that, the duplicate articles that had been extracted from digital databases were excluded. After reading the title, abstract, and introduction and focusing on the conclusion, the research articles that partially mentioned and related to both metaverse and NFT and the challenges and solutions they faced were excluded. These articles cannot provide valuable information in this regard. Next step, the same exclusion processes are applied to research data that are concerned as financial, educational, marketing, and healthcare. These research articles do not fit with our thesis.

There is a focus in the scientific community on the metaverse and its basic pillars and a lack of articles on NFT immunization in the metaverse. Emphasis has been placed on abstracts and conclusions because titles of research articles are no longer scientifically sorted into the type of information required. Figure **5** below shows the process of obtaining articles from databases and the iterative screening of the articles for relevant data to answer the research question. more detailed information can be found in Appendix A.

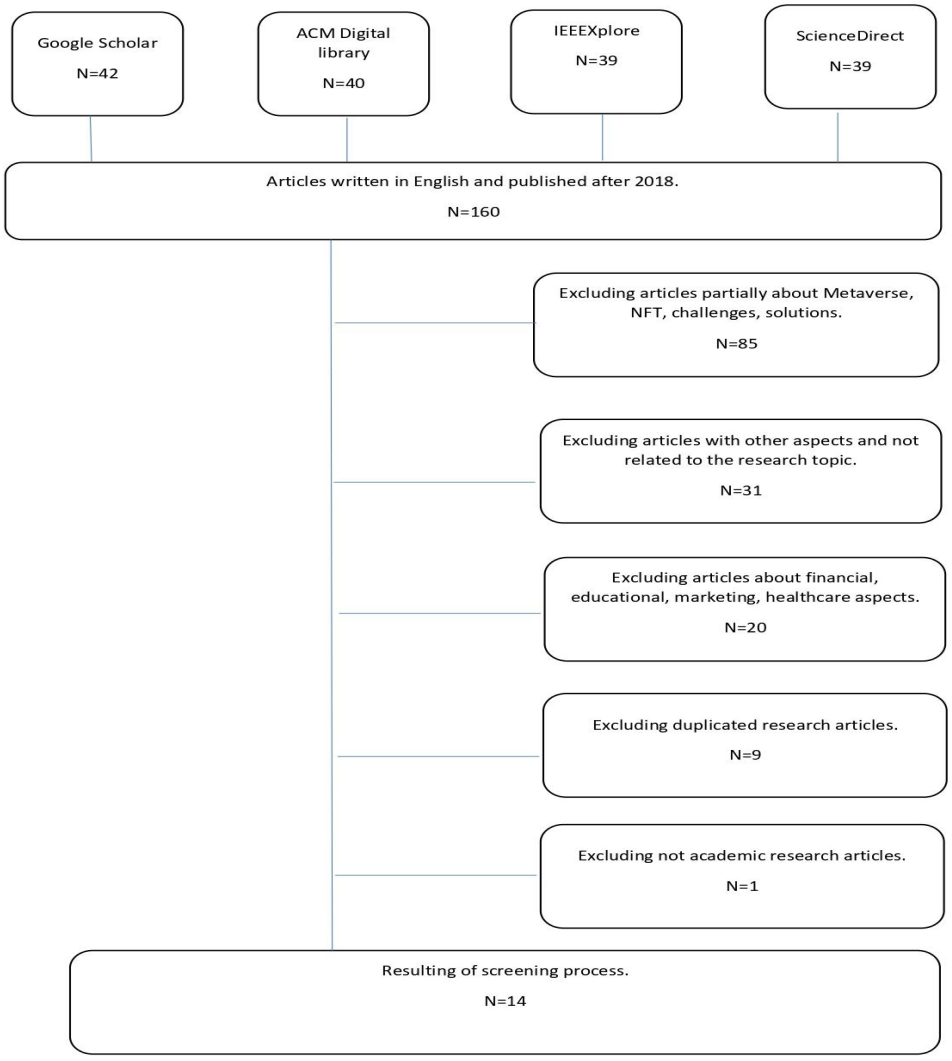

Figure 6: Exclusion / Inclusion Process

4 Result and analysis

4.1 Challenge 1: Identity Verification

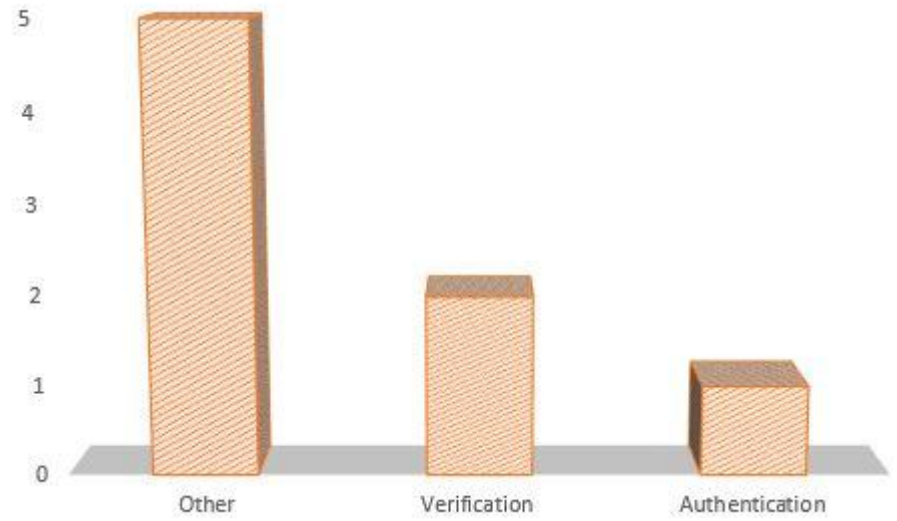

Figure 7: Security / Challenge 1

Regarding the security challenges, eight solutions were found in the analyzed papers. These solutions will provide NFT validation, authentication, and verification & facilitate user identity verification.

Christodoulou et al (2022) mentioned a type of solution which is the digital fingerprint. This solution intends to indicate how to identify and fully validate the authentication of each NFT. In most cases, any physical object is digitized and later saved through P2P(peer-to-peer) storage networks. At the same time, the digital fingerprint is generated using hashing algorithms(ex, SHA256 which are functions that enter data of arbitrary length and whose results are always of fixed length. One of its advantages is that its results are unexpected, collision-resistant, and one-way direction) to form a digital representation of it. After that, it's pushed to blockchain in several ways, including, for example, smart contracts or on the block by operation code that identify which basic computer operation in the instruction set is to be executed. To verify the authenticity of the digital representation of the NFT, calculating the given NFT hashing value and comparing it to the same hash value stored on the blockchain is required. The value is calculated using one-way Hash functions named(AKA message digests).

Cao et al (2022) propose a decentralized NFT anti-theft mechanism called TokenPatronus that provides strong protection for holders and thus facilitates the verification of their identities. This mechanism is managed through the smart contract and Oracle node layers. It has three stages described below, pre-event, in-event, and post-event replevin:

Pre-event shows the status of the token. Usually, it's unlocked with a function provided to lock it. This is achieved via the decentralized access control (DAC) module. Changing the status of the token requires an additional wallet signature.

