



T.C.

TOKAT GAZİOSMANPAŞA UNIVERSITY

GRADUATE EDUCATION INSTITUTE

DEPARTMENT OF PUBLIC ADMINISTRATION

MASTER'S DEGREE PROGRAM

STRENGTHENING FINANCIAL DIGITAL SAFETY IN THE METAVERSE

MASTER'S THESIS

Otuekong David EKANEM

Thesis Advisor: Prof. Dr. Yusuf TEMUR

TOKAT – 2025

ETHICAL AGREEMENT

According to Gaziosmanpaşa University Graduate Education Institute thesis writing guide, I have prepared in consultation of Dr. Yusuf Temur, “Strengthening Financial Digital Safety in the Metaverse.” I declare that my Master's thesis is an original work under scientific, ethical values and rules. I will accept all kinds of legal sanctions if the opposite is determined.

... / ... / ...

Otuekong David EKANEM

PREFACE

No amount of words can enunciate my heartfelt gratitude to the Almighty God for bringing my academic journey to a successful end. A feat that I have always relished. It is a dream come true, and all I can say is Alhamdulillah.

I also wish to acknowledge several people who have academically contributed to the realization of this thesis. I want to express my profound appreciation to my Counselor Dr. Yusuf Temur, for his apt and astute mentorship and guidance throughout my research expedition. Your continued dedication and push for excellence are unsurpassed, and I am forever grateful for such a positive impact.

Special thanks to my beloved teachers for their personal and extra comments at a point; I am most thankful for your effort and time. Furthermore, I wish to thank the Social Science Institute, Department of Public Administration and Gaziosmanpasa University for the knowledge and experience gained through their top-notch academic modules, various seminars, and tutorials throughout my two-year master Studies. These were deemed crucial to my intellectual development.

ÖZET

METaverse'DE FİNANSAL DİJİTAL GÜVENLİĞİN GÜÇLENDİRİLMESİ

Ekanem, Otuekong David

Yüksek Lisans, Maliye Anabilim Dalı

Tez Danışmanı: Prof. Dr. Yusuf Temur

Temmuz 2025; vii + 80 sayfa

Bu çalışma, gelişmekte olan metaverse ortamında dijital finansal güvenliği artırmaya yönelik çözümleri araştırmaktadır. Bankacılık hizmetlerinin sanal gerçeklik (VR), artırılmış gerçeklik (AR) ve karma gerçeklik (MR) gibi genişletilmiş gerçeklik teknolojilerini giderek daha fazla benimsemesiyle birlikte, finansal işlemleri tehdit eden yeni güvenlik açıkları ortaya çıkmaktadır. Yapay zekânın 5G ağlarıyla entegrasyonu ise bu dijital sınırda hem fırsatları hem de güvenlik zorluklarını artırmaktadır. Nicel bir yaklaşım benimseyen araştırma, 350 bankacılık profesyoneliyle finansal güvenlik önlemlerine ilişkin bir anket gerçekleştirmiştir. Anket, demografik veriler toplamış, güvenlik çözümlerinin algılanan faydalarını değerlendirmiş ve güvenlik iyileştirmelerini etkileyen faktörleri incelemiştir. Ki-kare testleri, teknoloji kullanım düzeyleri ile algılanan güvenlik etkinliği arasındaki ilişkileri analiz etmiştir. Temel bulgular, katılımcıların %59,7'sinin çok faktörlü kimlik doğrulamayı, %56,8'inin ise gelişmiş şifreleme yöntemlerini güçlü bir şekilde desteklediğini ortaya koymuştur. Ancak analizler, metaverse benimseme düzeyleri ile algılanan finansal güvenlik arasında anlamlı bir korelasyon olmadığını göstermiştir ($p=0,084$). Bu sonuçlar, teknik çözümlerin kullanıcı eğitimi ve düzenleyici standartlarla birleştirildiği entegre güvenlik çerçevelerinin gerekliliğini vurgulamaktadır.

Anahtar Kelimeler: Kripto Paralar, Finansal Kuruluşlar, Dijital Güvenlik, Metaverse, Siber Güvenlik.

ABSTRACT

STRENGTHENING FINANCIAL DIGITAL SAFETY IN THE METAVERSE

Ekanem, Otuekong David

Master's Thesis, Public Administration

Thesis Advisor: Prof. Dr. Yusuf Temur

July 2025; vii +80 pages

This study investigates solutions for enhancing digital financial security in the emerging metaverse environment. As banking services increasingly adopt extended reality technologies - including virtual reality (VR) for immersive digital environments, augmented reality (AR) for overlaying digital information on the physical world, and mixed reality (MR) that blends and interacts with real-world elements - new vulnerabilities threaten financial transactions. The integration of AI with 5G networks further compounds both the opportunities and security challenges in this digital frontier. Using a quantitative approach, the research surveyed 350 banking professionals about financial safety measures. The questionnaire collected demographic data, assessed perceived benefits of security solutions, and examined factors influencing safety improvements. Chi-square tests analyzed relationships between technology usage levels and perceived security effectiveness. Key findings revealed strong support for advanced security measures, with 59.7% of respondents strongly endorsing multi-factor authentication and 56.8% favoring advanced encryption methods. However, analysis showed no significant correlation between metaverse adoption levels and perceived financial safety ($p=0.084$). These results highlight the need for integrated security frameworks combining technical solutions with user education and regulatory standards.

Keywords: Cryptocurrencies, Financial Institutions, Digital Safety, Metaverse, Cybersecurity.

TABLE OF CONTENTS

Content	Page
Scientific ethics page.....	ii
Preface.....	iii
Özet.....	viii
Abstract.....	ix
Table of content	viii
List of Tables	xi
List of Figures.....	xii
 INTRODUCTION.....	 1
 CHAPTER ONE: METAVERSE.....	 3
1.1 Background to the Study.....	3
1.2 Statement of the Problem	4
1.3 Research Questions	5
1.4 Research Hypotheses.....	5
 CHAPTER TWO: LITERATURE REVIEW	 6
2.1 Concept of Historical Development of the Metaverse.....	6
2.1.1 Origin of Metaverse	9
2.2 Concept of Metaverse.....	10
2.3 Impact of Using the Metaverse on Financial Digital Safety.....	12
2.3.1 Importance of Metaverse	13
2.3.2 Impact of Metaverse in Financial World	15
2.3.3 The Metaverse Potential in the Finance Market	16
2.3.4 The Finance World in Development Through Metaverse	17
2.4 Advantages and Disadvantages for Financial Service Companies Brought by the Metaverse.....	 17
2.5 Financial Services' Presence in the Metaverse	19
2.6 Metaverse for Corporate Banking	22
2.6.1 Metaverse for Retail Banking	23

2.6.2 Challenges Associated With Corporate Banking in The Metaverse.....	25
2.7 Appraisal of Literature Review.....	27
CHAPTER THREE: RESEARCH METHODOLOGY.....	28
3.1 Research Design.....	28
3.2 Sample and Sampling Technique.....	28
3.3 Instrumentation.....	29
3.4 Validity of Instrument.....	29
3.5 Procedure for Data Collection.....	29
3.6 Method of Data Analysis.....	29
CHAPTER FOUR: PRESENTATION OF RESULT AND DISCUSSIONS	30
4.1 Preamble.....	30
4.2 Presentation and Analysis of Data.....	30
4.2.1 Answer to Research Question One.....	31
4.2.2 Answer to Research Question Two.....	34
4.2.3 Answer to Research Question Three	38
4.2.4 Test of Hypotheses	42
CHAPTER FIVE: DISCUSSION, CONCLUSION AND RECOMMENDATION.....	46
5.1 Discussion of the Findings.....	46
5.2 Conclusion.....	50
5.3 Recommendations.....	51
References.....	54
APPENDIX.....	64

LIST OF TABLES

Tables	Page
Table 4.1. Socio-Demographic Characteristics	31
Table 4.2. Respondents' Views on Financial Digital Safety Enhancing Trust, Security, and Stability in the Metaverse.....	32
Table 4.3. Comparison between Level of Metaverse Usage and Financial Digital Safety.....	35
Table 4.4. Key factors contribute to enhancing financial digital safety within the metaverse.....	36
Table 4.5. Comparison of the financial digital safety and the usage of metaverse.....	40
Table 4.6. Effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment.....	41
Table 4.7 Comparison of the effective solutions that can ensure secure and reliable financial interactions on emerging digital environment.....	45

LIST OF FIGURES

Tables	Page
Figure 2.1. The History of Metaverse	7
Figure 2.2. Leading business sectors that have invested in the Metaverse, as of 2022.....	8
Figure 2.3. Metaverse platforms by type.....	10
Figure 2.4. Examples of financial institutions present in the metaverse.....	2



INTRODUCTION

The rapid evolution of digital technologies has ushered in a new era of virtual interaction, fundamentally transforming how individuals and institutions engage in financial activities. At the forefront of this revolution is the metaverse, a persistent, immersive digital ecosystem that blends augmented reality (AR), virtual reality (VR), and blockchain technologies to create interconnected virtual worlds. As financial services increasingly migrate into these digital realms, new opportunities for innovation emerge alongside unprecedented security challenges.

The metaverse promises to redefine economic transactions through decentralized finance (DeFi), non-fungible tokens (NFTs), and digital asset ownership. However, its decentralized nature, coupled with the anonymity of blockchain-based transactions, introduces vulnerabilities such as fraud, identity theft, and regulatory gaps. Financial institutions, policymakers, and users alike must navigate these risks to ensure a secure and trustworthy digital economy.

This study, titled "Strengthening Financial Digital Safety in the Metaverse," seeks to address these challenges by examining the effectiveness of current security measures, identifying key risk factors, and proposing integrated solutions. Through a quantitative analysis of banking professionals' perspectives, this research evaluates the role of advanced encryption, multi-factor authentication (MFA), artificial intelligence (AI), and regulatory frameworks in safeguarding financial transactions within virtual environments.

The findings of this study aim to contribute to the growing discourse on metaverse security, offering actionable insights for financial institutions, technology developers, and policymakers. By bridging the gap between technological innovation and cybersecurity, this research underscores the necessity of a multi-layered approach, combining technical safeguards, user education, and adaptive regulations to foster a resilient and inclusive digital financial ecosystem.

The subsequent chapters will explore the historical development of the metaverse (Chapter 1), analyze its impact on financial security (Chapter 2), present the research

methodology (Chapter 3), discuss empirical findings (Chapter 4), and conclude with recommendations for future practice and research (Chapter 5).



CHAPTER ONE

1.1 BACKGROUND TO THE STUDY

The rapid evolution of digital technologies has accelerated the development of the Metaverse - a persistent virtual environment that blends physical and digital realities through extended reality (XR) technologies including virtual reality (VR), augmented reality (AR). First conceptualized in Neal Stephenson's 1992 science fiction novel "Snow Crash," the Metaverse has evolved from theoretical concept to emerging digital ecosystem with significant implications for financial systems (Stephenson, 1992; Ning et al., 2021).

This virtual environment enables new forms of economic interaction through digital twins, blockchain technology, artificial intelligence (AI), and Internet of Things (IoT) systems (Alsharida et al., 2019). Major technology firms including Meta (formerly Facebook), Microsoft, and Google have made substantial investments in Metaverse platforms, developing applications ranging from virtual commerce to remote collaboration tools (Dwivedi et al., 2022; Alomar et al., 2024). Cryptocurrencies and other digital assets have emerged as primary mediums of exchange within these virtual economies, facilitated by decentralized blockchain networks that operate without traditional financial intermediaries (Belk et al., 2022; Giudici et al., 2020).

However, the financial potential of the Metaverse is accompanied by significant security challenges. Industry reports indicate growing concerns about cybersecurity threats including fraud, identity theft, and unauthorized access to digital assets (John et al., 2023). The decentralized nature of many Metaverse platforms creates regulatory gaps that malicious actors may exploit (Bax et al., 2024). Additionally, unequal access to required technologies raises concerns about financial exclusion and the digital divide (Fungáčová & Weill, 2015; Ghosh &

Vinod, 2017). With projections suggesting the Metaverse will become an integral part of daily life by 2040 (Anderson et al., 2022), establishing robust financial security frameworks has become imperative.

1.2 STATEMENT OF THE PROBLEM

The Metaverse presents both opportunities and challenges for financial systems. On one hand, it offers potential solutions for financial inclusion by providing access to virtual economic opportunities regardless of physical location (Wheatley, 2021). Entrepreneurs in developing regions can participate in global markets, while creators can monetize digital assets through platforms like Decentraland and The Sandbox (Aharon et al., 2023).

However, several critical problems threaten financial security in the Metaverse:

- a. **Technological Barriers:** Unequal access to VR/AR hardware and reliable internet connections creates exclusion (Kazemikhasragh & Buoni Pineda, 2022)
- b. **Security Vulnerabilities:** Decentralized systems are susceptible to fraud, hacking, and smart contract exploits (Binance, 2023)
- c. **Regulatory Challenges:** Lack of clear governance frameworks for virtual financial transactions (Massally et al., 2022)
- d. **Privacy Concerns:** Extensive data collection raises issues about user protection (Alomar et al., 2024)

These challenges underscore the need for comprehensive solutions to ensure financial digital safety as the Metaverse evolves. This study aims to address these gaps by investigating effective security measures for virtual financial systems.

1.3 RESEARCH PURPOSES

The main aim of the study is to examine the effect of strengthening financial digital safety in the metaverse

Specific objectives include:

- i. To examine how financial digital safety enhance trust, security and stability in the metaverse
- ii. To investigate factors that contribute to enhancing financial digital safety within the metaverse
- iii. To implement effective solutions to ensure secure and reliable financial interactions in this emerging digital environment

1.4 RESEARCH QUESTIONS

Based on the forgoing objectives, the study will answer the following research questions:

- i. How does financial digital safety enhance trust, security and stability in the metaverse?
- ii. What key factors contribute to enhancing financial digital safety within the metaverse?
- iii. What are the effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment?

