EGE AKADEMİK BAKIŞ / *EGE ACADEMIC REVIEW*

Cilt 24 • Sayı 2 • Nisan 2024
SS. 289/300
Doi: 10.21121/eab.1441950
Başvuru Tarihi: 23.02.2024 • Kabul Tarihi: 12.03.2024

Article Type: *Research Article*

Analysis of Metaverse and Cryptocurrency Crimes in Forensic Accounting

Fatma AKYÜZ[1], Selçuk GÜLTEN[2]

ABSTRACT

The purpose of this study is to collect data on crimes that encompass the technological and software aspects referred to as the "new generation," and to analyze case studies and legal incidents related to crimes committed within the scope of the metaverse and cryptocurrency.

The starting point of the study is the analysis of court decisions related to metaverse and cryptocurrency crimes. Within the scope of the study, thousands of court decisions have been scanned using text mining techniques. The keywords "metaverse," "bitcoin,""digital currency,""cryptocurrency," and "digital money" have been included in the search algorithm for the word corpus. Although no court decision containing the word "metaverse" was found, 37 decisions were identified in which the other terms from the word corpus were mentioned. The oldest decision dates back to July 12, 2019, while the most recent decision is dated March 23, 2023. In addition to the decisions of first-instance courts, the decisions of appellate and higher judicial authorities have also been examined within the framework of text mining studies.

Keywords: Metaverse, Bitcoin, Dijital Currency, Cryptocurrency Crimes, Dijital Money.

JEL Classification Codes: M20, M40, GOO, G10

Referencing Style: APA 7

INTRODUCTION

Metaverse is referred to as a digital world that resembles or mirrors the real world. In the metaverse, people interact with their digital shadows called avatars, which can perform various transactions and engage in commercial activities. This digital world is also considered a repository of metadata. As the use of such new technologies becomes more widespread, various legal issues arise, necessitating a rapid reconsideration of regulatory frameworks.

Forensic accountants are required to closely monitor technological advancements and take precautions against the possibility of criminals developing various methods by utilizing these new technologies. Concepts such as the Internet of Things, blockchain, big data, artificial intelligence, cryptocurrency, augmented virtual reality, non-fungible tokens (NFTs), decentralized finance (DeFi), and Industry 4.0 have emerged and gained attention. These concepts are believed to be a result of the digitization driven by the rapid advancements in computer, software, and internet technologies in recent years. With the development and widespread adoption of publicly accessible metaverse environments, forensic accountants are faced with a new type of crime. From a forensic accounting perspective, metaverse worlds can be evaluated from three different angles. Firstly, it is whether metaverse worlds introduce new dimensions to known internet crimes. Secondly, it is whether the virtual world and financial criminal behaviors can be acknowledged as a separate societal domain where forensic accountants can analyze and investigate. It can be argued that the findings of forensic accounting in the real world may not be universally applicable to the conditions of the virtual world. Attempting to apply them in such a context is likely to give rise to conceptual and legal challenges. Thirdly, the use of virtual worlds can have certain effects on users' real lives. These effects can be exemplified by the economic activities in the virtual world, leading to various cybercrimes, and exerting negative influences on the real society. The metaverse environment should not be perceived as outside the realm of legal order, and particularly, legal rules should be applicable when considering the impacts and consequences on the real world.

[1] Doç. Dr., Uşak Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, Muhasebe Finansman ABDs, fatma.akyuz@usak.edu.tr

[2] Serbest Muhasebeci Mali Müşavir, selcukgulten2@hotmail.com

In cases of crimes committed within the metaverse, the issue of which country has jurisdiction emerges as a significant problem. Determining which country's laws are applicable to activities conducted in the metaverse and which country has the authority to punish criminals becomes a fundamental legal debate. Some of the challenges faced include identifying the perpetrator and determining the extent of financial loss due to the use of various cryptocurrency units. In this regard, it is known that according to network identity management principles, telecommunications companies, internet service providers, or network operators are required to verify users' network identities and real identities.