In-event contains a risk control engine based on an Oracle node to block potentially stolen NFT transactions. The output for this engine is three transaction statuses: safe(no action), may be lost(suspicious transaction, freeze NFT transaction for a while), and hacked(locked and transferred to the treasury, ability to recover by genuine owner via decentralized arbitration system).

Post-event contains a decentralized arbitration system to handle NFTs stolen by hackers. The users can report incidents. Later the system will make further decisions.

Descriptors are used in the computer world to describe the visual attributes and features of algorithms, images, and videos (Vassou et al., 2017). This type of solution is suggested by Christodoulou et al (2022) Utilizing these visual descriptors. Descriptors will give a unique identification scheme that uses all features that verify the authenticity of each NFT individually. In the case of using smart devices (virtual reality glasses) and visual descriptors to verify some visual information, This will enable the verification algorithm to determine the appropriate features for verification and what the algorithm needs to do, like rotating or reducing light sensitivity.

Hosseini Bamakan & Solouki (2022) suggested dNFTs as a solution. A type of NFT with unique smart contract features that changes the metadata of the NFT if certain conditions are met. Off-chain oracle nodes are relied upon to update the information and then compare the old and new information in case of any tampering with the information. DNFT guarantees the decentralized nature, transparent environment, authentication, and verifiability of all these features. DNFT also ensures greater efficacy of these features and the possibility of using them more outside the scope of traditional collection and handling. This openness has a huge impact on technology markets in all fields. The dependency of the Oracle node network offers the ability to provide such features.

Gupta et al (2023) proposed Zero Trust Architecture (ZTA) which is based on “Don’t trust, verify “.This model includes user/entity verification which makes it different from other models. It’s a multi-party decentralized security model more suited for open collaborative environments. This model is based on predefined & contentious verification of users who want to access the metaverse. Moreover, a continuous authentication and verification for users with fine-grained access control, and data validation with traffic logs through blockchain and Oracle decentralized networks DONs which are effective data validation frameworks enabling credible off-chain data to be used as part of on-chain data within the metaverse (Ott, 2009). As a result, verified and authenticated identities, users full control of their privacy, pre-defined rules and regulations, user interaction monitoring, and user removal in case of violation can be achieved.

Wang et al (2022) mentioned a cloud-based mutual authentication(one-time authentication) model for wearable medical devices that have been presented by Srinivas et al (2020) to prevent device impersonation in healthcare monitoring systems with a password change and smart card revocation functions. Counting on identity verification and security analysis boosts the session key's security vs active and passive attacks. However, this model may cause friction such as unauthorized privileges. To resolve this issue, Zhao et al (2020) propose a continuous authentication model to support seamless device authentication. Results show high accuracy with 90.73%.