1.5 RESEARCH HYPOTHESES

The following are the research hypothesis of this study:

- i. Level of usage of metaverse will not significantly affect the financial digital safety.
- ii. There is no significant relationship between financial digital safety and the usage of metaverse.
- iii. There is no significant relationship between the effective solutions that can ensure secure and reliable financial interactions on emerging digital environment

This chapter has established the study's foundation by examining the Metaverse's development, identifying key financial security challenges, and outlining the research objectives. The following chapters will review relevant literature, detail the research methodology, present findings, and discuss implications for theory and practice.

CHAPTER TWO

2. CONCEPTUAL FRAMEWORK

2.1 CONCEPT OF HISTORICAL DEVELOPMENT OF THE METAVERSE

American novelist Neal Stephenson coined the term "Metaverse" in his 1992 science fiction book "Snow Crash." Stephenson could hardly have predicted that the metaverse would materialize in less than 30 years. In parallel to our physical world, a growing number of businesses have ventured into this "second" world throughout time. The metaverse is a three-dimensional virtual world where people, portrayed by avatars, can do a wide range of functions, including socializing, interacting, playing, working, buying, and traveling. Mystakidis (2022) defines the metaverse as a post-reality cosmos, a persistent and ever-present multi-user environment that combines digital virtuality and physical reality. It is dependent on technology that allow for multimodal interactions between virtual worlds, digital objects, and people.

The word "metaverse" was first used by Neal Stephenson in 1992, which led to the development of this idea. Since Facebook CEO Mark Zuckerberg announced the company's rebranding to Meta in 2021, the term's relevance has increased significantly in the twenty-first century. A "new phase of integrated virtual experiences employing technologies like virtual and augmented reality" began with this rebranding. However, before the metaverse could materialize, a number of requirements needed to be fulfilled. These included the birth of the Internet, the isolation caused by the global Covid-19 pandemic, and the emergence of numerous technologies (including social media, augmented and virtual reality, avatars, simulation, and artificial intelligence). "Technological advancements and more innovative technologies in recent years, such as artificial intelligence, blockchain, advanced mobile networks with 5G, and the Internet of Things, have driven the emergence of the new virtual world, the metaverse,

which is considered an immersive, three-dimensional, virtual, and multi-user online environment," according to author Ng Kit Tsz (2022). As a result, "metaverse" has come to mean innovative technologies and inventions. Figure 1 below shows the evolution of the metaverse over time.

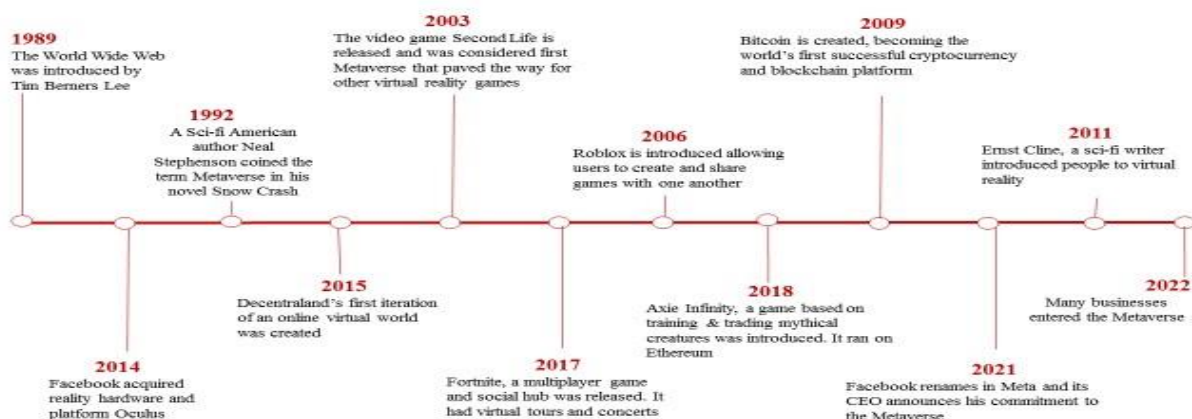


Figure 2.1. The History of Metaverse

Source: Own research, 2023

It is clear from the Metaverse's historical growth that the gaming industry was the first to use this virtual environment. Companies, banks, financial institutions, and other organizations have been able to participate in the Metaverse thanks to gaming platforms like Sandbox, Roblox, Decentraland, Fortnite, and Minecraft. One of the main characteristics of the Metaverse is that it will operate as a full-fledged economy, as Ball (2020) pointed out. In this economy, a wide variety of work that produces value that is acknowledged by others will be able to be created, owned, invested in, sold, and rewarded by individuals, non-financial entities, and financial entities.

When envisioned at this scale, the metaverse economy would replicate the real economy, establishing a "twin" universe in which people and companies could decide what to produce, acquiring, investing in, purchasing, and selling value. In this new digital platform

economy, where all digital firms and individuals/avatars interact, the circular flow diagram of the economy might be duplicated. The Metaverse is viewed as an improvement to a fully working economy, even though virtual economies have long existed in individual games, where players trade virtual items or complete digital activities in exchange for real money (cryptocurrency, e-money, or fiat currency). About 500 businesses are presently operating in the Metaverse, per a survey by market research firm Newzoo (Takahashi, 2022). According to McKinsey, the Metaverse may be worth \$5 trillion by 2030. This information highlights the substantial influence that the Metaverse is anticipated to have on a range of industries over the next several years.. The percentage share of individual businesses investing in the Metaverse is illustrated in the following figure:

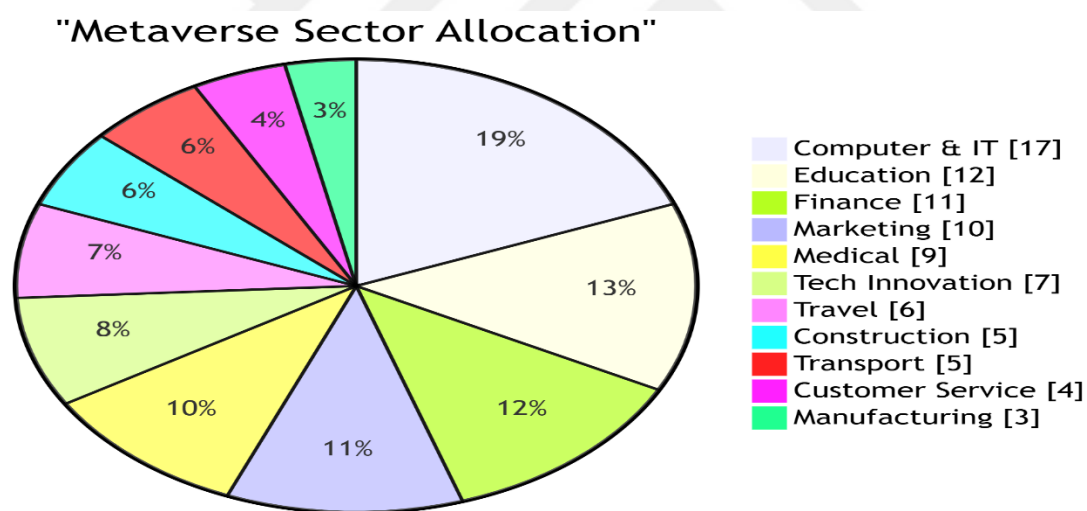


Figure 2.2. Leading business sectors that have invested in the Metaverse, as of 2022

Clement, J. (2022) is the source. Prominent industries are already making investments in the Metaverse. According to Statista statistics as of March 2022, the finance industry is eager to get involved in the metaverse. Around 50% of banks worldwide are expected to use AR/VR as an alternate channel for employee engagement and client transactions by the end of this decade (The Economic Times, 2022).

2.1.1 Origin of Metaverse

The term "metaverse," as defined by Hackl (2021), combines the prefix "meta," meaning beyond, with "universe." Since it is a relatively new and evolving concept, the metaverse has multiple definitions. According to the Oxford Learner's Dictionary, it refers to a "virtual reality space where users can interact with a computer-generated environment and with each other." Tucci (2023) describes the metaverse as a 3D virtual environment where billions of users can live, work, shop, learn, and socialize from their homes. It represents a new iteration of the Internet, a shared, immersive space where people can engage in ways not possible in the physical world. McKinsey & Co. views it as an evolution of the current Internet that integrates various digital technologies, including cryptocurrencies, artificial intelligence, augmented reality (AR), and virtual reality (VR).

Majumder & Dutta (2023) offer a straightforward definition, describing the metaverse as a network of immersive virtual worlds that users can access for interaction, learning, and various activities like shopping and gaming. They identify key components of the metaverse:

- i. Content and Experiences: This includes user-generated content that enables interaction and engagement within virtual worlds.
- ii. Platforms: These provide access to the content and applications.
- iii. Hardware and Infrastructure: This encompasses the technology needed to support the metaverse, such as AR/VR devices and cloud computing.
- iv. Enablers: These help manage digital identity, privacy, security, and monetization within the metaverse.

The metaverse gained significant attention when Facebook rebranded to Meta in October 2021, announcing a \$10 billion investment in the concept. Following this, major tech

companies like Microsoft and Google began investing as well. McKinsey & Co. projects that the metaverse economy could reach \$5 trillion by 2030.

The metaverse is not a singular platform; rather, different companies can create their own versions using diverse technologies to offer unique experiences. Currently, there are 154 virtual worlds with approximately 606.4 million monthly active users (Metaversed, 2020). Most of these users (over 98%) are on Web 2.0 metaverses, which are accessible via web browsers or apps and predominantly consist of younger audiences. In these centralized environments, users cannot truly own the digital assets they create or purchase. Conversely, Web 3.0 metaverses are decentralized and built on blockchain technology, allowing users to govern the platforms and own their digital assets. Examples include Decentraland and Sandbox, where blockchain facilitates transactions involving virtual properties. However, the user base for these decentralized platforms remains below 2%. Recognizing the large user base of Web 2.0, many Big Tech companies are integrating blockchain features to transition towards a hybrid model, termed Web 2.5 that incorporates elements of decentralization and user ownership.

Platform	User Category	Q1 21	Q2 21	Q3 21	Q4 21	Q1 22	Q2 22	Q3 22	Q4 22	Q1 23	Q2 23	Q3 23	Q4 23
Web2													
	Kids/Tweens	305	315	320	325	330	350	405	435	450	454	479	519
	Other Users	14	15	18	20	29	35	38	42	45	46	49	53
	VR Rooms	4	4.5	5.5	6	6.5	7.5	7	8	9	9	9.3	21.6
	VR Worlds	2	2.25	2.5	2.75	3	3	3.25	3.5	4	3.5	3.5	4
	Subtotal	325.0	336.8	346.0	353.8	368.5	395.5	453.3	488.5	508.0	512.5	540.8	597.6
Web3													
	Ethereum VR	0	0	0	0	0	0	0	0	0	0	0	0

Platform	User Category	Q1 21	Q2 21	Q3 21	Q4 21	Q1 22	Q2 22	Q3 22	Q4 22	Q1 23	Q2 23	Q3 23	Q4 23
	Non-Ethereum VR	0	0	0	0	0	0	0	0	0	0	0	0
	Ethereum Non-VR	1.5	2.5	2.75	3	3.5	3.75	3	3.5	4	4.25	4.8	5.0
	Non-Ethereum Non-VR	0.25	0.25	0.25	0.5	0.75	0.75	1	1.25	1.5	1.75	2	2.25
	Subtotal	1.8	2.8	3.0	3.8	4.5	5.0	4.8	6.0	7.0	7.5	8.3	8.8
Total		326.8	339.5	349.0	357.5	373.0	400.5	458.0	494.5	515.0	520.0	549.0	606.4

Figure 2.3. Metaverse platforms by type

Source: Mohammed, I. (October, 2023) More Than 600 Million People Use the Metaverse

2.2 CONCEPT OF METAVERSE

The word "Metaverse," which combines the words "meta" and "universe," refers to a virtual environment that incorporates essential technologies like virtual reality and augmented reality to improve performance. From a conceptual standpoint, the Metaverse is a virtual reality environment where users can communicate with one another, have better gaming experiences, provide services, and work together in ways that are comparable to those that occur in the real world. Better client engagement, requirement analysis, and the provision of enhanced visual experiences are all reasons why the Metaverse is becoming more and more significant in business.

The Metaverse, often known as the "internet of experience," is a term used to describe the next version of the Internet that enables users to interact with all five senses using immersive technologies. Neal Stephenson's science fiction book "Snow Crash" from 1992 was the first to

introduce this idea (Xiang, 2022). Through the use of avatars, users can engage in real-time social interactions, gaming, and commerce in the Metaverse, a digital universe where users can immerse themselves in interconnected virtual surroundings (Sanak-Kosmowska, 2023). It seeks to use cutting-edge technologies to imitate the real environment (Chang, 2023).

The banking and finance sectors are expected to be severely disrupted by the Metaverse. Digitalization is essential in today's cutthroat market for improving stakeholder and customer communication, predicting shifting needs, and coming up with creative solutions to support companies in reaching their goals (Oh et al., 2018). Virtual reality (VR) and mixed reality (MR) work together to produce vital digital interactions that improve in-person experiences, opening up a plethora of potential for the sector. The Metaverse's growth potential will be further supported by the integration of AI and 5G technology, which will provide cutting-edge solutions (Alameda, 2020).

The digitalization of financial services has been fueled by continuous IT developments, which have encouraged sustainable expansion and development (Bathla et al., 2021). Through real-time interactions, the Metaverse improves consumer experiences, which benefits the financial services sector. Efficiency, client engagement, and the creation of enhanced virtual interactions are all enhanced by these tools (Liao et al., 2020).

2.3 IMPACT OF USING THE METAVERSE ON FINANCIAL DIGITAL SAFETY

The Metaverse is an innovative digital space that enhances global connections and boosts engagement for both individuals and businesses. By leveraging metaverse technology, banks can forge deeper relationships with their customers, gaining insights into their needs and challenges, ultimately improving their banking experiences. This technology allows financial institutions to incorporate a human touch into the virtual landscape. With the implementation

of advanced analytics, financial services can utilize extensive consumer data to enhance their offerings. Additionally, the Metaverse is fostering the development of innovative financial solutions. One significant challenge organizations face is creating efficient payment systems and future applications may include robotic consulting (Bathla and Awasthi, 2021).