Metaverse concept being a relatively new phenomenon, there are few studies in the literature that specifically examine the risks in the metaverse domain and its connection to forensic accounting. In a study titled "Identity, Crimes, and Legal Sanctions in the Metaverse" by Qin, Wang, and Hui (2022), it is emphasized that the establishment of an international legal framework is necessary to promote international cooperation, facilitate crime investigations, and support democratic governance. It is emphasized that all active entities in the virtual realm are composed of humans and that human behaviors should adhere to rules such as law and ethics. In another study titled "Metaverse: Welcome to the New Fraud Market" by Smaili and Rancourt-Raymond (2022), the fraud triangle was adapted to the metaverse domain based on 21 articles published between 2021 and 2022. In the study titled "Rules of the Metaverse" by Zhang (2022), emphasis is placed on the need for criminal law in the metaverse. The study discusses the importance of predefining legal sanctions and penalties to be applied when criminal behavior occurs. Another study, "Digital Forensic Investigation Framework for the Metaverse" by Seo, Seok, and Lee (2023), proposes a forensic framework specifically tailored for digital investigations in the metaverse for the first time. In the study titled "Financial Crimes in the Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities" by Wu, Lin, Lin, Zheng, Huang, and Zheng (2023), the focus is on definitions, relevant case analyses, and existing academic research related to such crimes.

CONCEPTUAL FRAMEWORK

In the conceptual framework of the study, concepts such as metaverse, avatar, cryptocurrency, non-fungible token, digital twin, and metaverse wallet have been attempted to be explained.

Concept of Metaverse

With the acceleration of global digital transformation, activities such as remote work, virtual conferences, online education, and internet banking have increased the recognition of the Metaverse. However, despite the increased recognition of the Metaverse concept, there is no agreed-upon or universally accepted definition. Metaverse is considered as the name given to the virtual world where users create its content in a three-dimensional form (Tekin, 2022). The concept of the Metaverse is expected to elevate the interfaces (experience) for users to interact with the internet from two-dimensional to three-dimensional.

Metaverse is defined as a digital realm that combines features of mobile devices, social media, virtual and augmented reality, online gaming, blockchain, and cryptocurrency, creating a vast and interactive online virtual experience (Kaya, 2022). At this point, the Metaverse is the result of technological innovation reaching a certain stage of development. It is described as a scalable immersive 3D virtual world or network of worlds where users can interact with each other and with applications and environments, enabling individual presence and simultaneous collaborative actions through interoperable services (Beşinci, 2023).

Metaverse is a next-generation internet approach that is based on principles such as virtual reality, augmented reality, decentralization, autonomy, and real-time activity. At this point, it is seen as a brand new format or stage that integrates next-generation information technologies and guides the development of the internet towards Web 3.0. Since the structure of the Metaverse is still in its early stage, it is not possible to talk about a final structure (Koç, 2023).

One of the most significant differences that distinguishes the concept of the Metaverse and Metaverse worlds from other virtual platforms and 3D computer games is the idea that all content within the platform is created by the users themselves (Gönülal, 2022). The creation of 3D content, giving the user a sense of being there, and creating an environment that resembles the perception of the real world through the five senses are among the innovative aspects of the Metaverse concept. In the Metaverse universe, individuals are envisioned to use virtual reality goggles and interact through their avatars (virtual bodies) to attend concerts, watch movies, visit museums, go shopping, and even purchase virtual real estate (Başoğlu, 2023).

Due to the emergence of the Metaverse as a social phenomenon, it is also possible for this new technology to be used for criminal purposes. However, since the crimes committed in this environment are very new, there are currently no sufficient standards in place for preventing, detecting, or investigating these crimes.

Concept of Avatar

An avatar is considered as an individual's virtual extension, reflecting specific images, behavioral characteristics, personalities, values, preferences, and digital rituals within the Metaverse environment. Through their avatars, both individuals and organizations are able to easily navigate and interact with various spaces and engage with one another (Atak, 2022).

An avatar is considered as a model of transferring human consciousness into a digital object. In this model, individuals are able to navigate digital environments using their avatars as if they were their own physical bodies. By utilizing a digital body, an attempt is made to create a perception of the five senses within the virtual world. However, in the context of Metaverse crimes, the issue of determining the responsible party for the crimes committed by avatars becomes problematic.

The Concept of Cryptocurrency

Cryptocurrency is defined as a digital form of currency created and operated in a decentralized manner, based on blockchain technology. It is a software-based currency that people attribute value to, without being subject to a central authority. Cryptocurrencies are encrypted using cryptographic systems, providing security and protection for digital or virtual money (Bil, 2023). While the intangible nature of cryptocurrencies raises questions for individuals, their impact on the financial sector and their role as pioneers in technological advancements have gradually gained trust over time (Gürbüz, 2023). Therefore, it is predicted that in the future, both similar and more complex new types of virtual currencies will continue to emerge (Isfarin, 2022).

In the Metaverse environment, the occurrence of relatively new generation crimes such as theft of cryptocurrencies, their fraudulent use, and their exploitation for money laundering purposes is possible. It is believed that forensic accountants will play an important role in efforts to investigate and shed light on financial crimes in this context.