Wang et al (2022) also mentioned that Shen et al (2020) proposed a decentralized, dispersed cross-domain blockchain scheme for IOT devices named XAuth using a PKI system based on ZNP(zero-knowledge proof). Leveraging blockchain consensus Shen et al (2020) bypass issues with recognizing identities that are involved in extremely complex cross-domain authentication. It improves the response speed arising from the low throughput of blockchains as well as user protection.

In terms of spoofing and tampering issues, Ali et al (2022) recommended using cold wallets to prevent private-key leakage and share both hash and original data to compare with. Therefore, it facilitates user identification.

4.2 Challenge 2: Fraud

Figure 8: Fraud / Challenge 2

Regarding the fraud challenges, four solutions were found in the analyzed papers. These solutions will provide user validity, reliability, fraud reduction & detection, and NFT user accuracy.

Smaili & de Rancourt-Raymond (2022) suggests that digital footprints can be tracked to reveal the identity of the avatar users in the real world and especially in the social metaverse due users can't change the virtual properties of the constructed virtual world. The steps mentioned below are suggested by Smaili & de Rancourt-Raymond (2022) to prevent and mitigate various risks related to metaverse and fraud:

1. Strict regulations of the metaverse ecosystem including crypto exchange, NFT, and blockchain. New metaverse establishment acts to encompass transactions/actions. Additionally, requirements for platform owners to create certain rules for preventing slippage and ensuring minimum safety for users. An adequate program should be considered to mitigate and respond to metaverse risks. The way of mitigating metaverse risks, resources used, and methods to protect identity should be mentioned.
2. Assistance metaverse users in case of fraud which include a deactivating avatar, leaving the metaverse, and deleting any information related to the metaverse.
3. Involving insurance companies in the metaverse to serve users.
4. Create global authority with the help of internal/external, and public/private cooperation to oversee and control the metaverse and prevent malicious use.
5. Adoption of a comprehensive approach within different parties to peek and identify the weaknesses and combat fraud, and scams using AI.

Hosseini Bamakan & Solouki (2022) mentioned the dynamic NFT(dNFT) with Time Stamped as a solution. Timestamped is a mechanism that works with the ability to digitally record the date and time of the event and store it on the blockchain. The reason to choose dNFTs to address fraud challenges is that dNFTs are secure NFTs and ownership information can also be securely identified in the public ledger. dNFT guarantees property rights based on smart contracts. It also safeguards sensitive information. The timestamp proves the validity of the information used and confirms its reliability and that it is not a fraud.

In all fields, especially education, and real estate Khan et al (2023) mentioned that relying on dynamic NFT will reduce fraud and contribute appropriate ways to show the person's experience in all respects.

Moreover, the use of dNFTs has a significant impact on this market regarding facilitating the transfer of ownership and smart payment features.

Leppla et al (2022) propose a distinct method for time series classification using a Multiple Convolutional Neural Network (MCNN). The aim is to find a more generalized NFT fraud detection tool that combines many known features identified in old research. Those features will be enhanced by the MCNN model via extracting more features over varying time scales and windows. Black and white lists from the AtomicHub marketplace will be used to enable supervised learning. Then, PCA and K-means time series methods are utilized to reduce feature space dimension and data classifying and clustering of the black-and-white lists. The model shows the ability to detect fraudulent patterns in buyer-seller network transactions. This model brings more reliability and accuracy for NFT users.

4.3 Challenge 3: Ownership

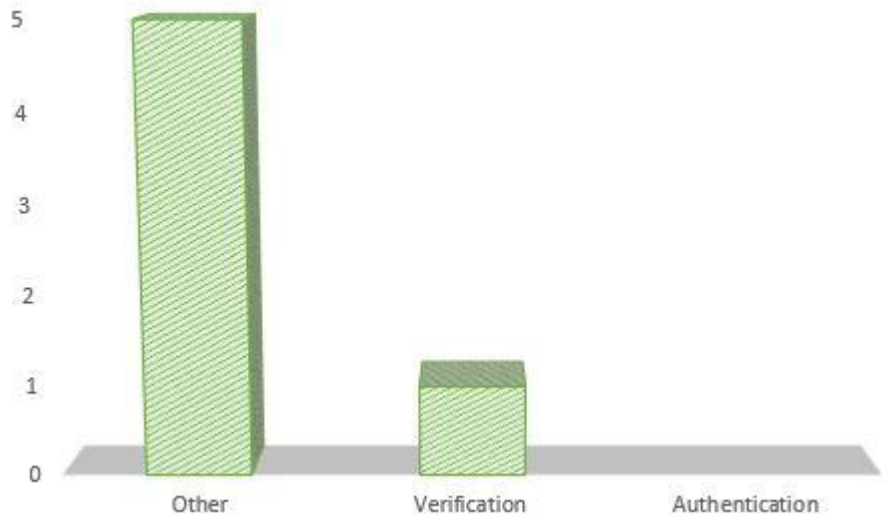

Figure 9: Scams / Challenge 3

Regarding the scam's challenges, six solutions were found in the analyzed papers. These solutions will provide user confidence and verification, NFT authenticity.