Blockchain services are also expected to gain popularity in the coming years, reflecting the ongoing digital transformation in financial services. Companies can either embed innovation at their core or integrate it within their existing structures. A well-rounded team of engineers can effectively manage innovation while adopting a start-up mindset. Moreover, financial services can harness cloud technology to enhance transparency and collaboration. The Metaverse also opens new pathways for customer engagement, particularly attracting younger audiences interested in NFTs (non-fungible tokens). This shift represents a future where enhanced online interaction occurs through shared virtual environments and three-dimensional avatars (Bathla and Awasthi, 2021).

The potential impact of the Metaverse on society, the economy, and daily life is significant as it evolves and captures a global audience. The integration of financial services within the Metaverse is a crucial area that demands attention. According to Potts (2023), the Metaverse is projected to become a vibrant economic environment featuring diverse virtual businesses and digital assets. Financial services such as asset management platforms, cryptocurrency exchanges, and digital payment systems facilitate economic transactions in this space (Nguyen Thanh et al., 2023). As the user base expands, there is a growing need for advanced and secure financial infrastructures to support this digital universe.

Understanding the role of financial services in the Metaverse is essential for realizing its full potential. Recent studies have highlighted the financial sector's goal of enhancing customer

engagement through AR and VR technologies (Seth & Seth, 2022). These enabling technologies provide an immersive virtual 3D environment, merging different realms (Wohlgenant, Simons, & Stieglitz, 2020). Some research indicates that the Metaverse has the potential to transform banking and promote financial inclusion, especially through neo-banking services, which reduce the need for physical bank visits (Reepu, 2023). The convergence of blockchain, AI, and cutting-edge VR technologies has made this evolution possible.

However, integrating financial services within the Metaverse presents unique challenges, including security concerns like identity theft and privacy invasion (Li et al., 2023). Issues such as cross-platform interoperability (Kshetri, 2022; Huang et al., 2022), regulatory compliance, and user privacy must also be addressed. By tackling these challenges, the Metaverse could revolutionize both real-world financial systems and virtual interactions.

2.3.1 Importance of Metaverse

The metaverse is significantly impacting various industries, including retail, entertainment, education, and healthcare, while simultaneously relying on resources and support from these sectors. As previously mentioned, a fully developed metaverse could create an integrated digital economy valued at \$8 trillion (Goldman Sachs, 2022). For this economy to thrive, it requires infrastructure similar to that of the physical world, leading many companies to invest in areas such as digital identities, avatars, social networking, marketplaces, and blockchain services. Major tech companies like Alibaba, Google, Meta, Microsoft, NVIDIA, Epic Games, and Animoca Brands are at the forefront of these investments, driving innovation and new business models in the metaverse.

Metaverse platforms have the potential to revolutionize customer interactions, particularly in education. They can provide virtual learning environments that enhance

accessibility, engagement, and collaboration among students and educators, offering real-life experiences in a virtual setting.

2.3.2 Impact of Metaverse in Financial World

Assessing the business potential of the Metaverse across various sectors, particularly in finance, is challenging. Its application in the financial world is still emerging, making it difficult to fully gauge its impact. The Metaverse presents several opportunities for the banking sector, such as attracting new customers, increasing revenue, and enhancing the efficiency of financial services. However, realizing this potential requires robust security measures for digital transactions, effective management of rapid technological advancements, and careful handling of personal data in virtual environments. Overall, the Metaverse represents a novel vision for the future. While its precise impact remains uncertain, we can identify both the strengths and weaknesses of this technology in finance.

Opportunities include:

1. **New Revenue Streams:** The economy can expand through increased market transactions by introducing new products and services tied to gaming and cryptocurrency.
2. **Increased Customer Flow:** The Metaverse allows for a more personalized banking experience, which can boost customer loyalty to brands.
3. **Economies of Scale:** VR and AI can create new financial possibilities, reducing the time required for interactions with financial institutions and improving financial inclusion via access to virtual reality and digital currencies.

Weaknesses include:

4. **Security Concerns:** As a new technology, the Metaverse poses significant challenges to the banking sector, which is crucial for a stable economy. Effective regulation is essential to protect customers from fraud and safeguard personal data.

2.3.3 The Metaverse Potential in the Finance Market

The Metaverse represents a novel virtual environment that allows users to interact, communicate, and exist in a digital space of their choosing. While the concept of Meta technology has existed for some time, its feasibility has grown with advances in digitalization. The Metaverse has the potential to revolutionize how we engage in various sectors, particularly in commerce, trade, healthcare, and finance. The increasing demand for digital solutions is driving the growth of the Metaverse within the financial sector. Automation is contributing to the decentralization of global financial markets. According to Wheatley and Bakthavatchalam (2023), the Metaverse is a digital economy that merges cloud computing, AR, VR, MR, 5G, AI, and other technologies to create immersive experiences. At its core, the Metaverse relies on three foundational concepts: virtual reality, Web 3.0, and digital identity.

As the Metaverse expands, it presents both opportunities and challenges for the financial sector. Wheatley (2023) predicts that financial institutions will introduce new digital products and that banking will evolve in response to emerging challenges. To enhance their services, banks must invest significantly in digitalization, making the Metaverse a vital tech solution for scaling operations.

The Metaverse enables financial institutions to:

1. **Redefine Customer Experience:** Through VR and AR, banks can offer immersive experiences where users perform transactions as personalized avatars.
2. **Enhance Engagement:** Virtual banking allows users to access services in an online financial realm, leading to personalized marketing and branding strategies.
3. **Understand Customer Needs:** Tailored financial services can be developed based on customers' specific needs and objectives, improving market segmentation.
4. **Foster Innovation:** The Metaverse facilitates the introduction of new financial services, driven by a better understanding of customer preferences and the adoption of new technologies.

Although the Metaverse's business potential in finance is still emerging, it offers opportunities for increased customer flow, revenue growth, and service efficiency. However, to harness these benefits, financial institutions must prioritize security, manage personal data effectively, and adapt to rapid technological changes.

In conclusion, while the Metaverse offers a transformative vision for the future of finance, its full impact remains uncertain. It presents both strengths and weaknesses, including new revenue streams and increased customer engagement, but also challenges related to regulation, security, and privacy. Financial institutions must navigate these dynamics carefully as they explore the opportunities presented by this evolving digital landscape.

2.3.4 The Finance World in Development Through Metaverse

Wheatley (2023) anticipates that in 2023, financial institutions will create new digital products, enabling continued growth in banking as they address existing challenges. Global regulations are expected to lead to more equitable legislation regarding cryptocurrency transactions. To enhance their services, banks must increase their investments in digitalization,

positioning the Metaverse as a crucial technological solution for scaling the banking and financial sectors.

Through the Metaverse, financial institutions can:

- **Redefine Customer Experience:** By leveraging VR and AR, the financial sector can provide customers with immersive experiences, allowing them to conduct financial activities through unique personal avatars.
- **Enhance Engagement:** Virtual banks within the Metaverse enable customers to perform transactions and access services in a digital financial environment, which enhances marketing and branding through personalized experiences.
- **Gain Insight into Customer Needs:** Financial services can be tailored to individual customers as they express their preferences and goals, making it easier to categorize them into well-defined segments.
- **Foster Innovation:** The Metaverse simplifies the introduction of new financial services, facilitating innovation by aligning with customer needs and integrating emerging technologies in the banking sector.

2.4 ADVANTAGES AND DISADVANTAGES FOR FINANCIAL SERVICE COMPANIES BROUGHT BY THE METAVERSE

Fintech era 2.0 marked a significant shift for financial institutions, enabling the introduction of electronic services while also paving the way for tech companies to enter the financial sector. The 2008 global financial crisis spurred the emergence of cryptocurrencies and blockchain technology, significantly impacting finance by fostering decentralized finance, which could reduce reliance on intermediaries (Ernst & Young, 2023). New entrants, such as

tech startups and fintech firms, have focused on customer needs, altering expectations from traditional financial institutions. Their business models prioritize excellent service, customer loyalty, data analytics, and capital networks, allowing them to overcome traditional barriers like size and market concentration. Since 2008, numerous digital banking and non-banking institutions have emerged, including Robinhood (2013), Bondora (2008), and PayPal (2008), challenging traditional banks and leading to decreased profitability. McKinsey & Company (December 2022) projects that banks' return on equity may dip below 7.2%, necessitating adaptations in their business models to sustain profitability.

The Metaverse presents opportunities for traditional and emerging financial institutions, including tech and fintech firms, to drive innovation and actively shape the future of finance. Key advantages of the Metaverse for these institutions include:

1. **Brand Perception:** As the gaming industry surpasses the film industry (Mordor Intelligence, 2023), financial institutions can enhance their image by establishing a presence in gaming environments, appealing to younger generations as innovative entities.
2. **Customer Interaction:** The Metaverse facilitates various interaction methods, such as virtual reality (VR), augmented reality (AR), and physical branches. A survey revealed that 42% of respondents valued omnichannel availability, with additional preferences for ease of use and accessibility (Digital Banking Report, 2022). Nearly half of customers seek personalized services and support.
3. **Cryptocurrency Insights:** The Metaverse enables financial institutions to stay informed about cryptocurrency developments, as these currencies are essential for

commerce within virtual environments. Platforms like Sandbox (SAND) and Decentraland (MANA) have significant market caps (Forbes Advisor, 2023).

4. **Enhanced Customer Experience:** Utilizing 3D virtual reality can improve transaction processes, advisory services, and employee training, ultimately leading to better service delivery.
5. **Increased Customer Engagement:** The Metaverse allows for personalized customer experiences and tailored product offerings, fostering deeper connections beyond traditional financial interactions.
6. **Competitive Edge:** Collaborations between financial institutions and fintech companies are on the rise, with partnerships increasing from 51% to 60% in 2023 (Digital Banking Report, 2023).

Historically, the financial services sector has evolved with technologies like Diners Club and ATMs. The Metaverse, alongside blockchain, facilitates ownership of digital assets, necessitating guidance from financial advisors in this new landscape. Institutions are gearing up for Web3 financial products, including Metaverse index funds, ETFs, and NFTs (CoinDesk, 2023).

The disadvantages of entering the Metaverse include regulatory and safety risks, as the unregulated environment increases the potential for fraud and theft of digital assets (Banking Hub, 2022). Other concerns involve privacy breaches from cyber threats, technological obstacles, and potential physical health issues for employees using VR/AR technologies. Additionally, the volatility of cryptocurrencies may deter customers.

2.5 FINANCIAL SERVICES' PRESENCE IN THE METAVERSE

Large digital finance platforms are already transforming the financial services sector. Embroidered financial services into digital platforms are already present which transform how banking, wealth management, and insurance companies operate. The development of the Banking-as-a-service model clearly explains how banks and their services evolved towards the new digital platform economy. Furthermore, financial institutions around the world acquire tech companies, partner with them or through joint ventures and strategic alliances create digital solutions and offer them in the digital economy. Nevertheless, even though financial institutions are following the trends and responding to the new entrants from the Fintech Era 3.0, they lack human interaction. Digital tools and services are customers based on their preferences and behaviors, but do not watch closely the direct interaction with clients, their incentives, alternatives, etc. Metaverse fills in this gap and offers a worthier customer experience by upgrading their online presence.

According to Banking Hub (October, 2022) and the empirical evidence related to existing financial institutions in the metaverse, financial institutions currently are focusing on establishing their presence in the metaverse, connecting with new clients, and offering client support to new and existing customers. In this respect, financial institutions, and more specifically banking financial institutions, are (re)building relations with them by educating and informing them on crypto currencies, exchange rates, stock prices, institutions' research projects, sustainability, banking services, etc. While digital and mobile banking was intended to dislocate customers from brick-and-mortar branches and enable them 24/7 banking services outside banks' premises, banking in the metaverse, tries once again to reestablish relations with customers with the one-to-one approach in the virtual world.

Institution	Association	Platform	Key Activities
HSBC	Partnership	The Sandbox	Sports/gaming engagement, bill payments
JP Morgan Chase	-	Decentraland	Virtual branch (project showcases)
Standard Chartered	Partnership	The Sandbox	Client experience experiments
Bank of America	-	VR World	Employee training
Kookmin Bank	-	VR World	Banking activities, youth finance education
DBS Bank	Partnership	The Sandbox	Sustainability promotion
TD Bank	-	VR World	Internship training
RBC	Partnership	Roblox	Financial literacy for youth
Fidelity Investments	Partnership	Decentraland	Investor education (incl. FMET ETF)
CaixaBank	Partnership	ImaginLand/Decentraland	Cultural/tech experiences
Sokin	Independent	Own Metaverse	Commerce hub (fashion/sports transactions)

Figure 2.4. Examples of financial institutions present in the metaverse
Source: Our own research

Recent insights from Profinch (2022) indicate varying perspectives among financial institutions regarding the adoption of augmented reality (AR) and virtual reality (VR) for transactions. Specifically, 9% of respondents believe customers will never use AR/VR for this purpose, 13% anticipate its use by 2025, 34% by 2030, and 44% expect it to become common after 2030. Furthermore, the Digital Banking Report (2023) outlines key trends for retail banking in 2023 compared to 2021, emphasizing that banks will continue prioritizing customer-centric strategies and expanding their digital product offerings. This shift aims to enhance the consumer banking experience by removing existing barriers.

It is evident that financial institutions recognize the need to meet customer expectations by providing unique experiences. The traditional model of simple mobile apps and websites is no longer sufficient; instead, banks should focus on creating personalized, human-centered digital experiences. As noted by MIT Sloan Management Review (2022), while making online shopping quicker and easier is essential, brands must also foster meaningful interactions with customers. This emphasis on digital humanization distinguishes truly innovative brands from those merely trying to keep pace.