The Concept of Immutable Tokens

Non-fungible tokens (NFTs) are recognized as digital assets that represent tangible objects in the world, such as artworks, in-game items, collections, and videos. They are known as qualified intellectual property titles, emphasizing their immutable nature and compliance with punctuation and grammar rules (Güngör, 2022). Qualified intellectual property titles developed with blockchain technology are unique identities integrated into the virtual world (Baltacıoğlu, 2023). At this point, they serve as indisputable indicators of who created the digital asset and who owns it. NFTs provide provable uniqueness to digital products, thus assisting in determining ownership of the digital item.

NFTs provide standardized features to digital assets, making them suitable for trading. This feature enables fast and secure transactions of digital assets, granting them liquidity. The ability to exclude duplication, along with easy identification of the original digital asset, strengthens the liquidity feature. A system has been established to allow digital artworks to be digitally signed by the artist, thereby protecting the artist's copyright (Arıcı Turhangil, 2023).

Currently, the storage of NFT metadata is primarily achieved through online and offline methods. NFTs, with their verification capabilities, can quickly confirm information such as ownership, transaction history, and creation timestamps of digital assets. This consensus feature gives digital assets a certainty that can have various legal implications. The concept of ownership in the Metaverse operates differently and more complexly than in the physical world (Güven, 2022).

The approval of digital assets is essential for the economic sustainability and value-added development of Metaverse worlds. In future Metaverse applications, NFTs can contribute to generating meaning, economic activity, and various benefits (User, 2022). With the advancement of digital product industries, it is believed that NFTs have potential uses in financial markets, social ecology, and other fields. The use of NFT features in electronic invoices, enabling the creation of e-invoices that are impossible to counterfeit, immutable, and verifiable, can serve as an example in this regard.

However, within the scope of Metaverse crimes, the theft, copying, or imitation of NFTs, as well as the sale of these products as if they were genuine, may give rise to various new offenses.

The Concept of Digital Twins

In the Metaverse, the exact replicas of real-world objects can be created as digital twins. Through the use of sensors and artificial intelligence tools, digital counterparts of physical objects can be accurately generated. In this context, a digital twin is considered a virtual model designed to accurately reflect a physical object (Akturan, 2023).

Regarding Metaverse crimes, the question of whether certain actions involving a digital twin, such as the theft of a digital twin object or causing harm to it through an avatar, constitute offenses within the Metaverse, is currently being debated.

The Concept of Metaverse Wallet

A crypto asset wallet is defined as an address identified by a public key that can send and receive the relevant crypto assets (Çağlar, 2022). Crypto asset wallets are divided into hot (online) and cold (hardware) wallets. A cold wallet is known as the safest way for investors who do not frequently engage in cryptocurrency trading, such as long-term investors, to securely store their assets offline (Özkul, 2022). In this context, Metamask is considered a wallet used in the Metaverse environment for storing cryptocurrencies and conducting payments and transactions. Concerns such as the compromise of digital wallet passwords and the exploitation of cybersecurity vulnerabilities to obtain the values stored in these wallets are among the discussed topics in the realm of Metaverse crimes.

FIELDS OF FORENSIC ACCOUNTING

Forensic accounting is an interdisciplinary field that intersects accounting and law, while also drawing significant benefits from other areas such as forensic science and auditing. It focuses on the financial dimension and accounting aspects of events that constitute a crime, involving the examination of evidence and documentation to form opinions and generate reports. In other words, the concept of forensic accounting can be defined as the collection of financial-related information and the application of analytical thinking with the aim of obtaining evidence in legal matters (Özer, 2022).

Due to its relatively new nature, the forensic accounting profession has become a subject of interest for both accounting practitioners and academics, as it has not been able to prevent fraud and corruption despite all international regulations (Çekmen, 2022). Forensic accounting encompasses various fields that can be described as litigation support services, expert witness testimony, fraud, corruption, and abuse auditing. Forensic accountants are likely to encounter metaverse and cryptocurrency crimes within each of these subfields.

Litigation Support

Litigation support refers to the assistance provided by forensic accountants to all parties involved in a legal case concerning matters related to the court proceedings (Aytekin, 2022). Within the scope of litigation support, forensic accountants present evidence-based accounting-focused technical information to attorneys in order to help them construct their defenses and legal pleadings. Attorneys are expected to share information about their clients with forensic accounting experts under written consent and confidentiality agreements.

Forensic accountants can indeed provide litigation support services in cases involving metaverse and cryptocurrency crimes. Naturally, whether metaverse and cryptocurrency crimes are brought before judicial authorities or not becomes significant. In this study, text mining analyses conducted on court decisions have not yet revealed any instances of the term “metaverse.” However, when text mining studies were conducted on court decisions concerning cryptocurrency, 37 cases were identified. It is worth noting that not all incidents are brought before judicial authorities, and considering stages such as mediation and settlement, the number of cases is expected to be higher.