Hosseini Bamakan & Solouki (2022) introduced dynamic non-fungible tokens (dNFTs) as a new type of NFTs to address the scam challenges represented by ownership. dNFTs are promising experiments and paradigm shifts in the ownership of digital assets. Utilizing blockchain technology with dNFT results in the possibility of confirming the authenticity of a dNFT in multiple forms with ownership confirmation at the same time. Some of the NFT constants are fixed like token identifiers, a smart contract address located where the NFT is stored on the blockchain. These constants represent the value of NFT. However, to try to change the metadata that represents assets or events in the real world, we must change the dNFT metadata. There is the possibility to modify and change this metadata with the help of smart contracts by responding to specific conditions using Oracle nodes. Oracle nodes, which are data feeds belonging to a third party. These nodes act as an intermediary between off-chain or on-chain data sources. These nodes fetch and validate data for Web3 smart contracts including dNFT contracts. In general, smart contracts are created on a specific blockchain. These contracts can interact with the blockchain's ledger to retrieve the requested information. No information can be retrieved or altered outside the scope of the same blockchain. Using off-chain or computing services that Oracle provides to users and based on values previously determined by the Smart contracts, the information is updated in dNFT. Therefore, a blockchain's oracles must have accurate data at all times. Thus, the authenticity can be confirmed and

verified using dNFT and its legal sources. The possibility of updating data by Oracle in a continuous, independent, and decentralized manner. It doesn't require any intervention from the user.

Rug pull is a scam in which an NFT developer inflates a project to attract investors and then disappears with their money. Šljukić (2022) proposes an NFT Rug pull tool to register NFT projects in a specific database. This will enhance the level of confidence for both owners and investors and prove that the project is not fake. This is achieved by including records of projects in a database with information about owners, team members, and their verifications and keeping it up to date. All of this is to make the investors more confident about the reliability and legitimacy of the project and its owners. This step is critical to project owners due to it will make their project more attractive to investors.

As a team member of the NFTRug, and after the relationship that investors can build with the project's owners, investors can have a closer look at the project management process and get access to the extended information which is not available to the public. Using a web interface is a way of changing the information between the parties which includes NFT assets that exist, activity analyzing of communities around the project, and personal information collected for the project in the past. The NFTRug will inform the parties if irregularities appear during the monitoring process. Moreover, to give more strength and legitimacy, video meetings for project parties can be managed with project fact verification via machine learning tools. Finally, use a verification badge to prove that the project is being verified.

Das et al (2022) mentioned that no NFTM has made any steps toward enforcing KYC (Know Your Customer) rules nor implemented AML/CFT (Anti-Money Laundering - Combating the Financing of Terrorism) measures. This led to " How can token contracts be verified ? ". NFT authentication is critical for all users and it relies on the smart contract being managed. Therefore, NFTM recommended buyers verify the address collection from official sources, e.g. project web page, and avoid using known collection names with special characters.

Bhujel & Rahulamathavan (2022) recommend that all users identify the red flag of the project before investing to avoid scams and rug pulls. Moreover, using NFT Explorer to analyze the purchases and merits associated with wallet ID.

Battah et al (2022) propose an AI model based on blockchain and non-fungible tokens by employing the smart contract to enforce ownership and easy access. After that, a proxy re-encryption Oracle is used to securely store, fetch, and share the data related.

5 Discussion

The overall goal of this thesis is to answer the following question: "How can NFT trading be improved in the metaverse?". After collecting research articles from databases and analyzing them using the developed protocol, and based on the three challenges obtained from the collected research articles, to reach the best ways to answer each challenge, the main research question was answered. The discussion section includes opportunities that are repeatedly raised and some controversy about the mechanism of dealing with challenges, as well as some of the issues that have been left unanswered.

By looking at the results section of this thesis, we can address the challenges that have been mentioned and which represent the main question. Depending on the categories derived from data analysis, three of the technologies that dominated the development of solutions to the challenges can be identified, namely smart contracts, oracle nodes, and blockchain. The rest of the solutions presented to the challenges represent individual and non-repeated ideas.

Regarding smart contracts, it showed the possibility of using this solution to support more protection of owners' identities. Based on dynamic NFT and the ability to change metadata, increasing the confirmation and authentication of user identities and a higher degree of transparency. Moreover, NFT authentication

comes in several forms, with the owner's immediate involvement. Also, change the NFT metadata to confirm user authentication and confirm ownership. This is achieved in a decentralized manner with oracle Node, as it is considered a third party that works to block stolen NFT transactions and confirm ownership by relying on re-encryption Proxy. The flexibility of smart contracts and their volunteering to current conditions facilitated these solutions. With the reliability of users and NFTs provided by these technologies, the NFT trading in the metaverse increases and becomes more secure.

Using blockchain enables authentication and confirmation for NFT users continuously due three reasons. First, verified ledger. Second, decentralized processes. Third, owner access rights via protocols like digital wallets. Furthermore, data validation of NFT metadata with a single source of reliable information to all users at every stage. Also, quick response to identify users' identities using a cross-domain blockchain scheme which includes PKI and ZNP techniques.