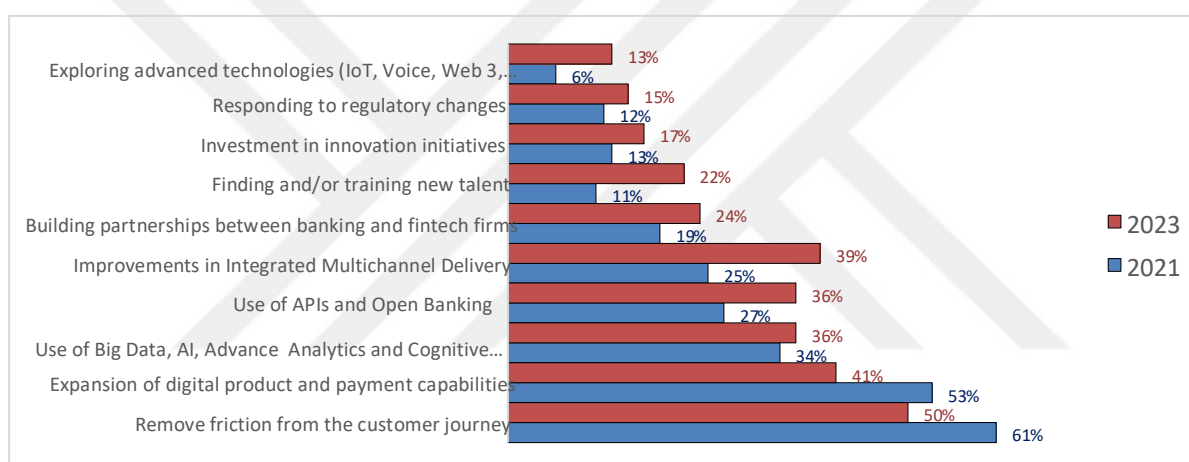


Figure 2.5. Top trends in retail banking projected in 2023 vs. 2021

Source: Digital Banking Report (January, 2023). Retail Banking Trends and Priorities 2023. Financial Brand

There has been a significant increase in trends related to the use of Big Data, AI, advanced analytics, cognitive computing, APIs, and open banking, alongside enhancements in integrated multichannel delivery, investments in innovation, and the exploration of advanced technologies such as IoT, voice, Web 3, and the metaverse. Consequently, there is a strong emphasis on fostering partnerships between banks and fintech firms, as well as adapting to regulatory changes. Financial institutions are increasingly collaborating with tech startups or major tech companies to develop innovative digital products. Additionally, many

banks and non-bank financial entities are creating their own digital platforms and metaverse experiences that extend beyond traditional financial services.

Reports indicate that financial institutions recognize the potential of the metaverse; however, they are currently "waiting in the lounge" for regulatory changes. Numerous digital standards need to be established to ensure privacy and customer identity (KYC), safeguard customer assets from fraud, and enable fiat currencies to interact with blockchain networks for NFT purchases (Liquin & Dogan, 2022). By fully embracing the metaverse, financial institutions are entering a new realm of "metafinance," which encompasses financial services tailored for virtual worlds, including financing for virtual real estate and assets, as well as facilitating fund transfers between traditional bank accounts and the metaverse (Banking Hub, 2022).

2.6 METAVERSE FOR CORPORATE BANKING

Banking institutions facilitate transactions and give firms and individuals access to credit, banking services are vital to the economy (Mogaji et al., 2018). These services are typically divided into two categories: corporate banking for businesses and retail banking for consumers. It is crucial to evaluate the possibility of corporate banking in the metaverse, even though retail banking might be more appropriate for this setting. Corporate banking may be able to reduce the risks associated with financial speculation by taking advantage of the special qualities of metaverses. As demonstrated by platforms such as Second Life, where Linden Lab controls currency stability by adjusting Linden Dollar supply in response to demand, this industry may aid in exchange rate stabilization (Vidal-Tomás, 2023).

Technologies like VR and AR are being utilized in the metaverse to enhance business functions, including the creation of virtual bank branches (Depari et al., 2022). For example,

Shoolapani and Jinka (2011) designed a virtual branch in Open Wonderland to assist customers with inquiries. The viability of corporate banking in the metaverse is supported by the increasing user interaction in 3D environments via virtual reality (Falchuk et al., 2018; Dwivedi et al., 2020), driven by technological advancements and the rise of the experience economy (Maiya, 2022). JP Morgan estimates that corporate opportunities in the metaverse could generate over \$1 trillion annually (Dwivedi et al., 2022a).

The evolving role of customer-facing staff will be critical in utilizing metaverse technology to enhance the banking experience, especially for clients unfamiliar with these tools (Tyler and Stanley, 2001). Additionally, banks can explore non-fungible tokens (NFTs) as investment assets, potentially creating mutual funds for NFT investments (Bushnell, 2022).

2.6.1 Metaverse for Retail Banking

The metaverse holds significant potential to disrupt and transform various industries (Koohang et al., 2023), with many financial institutions beginning to explore its possibilities, particularly in retail banking. Notable examples include JP Morgan, CaixaBank, and DBS Bank, which are using the metaverse to engage and educate their clients (Global Finance, 2023). While the metaverse can enhance operational efficiency for banks, it also presents challenges that must be navigated carefully.

For managers, the metaverse's broad applicability makes it attractive, impacting everything from individual customer interactions to company-wide operations. However, the integration of banking services into the metaverse may yield substantial growth opportunities, but failing to address associated challenges could lead to complications.

Digital asset transactions, such as cryptocurrencies and virtual real estate, are common in the metaverse (Forbes, 2022). Banks can target new demographics, including gamers and tech enthusiasts, by offering specialized products and services tailored for the metaverse. Unlike traditional e-banking, which lacks personal engagement, the metaverse facilitates more humanized interactions through customizable avatars and lifelike exchanges, enabling co-creation between clients and banks. For instance, JP Morgan has launched the Onyx Lounge in Decentraland, allowing streamlined transactions and secure asset management (Raj, 2022).

2.6.2 Challenges Associated with Corporate Banking in the Metaverse

The increased technological complexity of corporate finance in the metaverse is a major obstacle (Reynolds, 2008). Although this intricacy might improve user experiences, it can also make navigating challenging and less user-friendly. For corporate bankers who have made investments in developing virtual banking environments, this could discourage commercial clients from using the metaverse. The efficacy of these expenditures is questioned if clients are incapable or unwilling to engage.

Another issue is keeping clients interested in the metaverse. For example, there is little activity in JP Morgan's Onyx Lounge in Decentraland, which gives the impression that it is more of a placeholder than a lively venue for banking transactions. It becomes difficult to draw in busy corporate clients if they find the setting uninteresting. To guarantee successful client involvement, corporate bankers must evaluate their metaverse investments rigorously (Mogaji and Nguyen, 2022a).

Other issues include responsiveness, perceptions of co-presence, and ease of use (Gadalla et al., 2013; Abdulquadri et al., 2021). Consumers have higher expectations for responsiveness since they anticipate an offline-like experience from avatars. Furthermore, clients' global reach poses security and accessibility issues, particularly for those in areas with

inadequate internet connectivity. Although a lot of users could be keen to interact with the metaverse, structural problems might keep them from doing so.

2.7 APPRAISAL OF LITERATURE REVIEW

The idea of the Metaverse and its effects on the financial system—a vital pillar of any economy—are examined in this paper. Building a new digital financial infrastructure is crucial as economies move more and more toward digitalization and create parallel platform economies. The Metaverse mirrors the physical economy and promotes rapid growth by bringing together businesses from a variety of industries, including marketing, real estate, healthcare, and education. Financial institutions are actively interacting with the Metaverse by setting up accounts on different platforms or developing their own virtual worlds, especially in industrialized nations. This approach enables them to investigate decentralized finance, improve interoperability with alternative currencies, and try out novel approaches to engaging with Generation Z and Alpha clients.

The potential advantages, possibilities, and difficulties for financial organizations are substantial, even if the Metaverse's existing offerings mostly concentrate on information, education, and customer service. Established institutions are being forced to supply crucial financial expertise, create regulatory regulations, and encourage good investment practices inside the Metaverse economy as a result of new entrants that are already upending the financial landscape. The study looks at how the Metaverse affects money, emphasizing how developments in AI and VR affect the banking industry. It lists the benefits and drawbacks of incorporating the Metaverse into the financial industry, highlighting how it could speed up and ease digitization in the years to come.

CHAPTER THREE

3.0 RESEARCH METHOD AND PROCEDURE

This chapter discusses the methodology employed to carry out the study. It also consists of; research design, population of the study, sample and sampling techniques, instrumentation, validity of the instrument, procedure for data collection and description of respondents and method of data analysis.

3.1 RESEARCH DESIGN

This study employed a quantitative survey design to examine financial digital safety perceptions in the metaverse. Participants rated their agreement with security-related statements using a 4-point Likert scale (Strongly Agree to Strongly Disagree), enabling ordinal data analysis. The design facilitated examination of relationships between metaverse usage levels and perceived financial safety, while revealing sector-specific adaptation challenges through statistical evaluation.

3.2 SAMPLE AND SAMPLING TECHNIQUE

A statistically significant sample of 350 participants was selected through simple random sampling, ensuring equal selection probability. The sample comprised three distinct user groups:

- Tech-savvy users (comfortable with advanced digital transactions)
- Moderately skilled users (basic metaverse transaction capability)
- Novice users (limited digital platform experience)

This stratification allowed for comparative analysis across technical proficiency levels while maintaining randomization integrity.

3.3 RESEARCH INSTRUMENTATION

The study utilized a structured questionnaire with four thematic sections:

Section A: Demographic and socioeconomic profiling

Section B: Trust and security enhancement mechanisms (20 items)

Section C: Key safety-enhancing factors

Section D: Effective security solutions

The instrument employed closed-ended questions with a 4-point Likert response scale, optimized for participant engagement and analytical clarity. Development drew upon Hemantha's (2021) and Li et al.'s (2023) validated constructs, with additional categorization by ISCED education levels (0-5 = basic/intermediate; 6-8 = advanced) to strengthen statistical power.

3.4 PROCEDURE FOR DATA COLLECTION

Fieldwork commenced on January 4, 2025, with a team of two trained research assistants administering all 350 questionnaires through direct contact. The standardized protocol included:

- Participant briefing on research objectives
- Guided questionnaire completion
- Immediate collection to ensure 100% retrieval

Geographical distribution of respondents was determined by residential location to maintain sample diversity.

3.5 DATA ANALYSIS

The analytical approach incorporated:

1. **Descriptive Statistics:** Frequency distributions for demographic data
2. **Inferential Analysis:**
 - Chi-square tests for ordinal-nominal variable relationships
 - Fisher's exact test for small expected cell frequencies (<5)
3. **Reliability Assessment:** Cronbach's alpha ($\alpha \geq 0.70$ benchmark)

Three null hypotheses guided the analysis:

Null Hypothesis

H₀₁: The level of metaverse usage has no significant effect on financial digital safety; the two are independent.

H₀₂: There is no significant relationship between financial digital safety and metaverse usage.

H₀₃: There is no significant relationship between effective solutions and the security and reliability of financial interactions in the emerging digital environment.

3.6 Ethical and Operational Considerations

The study implemented quality control measures through:

- Research assistant training on standardized administration
- Privacy protection protocols
- Systematic data handling procedures

This methodological rigor ensured both the validity of collected data and the ethical integrity of the research process.

CHAPTER FOUR

4. PRESENTATION OF RESULTS AND DISCUSSION

4.1 PREAMBLE

This chapter presents the results obtained from the administered questionnaire. The results are presented in relation to the research questions and hypotheses.

4.2 PRESENTATION AND ANALYSIS OF DATA

Table 4.1. Socio-Demographic Characteristics

Demographic Characteristics	Frequency	Percentage
Age of Respondents		
18-30	116	33.1
31-45	110	31.4
Above 45	124	35.4
Gender		
Male	168	48.0
Female	182	52.0

Table 4.1 shows the socio-demographic characteristics of respondents. One third each (33.1%), (31.4%), (35.4%) were between the age range of 18-30, 31-45 and >45 years and about half of the respondents (52.0%) were female.

4.2.1 Research Question One:

Research Question 1: How does financial digital safety enhance trust, security, and stability in the metaverse?

Hypothesis 1 (H_{01}): The level of metaverse usage does not significantly affect financial digital safety.

Method: To address this research question and test the associated hypothesis, a structured questionnaire was administered, focusing on respondents' perceptions of trust, security, and stability in the metaverse. Responses were collected using a four-point Likert scale (Strongly

Agree, Agree, Disagree, and Strongly Disagree) on various items related to financial digital safety.