Regarding other solutions not listed in the results, challenges can be addressed differently like using non-browser wallets and sustainable platforms such as SolarCoin and BitGreen, EtherScan, and ColdWallet. These solutions are individual results of studies and have not been widely used in the virtual world. These solutions need more support in communities that consider blockchain and Smart contracts the only solution to the challenges facing the NFT market in the metaverse. This market is growing exponentially compared to solutions that do not meet this growth.

5.1 Open Issues

Some neglected aspects of the proposed solutions could hinder access to the desired results. These areas are further discussed in the section below:

Regarding Multiple Convolutional Neural Networks (MCNN), Leppla et al (2022) stated that the model's inability to predict the risk of hijacking(Hijacking is the possibility of taking over and controlling computer systems, communications, and programs by attackers) whitelisted information by fraudsters. Incorrect prediction of whitelists is another issue. The system filters limited transactions as fraud, and this does not apply to the new original owners. Lastly, this model can also be used by scammers to evade detection. No article reviewed in this thesis explicitly states any solution to the open issue of whitelists Hijacking. Solutions can be drawn from the result section presented in this thesis with similar problems. here, the information regarding whitelists must be constantly updated.

The Reentrancy attack vulnerability in smart contracts is one of the problems that is still unsolved. The scammer executes a function that interacts with another contract and performs a call function again before the first function call completes, allowing the creation of a duplicate copy of the NFT. It is difficult for new users to distinguish the duplicate NFT from the original one(Chinen et al., 2020). No article reviewed in this thesis explicitly states any solution to the open issue of Reentrancy attack vulnerability. The solution includes checking components and updating all state variables before dealing with other contracts. The use of Mutex, which is a type of lock that was presented in the results section by Cao et al (2022), prevents the execution of multiple functions at the same time and function. Resorting to a third party to confirm smart contracts.

Regarding Zero Trust Architecture (ZTA): It is worth noting the importance of finding formulas and laws regulating the NFT trading process in the metaverse safely. There is a huge gap between organizations and legislation that defines the nature of this trade and what is legal and illegal. Also, the risk is that if the Oracle node is compromised, the dynamic NFT smart contracts will also be compromised. Therefore, maintaining the security and integrity of the Oracle network is of high importance for all solutions that count on it.

Rug pull tool: difficulty relying on one study case to draw reliable results. The NFT Rug pull project must be followed up for longer periods to ensure that the project can reduce fraud.

NFTM recommendations: Counterfeiters use similar collection names to bypass NFTM restrictions like adding(.) at the end of the string name or using upper or lower case. So far, no obvious solution has been adopted.

5.2 Reliability

Reliability in scientific research is the possibility of repeating all mentioned steps to get the same results. As a kind of reliability, the steps of scientific research should be detailed to demonstrate high reliability(Denscombe, 2010).
Work has been done to provide the reliability of this thesis by listing a detailed review of scientific articles after following the steps of collecting them from scientific databases. Also, the search strategy was mentioned along with the terms used, and the inclusion and exclusion criteria.
Concerning bias, since this thesis is a result of one author, there is a possibility of a certain percentage of bias in article selection and sampling. The reason behind this is the absence of another opinion. We note the possibility of errors in extracting data or classifying certain information. The bias of the collected articles should also be taken into account.

5.3 Validity

Validity carries two meanings: the first is the accuracy of the extracted data, and the second is the relevance of the extracted data to answering the research question, and whether these data achieve a reinforcement of the investigation of the research question Denscombe (2010).
The systematic literature review provides good validity due to its rigorous and robust approach. As explained above, the developed protocol was configured to identify useful information for answering the research question.

5.4 Limitations

During the data collection process for this thesis, a kind of challenge was encountered, such as limited access, due to the obligation to pay a subscription fee or a monetary value to obtain the required data. These articles are referenced and their effects are unknown. It is worth noting the help obtained by the supervisor to access some of these articles. Moreover, time constraints and a lack of previous research studies on this topic may harm this project. Technical issues were addressed, not legal or social components.

6 Conclusion

The transition to a virtual 3D reality in which a person can experience actions that cannot be achieved in real reality was difficult to achieve in the past. With technology, this idea has become available in our world today by introducing the metaverse. Everything an individual needs to have a real experience has become available in this world like currencies, collectibles, artwork, property, etc. As shown in this thesis, NFT which is the property that can be traded in the virtual world has become vulnerable to security issues, fraud, and scams. Here, the main question of this thesis is raised which is **“How can NFT trading in Metaverse be improved?”**. The elected solutions used to address these challenges use multiple formulas. The majority of those formulas rely on smart contracts, oracle nodes, and blockchain. A systematic literature review was conducted. 160 scientific articles were collected from digital databases. 14 articles that constitute the final results of this thesis are passing the developed exclusion and filtered protocol. After reviewing and analyzing all relevant articles, three main challenges were elected to represent the main question of this thesis with several solutions to address these challenges. The most frequent models found in the literature study achieving these solutions were smart contracts, oracle

nodes, and blockchains. The smart contract model based on the Oracle nodes provides the possibility to securely confirm the identity of traders to NFT. Also, limiting the possibility of scam operations depends on the possibility of verifying ownership from the owners in a real-time manner. By relying on blockchain and smart contracts, NFT metaverse trading opportunities are more secure. These technologies show the potential to reduce scams and fraud and enhance the security of NFT trading. These technologies can be utilized together to gain greater flexibility in facing these challenges. Developing regulations and systems that regulate this trading and urging platform developers to adopt these ideas leads to a safer environment. It should be noted that the mentioned solutions do not cover all the risks faced by traders in the metaverse. Scammers take advantage of the inability of developers to keep up with the huge development of this field to find appropriate solutions to immediate problems.

6.1 Future work

This thesis discussed the challenges faced by NFT in the metaverse, and what are the solutions that may help to get rid of these challenges. Future work can survey new technologies that contribute to more secure NFT trading and highlight the importance of laws and controls that help improve the trading situation. Systematic literature review analyses and results point to a predominant solution of smart contracts. For this, conducting a study to find a combination between smart contracts and self-sovereign identity solutions and the impact of self-sovereign identity in this area will be interesting.

References

Ali, O., Momin, M., Shrestha, A., Das, R., & Alhajj, F. (2022). *A review of the key challenges of non-fungible tokens*, (ELSEVIER). https://doi.org/10.1016/j.techfore.2022.122248

Aulia Mochram, R. A., Makawowor, C. T., Michael Tanujaya, K., & V. Moniaga, J. (2022). Systematic Literature Review: Blockchain Security in NFT Ownership. (IEEE). 10.1109/IEIT56384.2022.9967897

Barber, R. (2022, July 17). *NFT Statistics, Facts & Trends in 2023 [What are NFTs?]*. Cloudwards. https://www.cloudwards.net/nft-statistics/

Battah, A., MADINE, M., YAQOOB, I., SALAH, K., R. HASAN, H., & JAYARAMAN, R. (2022, October 19). Blockchain and NFTs for Trusted Ownership, Trading, and Access of AI Models. (IEEE). 10.1109/ACCESS.2022.3215660

Bhujel, S., & Rahulamathavan, Y. (2022). A Survey: Security, Transparency, and Scalability Issues of NFT's and Its Marketplaces. (MDBI).

Bryman, A. (2014). *social research methods* (4th ed.). New York: Oxford University Press Inc.

Cao, Z., Zhen, Y., Fan, G., & Gao, S. (2022). TokenPatronus: A Decentralized NFT Anti-theft Mechanism. (arXiv).

Chinen, Y., Yanai, N., Paul Cruz, J., & Okamura, S. (2020, Dec 11). RA: Hunting for Re-Entrancy Attacks in Ethereum Smart Contracts via Static Analysis. (IEEE). 10.1109/Blockchain50366.2020.00048

Choi, M., EL Azzaoui, A., Kumar Singh, S., Mohammed Salim, M., Reward Jeremiah, S., & Hyuk Park, J. (2022). *The Future of Metaverse: Security Issues, Requirements, and Solutions*. HCIS. http://hcisj.com/articles/?HCIS202212060

Christodoulou, K., Katelaris, L., Themistocleous, M., Christodoulou, P., & Iosif, E. (2022). NFTs and the Metaverse Revolution: Research Perspectives and Open Challenges. In *Blockchains and the Token Economy*. SpringerLink. 10.1007/978-3-030-95108-5_6

Das, D., Bose, P., Ruaro, N., Kruegel, C., & Vigna, G. (2022, april 27). Understanding Security Issues in the NFT Ecosystem. (arXiv).

Deng, W., Huang, T., & Wang, H. (2022, December 26). *A Review of the Key Technology in a Blockchain Building Decentralized Trust Platform*.

Denscombe, M. (2010). *The Good Research Guide: For Small-scale Social Research Projects*. McGraw-Hill/Open University Press.

Foteini Valeonti, F. V., Bikakis, A., Terras, M., Speed, C., Hudson-Smith, A., & Chalkias, K. (2021). Crypto Collectibles, Museum Funding and Open GLAM. (MDPI). 10.1007/978-3-030-95108-5_6

The Future of the Metaverse. (n.d.). Deloitte. https://www2.deloitte.com/us/en/pages/technology/articles/what-does-the-metaverse-mean.html

Gupta, A., Khan, H. U., Nazir, S., Shafiq, M., & Shabaz, M. (2023, Jan 12). Metaverse Security: Issues, Challenges and a Viable ZTA Model. (MDPI).