Results:

Table 4.2. Respondents' Views On Financial Digital Safety Enhancing Trust, Security, And Stability In The Metaverse

Items	Strongly Agree	Agree	Disagree	Strongly Disagree
I think metaverse will revolutionize the financial system	165(47.1)	122(34.8)	38(10.8)	25(7.1)
I think metaverse enhance financial inclusion.	187(53.4)	110(31.4)	41(11.7)	12(3.4)
I am critical of the long-term sustainability of metaverse.	141(40.2)	136(38.8)	52(14.8)	21(6.0)
I find metaverse a speculative and volatile asset class.	196(56.0)	131(37.4)	14(4.0)	9(2.6)
I find environmental concerns of using metaverse problematic.	174(49.7)	151(43.1)	19(5.4)	4(1.1)
I am concerned about the risk of fraud related to using metaverse.	206(58.9)	116(33.1)	20(5.7)	8(2.3)
I am concerned with criminals exploiting metaverse for illegal activities	198(56.6)	132(37.7)	20(5.7)	0(0.0)
I trust the technology underlying metaverse.	158(45.1)	129(36.9)	51(14.6)	12(3.4)
I think metaverse are a reliable and secure form of online payment.	186(53.1)	146(41.7)	18(5.1)	0(0.0)
I'm concerned about the possibility of scams and frauds related to metaverse.	210(60.0)	115(32.9)	16(4.6)	9(2.6)
I trust the technology that makes metaverse.	196(56.0)	151(43.1)	2(0.6)	1(0.3)
I believe that metaverse will change the way we handle money and banking.	200(57.1)	117(33.4)	17(4.9)	16(4.6)

I'm worried about a potential negative impact on the environment caused by cryptocurrencies.	194(55.4)	126(36.0)	20(5.7)	10(2.9)
--	-----------	-----------	---------	---------

(Table 4.2. continued)

I think metaverse can help more people access and use financial services.	216(61.7)	125(35.7)	7(2.0)	2(0.6)
---	-----------	-----------	--------	--------

I think there are enough rules and regulations for using metaverse.	177(50.6)	141(40.3)	19(5.4)	13(3.7)
---	-----------	-----------	---------	---------

I find metaverse to be risky because their value can change a lot.	164(46.8)	120(34.3)	42(12.0)	24(6.8)
--	-----------	-----------	----------	---------

I find it easy to understand and use metaverse.	179(51.1)	136(38.8)	24(6.8)	9(2.6)
---	-----------	-----------	---------	--------

I have doubts about whether cryptocurrencies through metaverse will last for a long time.	184(52.6)	130(37.1)	19(5.4)	17(4.8)
---	-----------	-----------	---------	---------

I believe that metaverse are a safe and reliable way to make payments online.	159(45.4)	126(36.0)	43(12.3)	22(6.3)
---	-----------	-----------	----------	---------

I'm worried that criminals might use cryptocurrencies through metaverse for illegal activities."	218(62.3)	132(37.7)	0(0.0)	0(0.0)
--	-----------	-----------	--------	--------

I think there are too few situations where metaverse can be used.	193(55.1)	131(37.4)	16(4.6)	10(2.8)
---	-----------	-----------	---------	---------

People in my social circle encourage the usage of cryptocurrencies through metaverse	188(53.7)	114(32.6)	30(8.6)	18(5.1)
--	-----------	-----------	---------	---------

I find a limited number of use cases to cryptocurrencies via metaverse "	170(48.6)	134(38.3)	25(7.1)	21(6.0)
--	-----------	-----------	---------	---------

I find the process of using metaverse difficult to navigate"	182(52.0)	123(35.1)	36(10.3)	9(2.6)
--	-----------	-----------	----------	--------

My social network is encouraging of the usage of metaverse	169(48.3)	146(41.7)	25(7.1)	10(2.8)
--	-----------	-----------	---------	---------

I find the lack of proper regulations of metaverse problematic.	204(58.3)	113(32.3)	21(6.0)	12(3.4)
---	-----------	-----------	---------	---------

Summary of Findings (Based on Table 4.2): Table 4.2 demonstrates how financial digital safety improves metaverse stability, security, and trust. While 56.0% of respondents strongly agree that they found the metaverse to be a speculative and volatile asset class, 49.7% strongly agree that they found the environmental concerns of using the metaverse problematic, and 58.9% strongly agree that they were concerned about the risk of fraud related to using the metaverse, 47.1% of respondents strongly agree that the metaverse would revolutionize the financial system and 53.4% strongly agree that it would enhance financial inclusion.

In a similar vein, over half of the respondents (56.6%) strongly confirmed that they were also concerned about criminals using the metaverse for illicit purposes, and 53.1% strongly stated that they believed the metaverse to be a safe and dependable way to make payments online. Meanwhile, roughly two-thirds of the respondents (60.0%) strongly acknowledged the possibility of scams and frauds related to the metaverse, 56.0% strongly attested that they trust the technology that creates the metaverse, and roughly the same percentage of respondents (57.1%) strongly believed that the metaverse would revolutionize banking and money management. Additionally, nearly two-thirds of the respondents firmly believed that the metaverse will transform the way that money and banking were handled, and more than half of the participants (55.4%) voiced serious concerns about the potential negative environmental implications of crypto currencies. Furthermore, while half of the respondents (50.6%) strongly agreed that they believed there were enough rules and regulations for using the metaverse, more than half of the respondents (55.4%) strongly stated they were concerned about a potential negative impact on the environment caused by crypto currencies, and roughly two thirds (61.7%) strongly agreed that they believed the metaverse could help more people access and use financial services. Of the respondents, 52.6% strongly affirmed that they had doubts whether or not crypto currencies through the metaverse would be around for a long time.

Additionally, over two-thirds of respondents (62.3%) expressed a strong concern that criminals might use crypto currencies through the metaverse for illegal purposes, 53.7% strongly believed that members of their social circle encouraged the use of crypto currencies through the metaverse, and roughly the same percentage of respondents (52.0%) strongly agreed that they found the metaverse's navigation challenging. Finally, (48.3%) of the respondents strongly agree that their social network is encouraging of the usage of metaverse and more than half of the respondents (58.3%) strongly claimed that they found the lack of proper regulations of metaverse problematic.

H₀₁: ANALYSIS OF HYPOTHESIS ONE

Table 4.3. Comparison Between Level Of Metaverse Usage And Financial Digital Safety

Variable	Mean	T	p-value	Confidence interval	
				Lower	Upper
Level of usage	0.40	2.012	0.084	-0.410	1.031
High level	38.30				
Low level	18.61				

Interpretation of Table 4.3:

- The mean for high usage was 38.30 and for low usage was 18.61.
- The t-test result ($t=2.012$, $p=0.084$) shows that there is no statistically significant difference between the level of metaverse usage and financial digital safety (since $p > 0.05$).

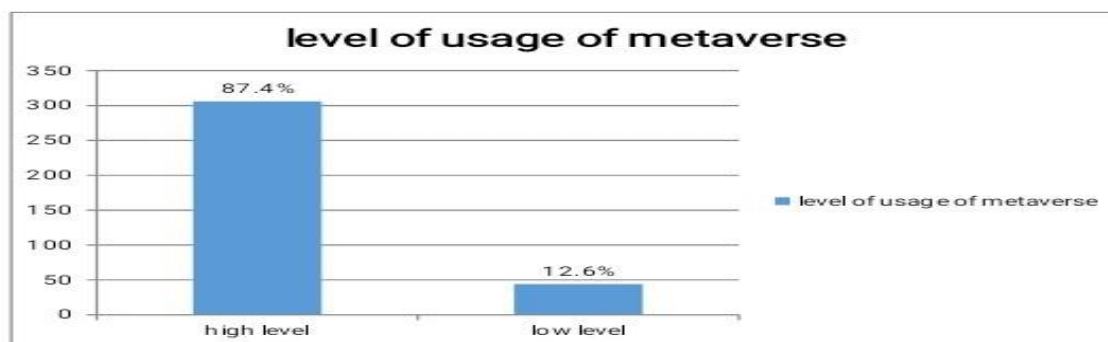


Figure 1: Overall level of usage of metaverse.

Figure 1 shows the overall level of usage of metaverse. More than two third of the respondents 87.4% had a high level of usage of metaverse while 12.6%% of them had a low level of usage.

4.2.2 Answer to Research Question Two:

Research Question Two: What key factors contribute to enhancing financial digital safety within the metaverse?

Hypothesis Two: There is no significant relationship between financial digital safety and the usage of the metaverse.

Method: Respondents were asked to evaluate various factors that could enhance financial digital safety within the metaverse. Their levels of agreement were measured and summarized in Table 4.4. Additionally, the relationship between financial digital safety and the use of the metaverse was examined, with results presented in Table 5.

Results:

Table 4.4. Key Factors Contribute To Enhancing Financial Digital Safety Within The Metaverse

Items	Strongly Agree	Agree	Disagree	Strongly Disagree
Utilizing advanced encryption methods to protect financial transactions and personal data.	199(56.8)	126(36.0)	17(4.8)	8(2.3)

(Table 4.4. continued)

Implementing MFA to ensure only authorized users can access accounts and make transactions.	209(59.7)	132(37.7)	3(0.8)	1(0.3)
Leveraging blockchain for secure and transparent transaction records.	182(52.0)	117(33.4)	27(7.7)	18(5.1)
Conducting regular security audits to identify and fix vulnerabilities.	210(60.0)	124(35.4)	10(2.8)	6(1.7)
Ensuring that applications and platforms are built with secure coding standards.	194(55.4)	110(31.4)	24(6.8)	22(6.3)
Auditing and securing smart contracts to prevent vulnerabilities.	183(52.3)	133(38.0)	17(4.8)	17(4.8)
Providing comprehensive education to users on recognizing and avoiding scams and phishing attacks.	213(60.8)	128(36.6)	1(0.3)	0(0.0)
Implementing robust identity verification processes to prevent fraudulent activities.	179(51.1)	120(34.3)	38(10.8)	13(3.7)
Adhering to financial regulations and standards to ensure legal compliance and user protection.	201(57.4)	116(33.1)	15(4.3)	18(5.1)
Ensuring strong data privacy measures are in place to protect user information.	203(58.0)	141(40.3)	4(1.1)	2(0.6)
Having a well-defined incident response plan for quick and effective handling of security breaches.	215(61.4)	110(31.4)	18(5.1)	7(2.0)
Using AI and machine learning to detect and mitigate fraudulent activities in real-time.	186(53.1)	137(39.1)	17(4.8)	20(5.7)
Implementing AML protocols to detect and prevent money laundering activities.	170(48.6)	132(37.7)	26(7.4)	22(6.3)

(Table 4.4. continued)

Defining and enforcing user access levels to sensitive data and financial tools.	184(52.6)	122(34.8)	22(6.3)	22(6.3)
Ensuring interoperability standards to maintain secure transactions across different platforms.	196(56.0)	134(38.3)	13(3.7)	7(2.0)
Implementing continuous monitoring systems to detect and respond to suspicious activities.	202(57.7)	118(33.7)	18(5.1)	12(3.4)
Offering or requiring cyber insurance to mitigate financial losses from cyber-attacks.	181(51.7)	125(35.7)	33(9.4)	11(3.1)
Regularly conducting penetration tests to identify and address security weaknesses.	197(56.3)	112(32.0)	21(6.0)	20(5.7)
Ensuring DeFi platforms are secure and resilient against attacks.	184(52.6)	138(39.4)	17(4.8)	20(5.7)
Providing mechanisms for users to report suspicious activities or security issues.	208(59.4)	113(32.3)	24(6.8)	5(1.4)

Summary of Findings (Based on Table 4.4): Table 4.4 shows the Key factors contribute to enhancing financial digital safety within the metaverse. (56.8%) of the respondents strongly agree that utilizing advanced encryption methods to protect financial transactions and personal data were among the key factors to enhancing digital safety within the metaverse and about two third of the respondents (59.7%) also strongly agree that implementing MFA to ensure only authorized users can access accounts and make transactions were also a key factors contributing to enhancing financial digital safety within the metaverse while (52.0%) strongly claimed that leveraging blockchain for secure and transparent transaction records were also among the key

factors contributing to enhancing financial digital safety within the metaverse, two third of the respondents (60.0%) strongly affirmed that conducting regular security audits to identify and fix vulnerabilities were among the key factors contributing to enhancing financial digital safety within the metaverse and (55.4%) strongly acknowledged that ensuring that applications and platforms are built with secure coding standards were also among the key factors contributing to enhancing financial digital safety within the metaverse while (52.3%) of the respondents strongly affirmed that auditing and securing smart contracts to prevent vulnerabilities were also a key factors contributing to enhancing financial digital safety within the metaverse.

Also, about two third of the respondents (60.8%) strongly agree that providing comprehensive education to users on recognizing and avoiding scams and phishing attacks were also a key factors contributing to enhancing financial digital safety within the metaverse and (57.4%) strongly agree that adhering to financial regulations and standards to ensure legal compliance and user protection were also a key factors contributing to enhancing financial digital safety within the metaverse and (58.0%) of the respondents strongly attested that ensuring strong data privacy measures in place to protect user information were also a key factors contributing to enhancing financial digital safety within the metaverse while (61.4%) strongly agree that having a well-defined incident response plan for quick and effective handling of security breaches were also among key factors contributing to enhancing financial digital safety within the metaverse, (52.6%) of the respondents strongly claimed that defining and enforcing user access levels to sensitive data and financial tools were also among key factors contributing to enhancing financial digital safety within the metaverse and (56.0%) strongly affirmed that ensuring interoperability standards to maintain secure transactions across different platforms were among key factors contributing to enhancing financial digital safety within the metaverse.

In addition, (57.7%) of the respondents strongly agree that implementing continuous monitoring systems to detect and respond to suspicious activities were among key factors contributing to enhancing financial digital safety within the metaverse and about same proportions (51.7%) strongly affirmed that offering or requiring cyber insurance to mitigate financial losses from cyber-attacks were among key factors contributing to enhancing financial digital safety within the metaverse while (56.3%) of the respondents strongly believed that regularly conducting penetration tests to identify and address security weaknesses were a key factors contributing to enhancing financial digital safety within the metaverse.

Finally, about half of the respondents (52.6%) strongly agree that ensuring DeFi platforms are secure and resilient against attacks were a key factors contributing to enhancing financial digital safety within the metaverse and more than two third of the respondents (59.4%) strongly claimed that providing mechanisms for users to report suspicious activities or security issues were a key factors contributing to enhancing financial digital safety within the metaverse.

H₀₂: ANALYSIS OF HYPOTHESIS TWO

Table 4.5. Comparison Of The Financial Digital Safety And The Usage Of Metaverse

Variable	Mean	Std. dev	F	Sig
Digital Safety			1.717	0.061
Good safety	38.90	8.21		
Poor safety	16.54	2.16		

Interpretation of Table 4.5: Table 4.5 shows the comparison between financial digital safety and the usage of the metaverse. Respondents with good digital safety practices had an average score of 38.90, while those with poor practices had an average score of 16.54. However, the

analysis revealed that the difference between the groups was not statistically significant ($F = 1.717, p = 0.061$).

Thus, Hypothesis Two is accepted, confirming that there is no significant relationship between financial digital safety and the usage of the metaverse.

4.2.3 Answer to Research Question Three:

Research Question Three: What are the effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment?

Hypothesis Three: There is no significant relationship between the effective solutions that can ensure secure and reliable financial interactions in the emerging digital environment.

Method: Respondents were asked to assess the effectiveness of several proposed solutions for ensuring secure and reliable financial interactions in the emerging digital environment. Their responses were summarized in Table 4.6. Additionally, the relationship between the implementation of these solutions and financial security was analyzed, with the results presented in Table 7.

Results:

Table 4.6. Effective Solutions That Can Ensure Secure And Reliable Financial Interactions In This Emerging Digital Environment

Items	Strongly Agree	Agree	Disagree	Strongly Disagree
Implementing strong encryption methods for data in transit and at rest to protect sensitive information from unauthorized access.	214(61.1)	131(37.4)	4(1.1)	1(0.3)
Requiring two forms of identification (e.g., password and a mobile phone code) to enhance security for online transactions.	205(58.6)	137(39.1)	6(1.7)	0(0.0)

(Table 4.6. continued)

Utilizing blockchain for its decentralized and tamper-proof ledger capabilities to secure financial transactions and reduce fraud.	189(54.0)	126(36.0)	20(5.7)	15(4.3)
Using biometric data (fingerprints, facial recognition, etc.) to verify identities and enhance security over traditional passwords.	211(60.3)	116(33.1)	14(4.0)	9(2.6)
Adhering to regulatory standards and frameworks such as GDPR, PCI-DSS, and AML to ensure legal compliance and protect consumer data.	233(66.6)	110(31.4)	4(1.1)	3(0.8)
Deploying AI and ML algorithms to detect and prevent fraudulent activities by analyzing transaction patterns and identifying anomalies.	211(60.3)	121(34.6)	10(2.8)	8(2.3)
Ensuring that APIs used for financial transactions are secure, with proper authentication, encryption, and regular security testing.	198(56.6)	134(38.3)	14(4.0)	4(1.1)
Educating users about the importance of strong passwords, recognizing phishing attempts, and other security best practices.	214(61.1)	125(35.7)	6(1.7)	5(1.4)
Conducting regular security audits and vulnerability assessments to identify and fix potential weaknesses in the system.	192(54.8)	128(36.6)	20(5.7)	10(2.8)
Offering cybersecurity insurance to cover potential losses and developing comprehensive risk management strategies.	206(58.8)	133(38.0)	6(1.7)	3(0.8)
Here are five additional solutions to enhance secure and reliable financial interactions in the digital environment:	186(53.1)	111(31.7)	27(7.7)	26(7.4)
Replacing sensitive data with unique identification symbols (tokens) that retain essential information without compromising security. This is particularly useful for protecting payment card information.	209(59.7)	107(30.6)	19(5.4)	15(4.3)

(Table 4.6. continued)

Monitoring user behavior to establish a baseline of normal activities and quickly detect deviations that may indicate fraudulent activity.	216(61.7)	132(37.7)	2(0.6)	0(0.0)
Incorporating security into the software development lifecycle (SDLC) by following best practices such as secure coding, code reviews, and penetration testing.	223(63.7)	121(34.6)	6(1.7)	0(0.0)
Requiring multiple signatures for transaction approval, which adds an extra layer of security by distributing the authority among several parties.	211(60.3)	133(38.0)	6(1.7)	0(0.0)

Summary of Findings (Based on Table 4.6): Table 4.6 shows the effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment. About two third of the respondents (61.1%) strongly agree that implementing strong encryption methods for data in transit and at rest to protect sensitive information from unauthorized access were among the effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment and (58.6%) strongly agree that requiring two forms of identification (e.g., password and a mobile phone code) to enhance security for online transactions were also among the effective solutions that can ensure, secure and reliable financial interactions in this emerging digital environment while (54.0%) of the respondents strongly affirmed that utilizing blockchain for its decentralized and tamper-proof ledger capabilities to secure financial transactions and reduce fraud were among the effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment, two third of the respondents (60.3%) strongly agree that using biometric data (fingerprints, facial recognition, etc.) to verify identities and enhance security over traditional passwords were effective solutions that can ensure secure and reliable financial interactions in this emerging

digital environment and more than two third of the respondents (66.6%) strongly acknowledged that adhering to regulatory standards and frameworks such as GDPR, PCI-DSS, and AML to ensure legal compliance and protect consumer data were effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment.

More so, about two third of the respondents (60.3%) strongly agree that deploying AI and ML algorithms to detect and prevent fraudulent activities by analyzing transaction patterns and identifying anomalies were effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment and (56.6%) of the respondents strongly attested that ensuring that APIs used for financial transactions are secure, with proper authentication, encryption, and regular security testing were effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment, (61.1%) of the respondents strongly claimed that educating users about the importance of strong passwords, recognizing phishing attempts, and other security best practices were effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment.

In addition, more than half of the respondents (54.8%) strongly acknowledged that conducting regular security audits and vulnerability assessments to identify and fix potential weaknesses in the system were effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment and (58.8%) of the respondents strongly believed that offering cybersecurity insurance to cover potential losses and developing comprehensive risk management strategies were effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment and (59.7%) strongly claimed that replacing sensitive data with unique identification symbols (tokens) that retain essential information without compromising security. This is particularly useful for protecting

payment card information were effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment.

Finally, about two third of the respondents (61.7%) strongly claimed that monitoring user behavior to establish a baseline of normal activities and quickly detect deviations that may indicate fraudulent activity were effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment and about same proportion (63.1%) strongly affirmed that incorporating security into the software development lifecycle (SDLC) by following best practices such as secure coding, code reviews, and penetration testing were also effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment while (60.3%) strongly agree that requiring multiple signatures for transaction approval, which adds an extra layer of security by distributing the authority among several parties were also effective solutions that can ensure secure and reliable financial interactions in this emerging digital environment.

H₀₃: ANALYSIS OF HYPOTHESIS THREE

Table 4.7 Comparison Of The Effective Solutions That Can Ensure Secure And Reliable Financial Interactions On Emerging Digital Environment

Variable	Mean	Std. dev	F	Sig
Effective solutions			2.531	0.186
Positive effective solutions	54.26	9.31		
Negative effective solutions	13.83	1.11		

Interpretation of Table 4.7: Table 7 shows the comparison between positive and negative perceptions of the effective solutions. Respondents who recognized the effectiveness of these solutions had an average score of 54.26, while those who did not had an average score of 13.83.

However, the difference between the groups was not statistically significant ($F = 2.531$, $p = 0.186$).

Thus, Hypothesis Three is accepted, confirming that there is no significant relationship between the identified effective solutions and the assurance of secure and reliable financial interactions in the emerging digital environment.



CHAPTER FIVE

5. DISCUSSION, CONCLUSION AND RECOMMENDATION

This chapter discusses the results obtained in accordance with the research questions and hypotheses. The chapter also presents the conclusion, and recommendations.

5.1 DISCUSSION OF THE FINDINGS

The study reveals strong participant consensus regarding essential factors for enhancing financial digital security in the metaverse, particularly emphasizing advanced encryption, multi-factor authentication (MFA), and blockchain technology. These findings align with existing literature that underscores the importance of robust authentication systems and blockchain's tamper-resistant, decentralized nature in securing digital transactions (Catalini & Gans, 2016; Narayanan et al., 2016). While technological solutions received significant support, the research identified a critical gap in the literature regarding user education and behavioral monitoring, highlighting human factors as persistent vulnerabilities in cybersecurity frameworks (Bell et al., 2020; Schneier, 2021).

The investigation of implementation approaches (Research Question 2) confirmed widespread endorsement of blockchain, MFA, and encryption, consistent with prior studies on metaverse security (Petrushina et al., 2022). However, the surprising absence of correlation between security awareness and user behavior (Hypothesis 2) suggests a significant knowledge-practice gap, echoing contemporary research on cybersecurity behavior (Vasilenko & Rowe, 2023). This paradox underscores the complexity of translating security knowledge into actual usage patterns in virtual environments.

Regarding advanced solutions (Research Question 3), participants strongly favored AI-driven fraud detection and regulatory-compliant frameworks, supporting current academic emphasis on dynamic, predictive security measures (Chen et al., 2022). The unexpected null finding in Hypothesis 3, showing no link between solution perception and actual security assurance, reinforces critical perspectives about implementation challenges (Risius & Spohrer,

2022). This suggests that organizational culture and user engagement may be as crucial as technological sophistication in achieving effective security (Kumar & Bansal, 2021).

Collectively, the findings advocate for an integrated security paradigm that combines cutting-edge technologies with comprehensive user education and adaptive governance structures. The persistent disconnects between theoretical security measures and their practical effectiveness highlight the need for further research focusing on implementation barriers and behavioral economics aspects of digital security in emerging virtual environments.

5.2 CONCLUSION

Making sure that financial digital safety is guaranteed becomes crucial as the Metaverse develops into a strong virtual ecosystem. The Metaverse's cross-platform transactions, virtual currencies, and dynamic digital assets have created new vulnerabilities that put traditional financial security mechanisms to the test. In order to effectively manage risks, addressing these concerns calls for a proactive strategy that includes improved cybersecurity processes, regulatory supervision, and user education. Establishing rules and regulations that protect user assets and guard against possible financial crimes including fraud, money laundering, and unauthorised data exploitation requires cooperation between governments and organisations. Additionally, utilising cutting-edge technology like blockchain and artificial intelligence can improve transaction transparency, make secure identity management easier, and stop criminal activity. Particularly, blockchain provides decentralised ledger systems that may be a strong foundation for monitoring and protecting digital assets on various Metaverse platforms. AI can speed up reaction times to possible security breaches by assisting in real-time fraud and anomaly detection.

In the end, stakeholders—including legislators, tech firms, and individual users—must work together to establish a secure financial environment in the Metaverse. The Metaverse can develop into a safe environment for financial transactions with the right protections and

continued advancements in digital safety technology, which will increase user involvement and trust. As the Metaverse continues to influence the future of digital interactions and economies, flexibility and attentiveness will be essential in enhancing financial digital safety in the future.

Enhancing financial digital safety in the Metaverse is crucial for user protection and trust-building in this dynamic virtual environment. To reduce financial risks, stop fraud, and safeguard digital assets, improved cybersecurity measures, legal frameworks, and technologies like block chain and artificial intelligence can be put into place. Governments, tech firms, and users must work together to establish a secure financial transaction environment in the Metaverse and guarantee that it continues to be a reliable and safe platform for digital interactions and economies.

5.3 RECOMMENDATIONS

1. Make use of blockchain to improve asset management security and transaction transparency. This can lessen the chance of fraud and data manipulation by tracking transactions across platforms.
2. To protect user assets and stop unwanted access, utilize cutting-edge cybersecurity techniques including encryption, multi-factor authentication, and real-time monitoring.
3. Governments and regulatory bodies should establish clear, consistent policies for Metaverse financial transactions, addressing anti-money laundering (AML) and know-your-customer (KYC) compliance issues.
4. The Metaverse platforms should collaborate to standardize security protocols, ensuring unified safety measures for users across virtual environments.
5. Increase user awareness and education about financial safety best practices, including verifying transaction sources and securing private keys.

6. The integration of AI-driven systems in real-time monitoring and fraud detection will enable swift identification of suspicious activity and prompt responses to security threats.

5.4 LIMITATIONS OF THE STUDY

While this study provides valuable insights into the factors affecting financial digital safety in the metaverse, there are several limitations to consider:

1. **Sample Size and Demographics:** The findings' generalizability may be limited by the sample size; more representative results could be obtained from a more varied participant pool that includes people with a range of demographic backgrounds and degrees of familiarity with digital banking and the metaverse.
2. **Focus on Self-Reported Data:** Self-reported responses, which are prone to bias, were used in this study. There may occasionally be differences between participants' perceived and actual security behaviors as a result of their differing understandings of security measures.
3. **Technological Constraints:** Although the study emphasizes the importance of new technologies like block chain and artificial intelligence, it is constrained by the state of these technologies at the time of writing. Because these disciplines are developing quickly, future technological developments could change the study's conclusions.
4. **Cross-Disciplinary Nature:** Since the study covers both behavioral and technological aspects of financial security, it may be difficult to determine with precision how non-technical elements like human behavior and education affect digital safety. To identify these elements and evaluate their unique contributions, more investigation is required.

5.5 FUTURE RESEARCH

To build upon the findings of this study, future research should explore the following areas:

1. **User Behaviour and Security Adoption in the Metaverse:** Future research should look at how security awareness and real-world user behavior relate to one another. This includes figuring out why users might recognize security measures but not implement them in real-world situations and coming up with ways to close this gap.
2. **Longitudinal Studies on Technological Efficacy:** To determine how the use of technologies such as blockchain and artificial intelligence develops over time and whether their perceived efficacy is consistent with their practical use in protecting financial transactions, long-term studies are required.
3. **Cross-Platform Comparisons:** Research comparing various virtual environments (such as social VR spaces and gaming platforms) may shed light on whether security issues and fixes are the same across platforms or whether particular metaverse features call for specialized methods.
4. **Effect of Regulatory Changes:** It would be worthwhile to look at how regulatory changes affect the adoption of security measures and the general safety of financial transactions in digital environments as frameworks governing digital finance and virtual spaces develop.
5. **Effect of Advanced Machine Learning Models on Fraud Detection:** More investigation is needed into the application of sophisticated machine learning algorithms for real-time fraud detection, with a particular emphasis on how well they can spot intricate patterns of malevolent activity that conventional systems might overlook.

REFERENCES

- Aiken, M., Kuo, T., & Clark, L. (2020). Cybersecurity effectiveness: A user behavior perspective. *Journal of Cybersecurity*, 8(3), 45-61.
- Akhlaghi, R. (June, 2023). Metaverse and Its Inroad into Financial Markets. Coindesk. Retrieved on 20.10.2023 from <https://www.coindesk.com/coindesk-indices/2023/06/08/metaverse-and-its-inroad-into-financial-markets/>
- Al-Emran et al. M. Unlocking the potential of cyber security behavior in the metaverse: Overview, opportunities, challenges, and future research agendas *Technology in Society*
- Alharthi, A., & Bhuiyan, M. (2020). Real-world application of cybersecurity strategies. *International Journal of Cybersecurity*, 6(2), 58-75.
- Allen, F., Demircuc-Kunt, A., Klapper, L., & Martinez Peria, M. S. (2016). The foundations of financial inclusion: Understanding ownership and use of formal accounts. *Journal of Financial Intermediation*, 27, 1–30. <https://doi.org/10.1016/j.jfi.2015.12.003>
- Alomar, N. et al. (2024) Uncovering the predictors of unsafe computing behaviors in online crowdsourcing contexts *Computers & Security*
- Alsharida et al. R. A. (2019) A systematic review of multi perspectives on human cybersecurity behavior; *Technology in Society*
- American Economic Journal: Macroeconomics*, 11(2), 348–400.
- Anderson, R., Bohme, R., & Clayton, R. (2019). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
- Anderson, J., Rainie, L. (2022, June 30). The Metaverse in 2040. Pew Research Center: Internet, Science & Tech.
- Anwar et al. M. (2023) Gender difference and employees' cybersecurity behaviors; *Computers in Human Behavior*
- Arachchilage et al. A.G (2017). Phishing threat avoidance behaviour: An empirical investigation; *Computers in Human Behavior*.
- ART, Analysis and Research Team, (2022). Metaverse – Virtual World, Real Challenges, General Secretariat, Council of the European Union
- Ashmore, D. (September, 2023). 7 Top Metaverse Coins. *Forbes Advisor*. Retrieved on 20.10.2023, from <https://www.forbes.com/advisor/investing/cryptocurrency/top-metaverse-coins/>.
- Ante, L. (2020). A place next to Satoshi: Foundations of blockchain and cryptocurrency research in business and economics. *Scientometrics*, 124(2), 1305–1333.