Han, N., Kim, E., Park, Y., & Jo, S. (2021, December). Educational applications of metaverse: possibilities and limitations. *journal of educational evaluation for health professions*. https://synapse.koreamed.org/articles/1149230

Hosseini Bamakan, S. M., & Solouki, M. (2022). An In-depth Insight at Digital Ownership Through Dynamic NFTs. (ACM digital library). org/10.1016/j.procs.2022.11.254

How does blockchain work? | *Stanford Online*. (n.d.). Stanford Online. https://online.stanford.edu/how-does-blockchain-work

Hughes, I. (2022, Feb 17). *The Metaverse: Is it the Future?* The magazine for the IT professional. https://doi.org/10.1093/itnow/bwac011

Introducing Microsoft Mesh. (n.d.). Microsoft. https://www.microsoft.com/en-us/mesh#tabx228a2366f0464a8ca2351068f172be25

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science*. Springer International Publishing.

Khan, F., Kothari, R., Patel, M., & Banoth, N. (2023, 3). Enhancing Non-Fungible Tokens for the Evolution of Blockchain Technology. (IEEE). 10.1109/ICSCDS53736.2022.9760849

Kitchenham, B. (2007, january). *Guidelines for performing Systematic Literature Reviews in Software Engineering*. https://www.researchgate.net/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering

Kitchenham, B. (2010). *Can we evaluate the quality of software engineering experiments?* https://www.researchgate.net/publication/221494751_Can_we_evaluate_the_quality_of_software_engineering_experiments

Kitsantas, T. (2022, June 22). Exploring Blockchain Technology and Enterprise Resource Planning System. (MDPI). https://doi.org/10.3390/su14137633

Kumar Mohanta, B., Panda, S. S., & Jena, D. (2018, october). *An Overview of Smart Contract and Use Cases in Blockchain Technology*.

The largest NFT/Metaverse hacks of 2021/2022. (2022, June 23). LinkedIn. https://www.linkedin.com/pulse/largest-nftmetaverse-hacks-20212022-entersoft-security

Leppla, A., Olmos, J., & Lamba, J. (2022). *Fraud Pattern Detection for NFT Markets*. https://scholar.smu.edu/datasciencereview/vol6/iss2/21

Mathew, S. (2014, march). Importance of Virtual Reality in Current World. *International Journal of Computer Science and Mobile Computing*, (IJCSMC). ISSN 2320–088X

Meta market. (n.d.). MarketsandMarkets. https://www.marketsandmarkets.com

Musamih, A., Dirir, A., Yaqoob, I., Salah, K., Jayaraman, R., & Puthal, D. (2022). NFTs in Smart Cities: Vision, Applications, and Challenges.

Olade, I., Fleming, C., & Liang, H.-N. (2022, May 22). BioMove: Biometric User Identification from Human Kinesiological Movements for Virtual Reality Systems. (MDPI). https://doi.org/10.3390/s20102944

Omair, B., & Alturki, A. (2020). Taxonomy of Fraud Detection Metrics for Business Processes. (IEEE), 1. 10.1109/ACCESS.2020.2987337

Ott, K. (2009, Mar 02). Virtual Reality and Simulations in Adult and Career Education. *Society for Information Technology & Teacher Education International Conference*, (AACE). 978-1-880094-67-9

Our NFT Market Report Q1 2022 is published. (2022, April 28). NonFungible.com. https://nonfungible.com/news/corporate/nft-market-report-q1-2022

Popescu, A.-D. (2021, august). *Non-Fungible Tokens (NFT) - Innovation beyond the craze*. https://www.researchgate.net/publication/353973149

Rehman, W., Zainab, H. e., Imran, J., & Bawany, N. Z. (2021). NFTs: Applications and Challenges.

Shen, M., Liu, H., Zhu, L. Z., Xu, K., Yu, H. Y., Du, X., & Guizani, M. (2020, May). Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT. (IEEE). 10.1109/JSAC.2020.2980916

Sigalos, M. (2022, January 6). *Crypto scammers took a record $14 billion in 2021*. CNBC. https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html

Šljukić, M. (2022). Register as a tool to fight utility NFT rug pull. (EBT).

Smaili, M. w. t. t. n. f. m. N., & de Rancourt-Raymond, A. (2022). Metaverse: welcome to the new fraud marketplace. (Emerald Publishing Limited). https://doi.org/10.1108/JFC-06-2022-0124

Smart, J., Cascio, J., & Paffendorf, J. (2007). *Metaverse Roadmap*. Metaverse Roadmap: Pathways to the 3D Web. https://mail.metaverseroadmap.org/

Srinivas, J., Kumar Das, A., Kumar, N., & J. P. C. Rodrigues, J. (2020). Cloud Centric Authentication for Wearable Healthcare Monitoring System. (IEEE). 10.1109/TDSC.2018.2828306

Tambe Ebot, A. (2023, May 5). Advance fee fraud scammers' criminal expertise and deceptive strategies: a qualitative case study. *Information and Computer Security*, (Emerald insight). 2056-4961

Tomkevičiūtė, A. (2023, March 20). *Discord Virus: What's It & How to Remove It?* Cybernews. https://cybernews.com/malware/remove-discord-malware/

Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. 10.1016/j.infsof.2015.03.007

Valeonti, F., Bikakis, A., Terras, M., Speed, C., Hudson-Smith, A., & Chalkias, K. (2021, october 24). *Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs)*.

Vassou, S. A., Anagnostopoulos, N., Amanatiadis, A., Christodoulou, K., & Chatzichristofis, S. A. (2017, November 16). *A Compact Composite Moment-Based Descriptor for Image Retrieval*. dl.acm.org.

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges.

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., H. Luan, T., & Shen, X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. (IEEE). 10.1109/COMST.2022.3202047

What is Blockchain Technology? - IBM Blockchain. (n.d.). IBM. https://www.ibm.com/se-en/topics/what-is-blockchain

What is Minting an NFT? How to Mint using OpenSea. (n.d.). OpenSea. https://opensea.io/learn/what-is-minting-nft

What is the Metaverse? (n.d.). Meta. https://about.meta.com/what-is-the-metaverse/

What is the Metaverse? (n.d.). Meta. https://about.meta.com/what-is-the-metaverse/

Zhao, T., Wang, Y., Liu, J., Chen, Y., Cheng, J., & Yu, J. (2020). TrueHeart: Continuous Authentication on Wrist-worn Wearables Using PPG-based Biometrics. (IEEE). 10.1109/INFOCOM41043.2020.9155526

Appendix A – Search Process

This appendix provides information about search strings and the iteration of the inclusion and exclusion criteria. As well as the number of articles that were generated with each search and the number of articles that were dispensed with each iteration. N represents the number of articles.

1- IEEE Xplore: Metaverse AND NFT AND challenges N=39

A- First iteration partially about metaverse, Non-fungible tokens, challenges, solutions -29 articles (N=10)

B- Second iteration about articles with other aspects and not related to the research topic -4 articles (N=6)

C- Third iteration about financial, educational, marketing, and healthcare aspects -1 article (N=5)

D- Fourth iteration about duplicate paper -0 articles (N=0)

E- Fifth iteration about not academic paper -0 articles (N=5)

2- ACM digital library: Challenges AND Solutions AND Metaverse AND N=40

A- First iteration partially about metaverse, Non-fungible tokens, challenges, solutions -16 articles (N=24)

B- Second iteration about articles with other aspects and not related to the research topic -17 articles (N=7)

C- Third iteration about financial, educational, marketing, and healthcare aspects -4 articles (N=3)

D- Fourth iteration about duplicate paper -0 articles (N=3)

E- Fifth iteration about not academic paper -0 articles (N=3)

3- ScienceDirect: Metaverse AND NFT AND challenges AND solutions N=39

A- First iteration partially about metaverse, Non-fungible tokens, challenges, solutions -19 articles (N=20)

B- Second iteration about articles with other aspects and not related to the research topic -7 articles (N=13)

C- Third iteration about financial, educational, marketing, and healthcare aspects -8 articles (N=5)

D- Fourth iteration about duplicate paper -3 articles (N=2)

E- Fifth iteration about not academic paper -0 articles (N=2)

4- Google Scholar: Solutions AND Non-fungible token AND Metaverse AND challenges N=42

A- First iteration partially about metaverse, Non-fungible tokens, challenges, solutions -20 articles (N=22)

B- Second iteration about articles with other aspects and not related to the research topic -3 articles (N=19)

C- Third iteration about financial, educational, marketing, and healthcare aspects -8 articles (N=11)

D- Fourth iteration about duplicate paper -6 articles (N=5)

E- Fifth iteration about not academic paper -1 article (N=4)

Reflection – Khalil Al-Towhi

During the past months, I learned practically about scientifically conducting a master's thesis. The scientific research strategy and research method appropriate to the research topic has been chosen. A systematic literature review, for further increasing knowledge in the field of computer and system science, was utilized to achieve the goals without ignoring the ethical aspect, which in turn helps to present an ethically sound thesis. Due to no personal information being gathered, the ethical aspects in this thesis are considered to be small. The thesis objectives have been completed.

As planned, the time was divided to complete each part within a specific period. Collecting and analyzing information was carried out smoothly and successfully to elicit the desired results. The results section required a double effort to be completed and I still feel it needed more effort. Ideas and arguments from another author with challenges that can be developed well lead to improved results even further. The peer review in SciPro certainly gives a boost of improvement to the work.

There are some difficulties that I encountered in obtaining a good number of scientific articles that contribute to enhancing the results. The weekly meetings with the supervisor helped greatly in analyzing the results and clarifying the problems that faced the thesis in all its stages.

The thesis topic was chosen based on several courses studied in this program, among these courses are

Internet of Things, Introduction to Information Security, and cyber security. The rest of the courses that were studied in this program with this thesis established a scientific base that I hope to benefit from to achieve future goals. This thesis will have a great impact on my future field of study and the type of jobs as well.

I hope that the results achieved in this thesis will be a scientific base through which I can dive deeper into this field to find a connection between Oracle nodes and SSI to improve the NFT environment in the metaverse. Solutions with a greater impact to reduce the phenomenon of scams and fraud and improve security in the field of the NFT in the metaverse are what I hope to involve in.

I am content and had a pleasant experience conducting this research at this level.