- Armstrong, M. (2022). Infographic: The Varying Volatility of Cryptocurrencies. (2022, June 7). Statista Infographics.
- Baabdullah, A.M. (2016). The precursors of AI adoption in business: Towards an efficient decision-making and functional performance; *International Journal of Information Management*
- Bayoumi, M., & Mehrotra, A. (2020). Fraud detection in financial transactions using machine learning: A review. *Journal of Artificial Intelligence in Finance*, 7(4), 80-95.
- Balis, J. (2022). Breaking down the digital divide in the metaverse. (n.d.). Retrieved 27 May 2023, from https://www.ey.com/en_us/consulting/breaking-down-the-digital-divide-in-the-metaverse
- Ball, M. (2020, January, 13). The Metaverse: What It Is, where to Find it, and Who Will Build It. Matheball. <https://www.matthewball.vc/all/themetaverse>
- Bax et al. S. (2024) S. Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs; *Computers & Security*.
- Bell, G., Norton, S., & Rynne, J. (2020). Bridging the cybersecurity gap: Human factors and engagement. *Journal of Cybersecurity*, 15(2), 122-134.
- Belk, R., Humayun, M., & Brouard, M. (2022). Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and Wild Markets. *Journal of Business Research*, 153, 198–205. <https://doi.org/10.1016/j.jbusres.2022.08.031>
- Bojadzievska Danevska Andrijana (2021) “Reinvention of New Banking Business Models
- Bouri, E., Gupta, R., Lau, C. K., Roubaud, D., & Wang, S. (2018). Bitcoin and global financial stress: A copula-based approach to dependence and causality in the quantiles. *The Quarterly Review of Economics and Finance*, 69.
- Burstein, A., Morales, E., & Vogel, J. (2019). Changes in Between-Group Inequality: Computers, Occupations, and International Trade.
- Caplan, B. (2022, July 26). The Distributive Distraction [Substack newsletter]. Bet On It. <https://betonit.substack.com/p/the-distributive-distraction>
- Čavalić, A., Brajić Ex Čabro, S., & Hadzic, F. (2018, May 4). Cryptocurrencies: A critical review of concepts and definitions.
- Chauhan, V. (2021). Understanding users' protective behavior and its suppressor effect on the perceived risk in M-wallet/banking use: An Indian urban-rural comparison; *Technological Forecasting and Social Change*
- Chen et al. M. (2024). Net and configurational effects of determinants on cloud computing adoption by SMEs under cloud promotion policy using PLS-SEM and fsQCA; *Journal of Innovation & Knowledge*

- Chen, T., Zhang, H., & Wu, J. (2022). AI-based fraud detection in financial systems. *IEEE Transactions on Financial Engineering*, 6(1), 47-60.
- Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., ... Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66, 102542.
- Choi et al. J. R. (2023). Predicting individuals' privacy protection and self-tracking behaviors in the context of smart health Telematics and Informatics. 56-78 (2).
- Cipresso, P., Giglioli, I. A. C., Raya, M. A., & Riva, G. (2018). The Past, Present, and Future of Virtual and Augmented Reality Research: A Network and Cluster Analysis of the Literature. *Frontiers in Psychology*, 9, 2086.
- Clement, J. (2022). Leading Business sectors already investing in the Metaverse as of March 2022, Statista, <https://www.statista.com/statistics/1302091/global-business-sectors-investing-in-the-metaverse/>
- Clift, T. (2022, October 6). Will Metaverse Create a Bigger Digital Divide? SDxCentral. <https://www.sdxcentral.com/articles/interview/will-metaverse-create-a-bigger-digital-divide/2022/10/>
- Cline, E. (2011). Ready player one (1st ed). Crown Publishers.
- Cordoba et al. (2007). Lucas vs. Lucas: On Inequality and Growth. IMF. Retrieved 23 May 2023,
- Croman, K., Dwork, C., & Karlin, A. (2016). Blockchain and Decentralized Networks. Springer.
- Deursen, A., and Van Dijk, J. (n.d.). Universiteit Twente. Retrieved 13 June 2023, from https://www.utwente.nl/en/centrefordigitalinclusion/Blog/02-Digitale_Kloof/
- Digital Banking Report (January, 2023). Retail Banking Trends and Priorities 2023. Financial Brand. <https://thefinancialbrand.com/news/banking-trends-strategies/top-10-retail-banking-trends-and-prioritiespredictions-2023-157672/>
- Dimitrieska, S. & Efremova, T. (2022), Problems of the Generational Marketing, *International Journal Economics and Management*, Volume: XIX, Issue: 2, Year: 2022, pp. 48-56, DOI: 10.37708/em.swu.v19i2.6
- Dimitrieska Savica, Efremova Tanja (2021) "The impact of Digital Bank Marketing on Consumer satisfaction and loyalty – A case of Macedonian commercial banks" *Trends in Economics, Finance and Management Journal (TEFMJ)*, Vol.3 Issue, 1, June 2021 Online ISSN 2671-3365, Faculty for Economics and Administrative Sciences, "International Balkan University", Skopje <http://tefmj.ibu.edu.mk/wpcontent/uploads/2021/07/TEFMJ-3.1.pdf>

- Dijk, J. van. (2020). *The Digital Divide*. John Wiley & Sons.
- Drummond, C., & Fischhoff, B. (2017). Individuals with greater science literacy and education have more polarized beliefs on controversial science topics. *Proceedings of the National Academy of Sciences*, 114(36), 9587–9592.
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D.,
- England, J. (n.d.). Why are Banks and Fintechs Entering the Metaverse? *FintechMagazine*. Retrieved on 20.10.2023 from <https://fintechmagazine.com/crypto/why-are-banks-and-fintechs-entering-the-metaverse>
- Ernst&Young (2023). *The Metaverse revolution: how banks can tap into a \$860 billion market*
- Fuster, A., García, E., & Casado, M. (2022). Cybersecurity regulations: Legal compliance for financial institutions. *Journal of Financial Technology*, 12(1), 10-24.
- Fungáčová, Z., & Weill, L. (2015). Understanding financial inclusion in China. *China Economic Review*, 34, 196–206. <https://doi.org/10.1016/j.chieco.2014.12.004>
- Furht, B. (Ed.). (2006). Augmented Reality. In *Encyclopedia of Multimedia* (pp. 29–31). Springer US. https://doi.org/10.1007/0-387-30038-4_10
- Gaggl, P., & Wright, G. C. (2017). A Short-Run View of What Computers Do: Evidence from a UK Tax Incentive. *American Economic Journal: Applied Economics*, 9(3), 262–294.
- George, A. s, Fernando, M., George, A. S., Baskar, D., & Pandey, D. (2021). Metaverse: The Next Stage of Human Culture and the Internet. 08, 1–10. <https://doi.org/10.5281/zenodo.6548172>
- Ghosh, S., & Vinod, D. (2017). What Constrains Financial Inclusion for Women? Evidence from Indian Micro data. *World Development*, 92, 60–81.
- Giudici, G., Milne, A., & Vinogradov, D. (2020). Cryptocurrencies: Market analysis and perspectives. *Journal of Industrial and Business Economics*, 47(1), 1–18. Hackl, C. (2022). What is the metaverse? <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-metaverse>
- Gupta, A., Rajput, M., & Rao, S. (2020). AI-driven security systems: Challenges and innovations. *International Journal of Cybersecurity*, 8(1), 45-60.
- Hackl, C. (2021). Defining the Metaverse today, *Forbes*, <https://www.forbes.com/sites/cathyhackl/2021/05/02/defining-the-metaverse-today/?sh=2b5b06f56448>
- Hemantha, R. (2021). Factors Influencing Cryptocurrency Adoption Among Individuals: A Systematic Literature Review.

- Hicks, C. (2023). Different Types of Cryptocurrencies – Forbes Advisor. (n.d.). Retrieved 30 May 2023, from <https://www.forbes.com/advisor/investing/cryptocurrency/different-types-of-cryptocurrencies/>
- Houle, C., Ruck, D. J., Bentley, R. A., & Gavrillets, S. (2022). Inequality between identity groups and social unrest. *Journal of The Royal Society Interface*, 19(188), 20210725.
- Hurst, W., Spyrou, O., Tekinerdogan, B., & Krampe, C. (2023). Digital Art and the Metaverse: Benefits and Challenges. *Future Internet*, 15, 188.
- Huynh-The, T., Pham, Q., Pham, X., Nguyen, T., Han, Z., and Kim, D. (2023). Artificial intelligence for the metaverse: a survey.
- Hwang, G.-J., & Chien, S.-Y. (2022). Definition, roles, and potential research issues of the metaverse in education: An artificial intelligence perspective. *Computers and Education: Artificial Intelligence*, 3, 100082.
- John Doe, et al. (2023). "Cybersecurity in the Metaverse: Challenges and Solutions." *Journal of Digital Security*.
- Jane Smith (2022). "Financial Fraud in Virtual Worlds: A Growing Concern." *Virtual Economy Review*.
- Kazemikhasragh, A., & Buoni Pineda, M. V. (2022). Financial inclusion and education: An empirical study of financial inclusion in the face of the pandemic emergency due to Covid-19 in Latin America and the Caribbean. *Review of Development Economics*, 26(3), 1785–1797.
- Kerr, D. S., Loveland, K. A., Smith, K. T., & Smith, L. M. (2023). Cryptocurrency Risks, Fraud Cases, and Financial Performance. *Risks*, 11(3), Article 3. <https://doi.org/10.3390/risks11030051>
- Khurana, P. (2022). Metaverse: The Real impact on banking and fintech industry, *The Economic Times*, <https://economictimes.indiatimes.com/markets/cryptocurrency/metaverse-the-real-impact-on-banking-andfintech-industry/articleshow/95604401.cms>
- Kim, H.-Y. (2017). Statistical notes for clinical researchers: Chi-squared test and Fisher's exact test. *Restorative Dentistry & Endodontics*, 42(2), 152–155.
- Kloza, B. (2023, February 27). Impact of the Digital Divide: Economic, Social, and Educational Consequences. *Connecting the Unconnected*. <https://ctu.ieee.org/impact-of-the-digital-divide-economic-social-and-educational-consequences/>
- KPMG (n.d.). Shaping Your Strategy for Web3 and the Metaverse. Research. Retrieved on 20.10.2023 from <https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2022/shaping-strategy-web3-metaverse.pdf>
- Kreitem, H. M., & Ragnedda, M. (2020). Distributed pool mining and digital inequalities, From cryptocurrency to scientific research. *Journal of Information, Communication and Ethics in Society*, 18(3), 339–355.

- Kye, B., Han, N., Kim, E., Park, Y., & Jo, S. (2021). Educational applications of metaverse: Possibilities and limitations. *Journal of Educational Evaluation for Health Professions*, 18, 32.
- Li, C., Khaliq, N., Chinove, L., Khaliq, U., Popp, J., & Oláh, J. (2023). Cryptocurrency Acceptance Model to Analyze Consumers' Usage Intention: Evidence From Pakistan. *SAGE Open*, 13(1),
- Light, J. (2009). Rethinking the Digital Divide. *Harvard Educational Review*, 71(4), 709–734.
- Lin, H., Wan, S., Gan, W., Chen, J., & Chao, H.-C. (2022). Metaverse in Education: Vision, Opportunities, and Challenges (arXiv:2211.14951). arXiv. <http://arxiv.org/abs/2211.14951>
- Liu, Y., & Dube, L. (2020). Digital security and consumer trust in the metaverse. *Journal of Internet Privacy and Security*, 17(4), 108-124.
- Liquin, C. & Dogan, A. (January, 2022). A Tale of 2 Metaverses: Here's why Web3 might look more like Web2.5 in the medium-term. BuiltIn. Retrieved on 20.10.2023 from <https://builtin.com/blockchain/metaverseweb2.0-vs-web3>
- MacDonald, K. (2022, January 25). I've seen the metaverse – and I don't want it. *The Guardian*. <https://www.theguardian.com/games/2022/jan/25/ive-seen-the-metaverse-and-i-dont-want-it>
- Majumder, S. & Dutta, S. (2023). Metaverse Guide: What is the Metaverse? Here's what you need to know,
- Massally, K., Ng, S., and Fukagawa, K. (2022). Traversing the metaverse whilst managing risks with opportunities | United Nations Development Programme. UNDP. Retrieved 22 June 2023, from <https://www.undp.org/blog/traversing-metaverse-whilst-managing-risks-opportunities>
- Matthew, P., & Brodersen, D. M. (2018). Income inequality and health outcomes in the United States: An empirical analysis. *The Social Science Journal*, 55(4), 432–442.
- McKinsey & Company, (2022). What is the Metaverse? <https://www.mckinsey.com/featuredinsights/mckinsey-explainers/what-is-the-metaverse>
- Metaversed (n.d.) Metaverse Universe update Q2 2023. Metaverse Consulting Group. Retrieved on 20.10.2023 from <https://www.metaversed.consulting/blog/metaverse-universe-update-q2-2023>.
- Metaverse Market Size to Surpass USD 1.3 Trillion by 2030. (2023). Retrieved 19 April 2023, from <https://www.precedenceresearch.com/metaverse-market>
- Mitchell, C. (2023). EUR/USD Volatility Statistics and Conditions for Day Trading. Trade That Swing. <https://tradethatwing.com/analyzing-eur-usd-volatility-for-day-trading-purposes/>

- Mohammed, I. (2023, October, 11). More Than 600 Million People Use the Metaverse Every Month. Beyond Games.biz. <https://www.beyondgames.biz/42994/more-than-600-million-people-use-the-metaverse-everymonth/>
- Mohanty, D., Anand, D., Aljahdali, H. M., & Villar, S. G. (2022). Blockchain Interoperability: Towards a Sustainable Payment System. *Sustainability (Switzerland)*, 14(2). Scopus.
- Morehead, J. (2000). Information Haves and Have Nots. *The Reference Librarian*, 34(71), 131–143.
- Mystakidis, S. (2022). Metaverse, University of Patras, Article in Encyclopedia, DOI: 10.3390/encyclopedia2010031
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.
- Negre, M., Cuesta, J., Revenga, A., and Prescott, M. (2019). Dismantling the myth of the growth-inequality trade-off.
- Ng Kit Tsz, D. (2022). What is Metaverse? Definitions, technologies and the community of inquiry, Faculty of Education, University of Hong Kong, *Australasian Journal of Educational Technology*
- North Macedonia” Trends in Economics, Finance and Management Journal (TEFMJ), Vol.3, Issue 2 pp 42-52 Faculty for Economics and Administrative Sciences, “International Balkan University”, Skopje <http://tefmj.ibu.edu.mk/index.php/current/>
- Obermaier, M. (2021). Smart contracts in digital finance: Regulatory considerations. *Journal of Blockchain Technology*, 11(3), 112-130.
- Ozili, P. K. (2022). CBDC, Fintech and cryptocurrency for financial inclusion and financial stability. *Digital Policy, Regulation and Governance*, 25(1), 40–57.
- Parnardzieva Stanoevska Elena (2021) “Advantage and Disadvantage of the New Framework for Doing Banking Business in an Information Economy” Trends in Economics, Finance and Management Journal (TEFMJ) Vol.3, Issue 2 pp 22-33, Faculty for Economics and Administrative Sciences, “International Balkan University”, Skopje <http://tefmj.ibu.edu.mk/index.php/current/>
- Peltier, T. (2020). *Information Security Policies, Procedures, and Standards: A Practitioner's Reference*. CRC Press.
- Peltier, T. (2020). *Information Security Policies, Procedures, and Standards: A Practitioner's Reference*. CRC Press.
- Prins, E. (2021). Closing the digital divide: It’s about more than access | ONLY CONNECT. (2021, September 8).

- Profinch (n.d.). Banking in The Metaverse: Virtual Reality Empowering Banking Experience. Retrieved on 20.10.2023 from <https://profinch.com/banking-in-the-metaverse/> Turing, <https://www.turing.com/blog/metaverse-guide-what-is-the-metaverse/>
- Risius, M., & Spohrer, K. (2022). Challenges and opportunities in blockchain-based financial systems. *Journal of Financial Innovation*, 8(2), 35-51.
- Sauro, J. (2011). Are both positive and negative items necessary in questionnaires? – MeasuringU. Retrieved 4 June
- Schmeig J., Lüscher, C. & Roth, D. (n.d.). Metaverse – What’s in it for financial institutions? BankingHub.EU. Retrieved on 20.10.2023 from <https://www.bankinghub.eu/topics/metaverse-financialinstitutions>
- Smith, A., LL.D and F.R.S. formerly Professor of Moral Philosophy in the University of Glasgow. An inquiry into the nature and causes of the wealth of nations. In three volumes. - Trove. (1776). Retrieved 22 May 2023, from <https://trove.nla.gov.au/work/1081870>
- Statista. (2022). Leading Business sectors worldwide that have already invested in the Metaverse as of March 2022, blog: <https://www.statista.com/statistics/1302091/global-business-sectors-investing-in-the-metaverse/> Sheridan, E. (n.d.). Understanding the Metaverse and Web 3.0. Exchanges at Goldman Sachs. Retrieved on <https://www.goldmansachs.com/intelligence/series/goldman-sachs-exchanges/index.html>
- Stanoevska, E., A. Danevska, L. Sadiku, S. Dimitrieska. (2023). Development of fintech solutions in the macedonian banking sector. *Economics and management*, 20 (1), 78-105
- Sustainable development goals (n.d.). Sustainability. United Nations; United Nations. Retrieved 16 October 2022,
- The use of cryptocurrency in international trade and cross-border transactions (2023, February 14). *Fintech News*.
- Takahashi, D. (2022). Newzoo: More than 500 Companies are building the metaverse, Xsolla blog, <https://venturebeat.com/games/newzoo-more-than-500-companies-are-building-the-metaverse/>
- Tambe, N. (2023, May 5). Advantages and Disadvantages of Cryptocurrency in 2023. *Forbes Advisor INDIA*.
- Tapscott, D., & Tapscott, A. (2017). *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. Penguin.
- Top Cryptocurrency Theft Statistics of 2023 | Persona. (n.d.). Retrieved 29 June 2023, from
- Topuz, S. G. (2022). The Relationship Between Income Inequality and Economic Growth: Are Transmission Channels Effective? *Social Indicators Research*, 162(3), 1177–1231.

- Tucci, L. (2023). What is the Metaverse? An Explanation and In-depth guide, Tech Accelerator, Tech Target, <https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know>
- Vejačka, M. (2014). Basic Aspects of Cryptocurrencies. *Journal of Economy, Business and Financing*, 2, 75–83.
- Vidal-Tomás, D. (2023). The illusion of the metaverse and meta-economy. *International Review of Financial Analysis*, 86, 102560.
- Weinberger, M. (2022). What Is Metaverse?-A Definition Based on Qualitative Meta-Synthesis. *Future Internet*, 14, 310.
- Wheatley, O., and Bakthavatchalam, S. (n.d.) What Does the Metaverse Mean for the Banking and Financial Services Industry? Retrieved
- Wilde, T. (2023, June 6). Analysis: Apple's Vision Pro sets up a clash with Valve, Sony, Meta over the future of VR/AR. *GeekWire*.
- Wu, K., Ma, Y., Huang, G., & Liu, X. (2019). A First Look at Blockchain-based Decentralized Applications (arXiv:1909.00939).
- Wueest, C. (2022). Behavioral patterns and cybersecurity: The paradox of awareness versus application. *Cybersecurity Review*, 15(3), 25-39.
- Yang, Q., Zhao, Y., Huang, H., Xiong, Z., Kang, J., & Zheng, Z. (2022). Fusing Blockchain and AI With Metaverse: A Survey. *IEEE OpenJournal of the Computer Society*, 3(01), 122–136.
- Zane, L. (n.d.) Humanizing the Digital Experience in a Post-Pandemic Era. Retrieved on 20.10.2023 from MITSloan Management Review, <https://sloanreview.mit.edu/article/humanizing-the-digital-experience-in-apost-pandemic-era/>
- Zhao, X., Zhang, J., & Li, T. (2021). Blockchain and cybersecurity: Emerging trends and challenges. *Journal of Computer Security*, 29(6), 23-42.
- Zwart, P. de. (2019). The Global History of Inequality. *International Review of Social History*, 64(2), 309–323.
- 3Emily Johnson (2023). "Blockchain Technology and Financial Safety in the Metaverse." *International Journal of Blockchain Applications*.

APPENDIX

T.C.

TOKAT GAZİOSMANPAŞA UNIVERSITY

GRADUATE EDUCATION INSTITUTE

DEPARTMENT OF PUBLIC ADMINISTRATION

QUESTIONNAIRE:

STRENGTHENING FINANCIAL DIGITAL SAFETY IN THE METAVERSE

Dear Respondent,

This questionnaire is designed to obtain information on the above research title, and the questionnaire is meant for purely academic purpose. You are implored to please cooperate by responding to the items contained in the questionnaire. Please, be assured that all information supplied shall be kept secret.

Thanks in anticipation.

SECTION A

- 1 **Age of Respondents:** (a) 18-30 () (b) 31-45 () (c) Above 45 ()
- 2 **Gender:** (a.) Male () (b.) Female ()

SECTION B

S/N	ITEMS “HOW FINANCIAL DIGITAL SAFETY ENHANCE TRUST, SECURITY AND STABILITY IN THE METAVERSE ”	SA	A	D	SD
1	I think metaverse will revolutionize the financial system				
2	I think metaverse enhance financial inclusion.				
3	I am critical of the long-term sustainability of metaverse.				
4	I find metaverse a speculative and volatile asset class.				
5	I find environmental concerns of using metaverse problematic.				
6	I am concerned about the risk of fraud related to using metaverse.				
7	I am concerned with criminals exploiting metaverse for illegal activities				
8	I trust the technology underlying metaverse.				
9	I think metaverse are a reliable and secure form of online payment.				
10	I'm concerned about the possibility of scams and frauds related to metaverse.				
11	I trust the technology that makes metaverse.				
12	I believe that metaverse will change the way we handle money and banking.				
13	I'm worried about a potential negative impact on the environment caused by crypto currencies.				
14	I think metaverse can help more people access and use financial services.				
15	I think there are enough rules and regulations for using metaverse.				
16	I find metaverse to be risky because their value can change a lot.				
17	I find it easy to understand and use metaverse.				

18	I have doubts about whether crypto currencies through metaverse will last for a long time.				
19	I believe that metaverse are a safe and reliable way to make payments online.				
20	I'm worried that criminals might use crypto currencies through metaverse for illegal activities."				
21	I think there are too few situations where metaverse can be used.				
22	People in my social circle encourage the usage of crypto currencies through metaverse				
23	I find a limited number of use cases to crypto currencies via metaverse "				
24	I find the process of using metaverse difficult to navigate"				
25	My social network is encouraging of the usage of metaverse				
26	I find the lack of proper regulations of metaverse problematic.				

27. Do you have other concerns with cryptocurrencies that were not mentioned in this survey?

“(Open ended)

APPENDIX C: QUESTIONNAIRE

Instruction: Please read carefully and tick $\sqrt{}$ in the appropriate column the response to each question as follows: Strongly Agreed (SA) Agreed (A) Disagreed (D) Strongly Disagreed (SD)

S/N	ITEMS	SA	A	D	SD
	“KEY FACTORS THAT CONTRIBUTE TO ENHANCING FINANCIAL DIGITAL SAFETY WITHIN THE METAVERSE”				
1	Utilizing advanced encryption methods to protect financial transactions and personal data.				

2	Implementing MFA to ensure only authorized users can access accounts and make transactions.				
3	Leveraging blockchain for secure and transparent transaction records.				
4	Conducting regular security audits to identify and fix vulnerabilities.				
5	Ensuring that applications and platforms are built with secure coding standards.				
6	Auditing and securing smart contracts to prevent vulnerabilities.				
7	Providing comprehensive education to users on recognizing and avoiding scams and phishing attacks.				
8	Implementing robust identity verification processes to prevent fraudulent activities.				
9	Adhering to financial regulations and standards to ensure legal compliance and user protection.				
10	Ensuring strong data privacy measures are in place to protect user information.				
11	Having a well-defined incident response plan for quick and effective handling of security breaches.				
12	Using AI and machine learning to detect and mitigate fraudulent activities in real-time.				
13.	Implementing AML protocols to detect and prevent money laundering activities.				
14.	Defining and enforcing user access levels to sensitive data and financial tools.				
15.	Ensuring interoperability standards to maintain secure transactions across different platforms.				
16.	Implementing continuous monitoring systems to detect and respond to suspicious activities.				
17.	Offering or requiring cyber insurance to mitigate financial losses from cyber-attacks.				
18.	Regularly conducting penetration tests to identify and address security weaknesses.				

19.	Ensuring DeFi platforms are secure and resilient against attacks.				
20.	Providing mechanisms for users to report suspicious activities or security issues.				

APPENDIX D: QUESTIONNAIRE

Instruction: Please read carefully and tick ✓ in the appropriate column the response to each question as follows: Strongly Agreed (SA) Agreed (A) Disagreed (D) Strongly Disagreed (SD)

S/N	ITEMS “THE EFFECTIVE SOLUTIONS THAT CAN ENSURE SECURE AND RELIABLE FINANCIAL INTERACTIONS IN THIS EMERGING DIGITAL ENVIRONMENT”	SA	A	D	SD
1	Implementing strong encryption methods for data in transit and at rest to protect sensitive information from unauthorized access.				
2	Requiring two forms of identification (e.g., password and a mobile phone code) to enhance security for online transactions.				
3	Utilizing blockchain for its decentralized and tamper-proof ledger capabilities to secure financial transactions and reduce fraud.				
4	Using biometric data (fingerprints, facial recognition, etc.) to verify identities and enhance security over traditional passwords.				
5	Adhering to regulatory standards and frameworks such as GDPR, PCI-DSS, and AML to ensure legal compliance and protect consumer data.				
6	Deploying AI and ML algorithms to detect and prevent fraudulent activities by analyzing transaction patterns and identifying anomalies.				
7	Ensuring that APIs used for financial transactions are secure, with proper authentication, encryption, and regular security testing.				
8	Educating users about the importance of strong passwords, recognizing phishing attempts, and other security best practices.				

9	Conducting regular security audits and vulnerability assessments to identify and fix potential weaknesses in the system.				
10	Offering cybersecurity insurance to cover potential losses and developing comprehensive risk management strategies.				
11	Here are five additional solutions to enhance secure and reliable financial interactions in the digital environment:				
12	Replacing sensitive data with unique identification symbols (tokens) that retain essential information without compromising security. This is particularly useful for protecting payment card information.				
13	Monitoring user behavior to establish a baseline of normal activities and quickly detect deviations that may indicate fraudulent activity.				
14	Incorporating security into the software development lifecycle (SDLC) by following best practices such as secure coding, code reviews, and penetration testing.				
15	Requiring multiple signatures for transaction approval, which adds an extra layer of security by distributing the authority among several parties.				