Indeed, due to the relatively new nature of metaverse and cryptocurrency crimes, there is a clear need for forensic accounting analysis in the process of developing defense strategies and preparing legal petitions. Furthermore, the importance of forensic accountants’ work in uncovering the accounting aspects of metaverse and cryptocurrency crimes is critical.

Expert Witness Testimony

Within the scope of expert witness testimony, forensic accountants provide their knowledge and expertise to the courts, both in written and oral form, particularly regarding financial crimes. As an expert witness, a forensic accountant analyzes the accounting aspects of the case and presents their findings in a report. Unlike a court-appointed expert, the forensic accountant supports their report with visual elements such as tables, graphs, and videos, and delivers an oral presentation in court. During this oral presentation, they answer questions from legal professionals present in the courtroom, including judges, prosecutors, and lawyers. It is through

this comprehensive examination of the case that legal professionals can make informed decisions.

In a court proceeding, a forensic accountant, as an expert witness, presents their own thoughts on accounting issues arising in the case, devoid of subjectivity and emotion, in a calm and composed manner (Yüksel, 2022). Acting impartially, the forensic accountant utilizes their technical knowledge and presents it to legal professionals in court, based on evidence and documentation, thereby assisting in the administration of justice.

The lack of established terminology and even a consensus on definitions regarding metaverse and crypto crime creates various communication problems in understanding the contents of written reports. It is believed that the inclusion of expert witness testimony specifically addressing metaverse and crypto crimes will further enhance the value of forensic accounting work.

Fraud, Corruption, and Abuse Examination

Forensic accounting, also known as investigative accounting, is a service that involves the examination of illegal issues that typically require legal sanctions (Altaylı, 2022). Investigating, probing, and monitoring negative financial events such as fraud, corruption, and embezzlement within companies to identify the perpetrators with evidence and documents constitute the most recognized field of forensic accounting. Forensic accountants go beyond traditional audit and accounting practices by employing techniques such as criminology, graphology, psychology, and forensic computing to shed light on incidents.

Forensic accounting in itself comprises subfields such as fraud prevention and fraud risk reduction, detecting financial losses caused by fraud, and uncovering perpetrated fraud. In relation to Metaverse and cryptocurrency-related financial crimes, forensic accounting services are highly needed for both crime prevention and risk reduction, identification of the perpetrator's avatar, and calculating the incurred financial losses. Until effective forensic investigations are conducted in the Metaverse and law enforcement agencies increase their efforts in this field, every forensic accounting task holds significant importance.

The characteristics of Metaverse, cryptocurrency, and blockchain technologies, such as providing privacy, lack of central authority, and unclear legal regulations, present various opportunities for criminals in this field. Forensic accountants can provide critical services to victims by assisting them in presenting digital and physical evidence and documents to legal authorities. They can support individuals in escalating incidents to the appropriate judicial bodies.

DIGITAL FINANCIAL CRIMES

Metaverse Financial Crimes

Due to the lack of precedents or existing applications with identification gaps, Metaverse gives rise to various new legal implications. The absence of effective regulation on blockchain or Web3 allows Metaverse to become a breeding ground for criminal activities, encouraging financial crimes such as fraud, code exploitation, money laundering, and illicit services (Wu, Lin, Lin, Zheng, Huang & Zheng, 2023). In the Metaverse, the use of unreal avatars and digital masks on social networks allows crimes to be committed in this manner. Some users who perceive the Metaverse as an unprecedented realm of freedom may seek to exploit this environment for their own nefarious purposes.

With the development and widespread adoption of public Metaverse applications, forensic accountants are facing new challenges. These include:

- The Metaverse can currently facilitate the commission of known financial crimes.
- New financial crimes can be committed in the Metaverse environment. The use of novel methods and applications for criminal activities can create vulnerabilities in combating crime.
- Regulatory gaps and the freedom-oriented environment in the Metaverse can provide opportunities for virtual criminals.

Regulatory bodies, financial authorities, governing boards, and fraud investigators should consider these risks before investing in a metadata repository (Smaili & Rancourt-Raymond, 2022). The absence of an established legal framework or criminal sanctions increases the potential for criminal activities to occur.

When users interact through their avatars, situations may arise in which disputes occur that are akin to transgressions beyond legal boundaries in the real world (Cheong, 2022). The identification of the subject matter of a transaction and the determination of the identities of those involved in the transaction are crucial in the investigation of Metaverse or digital currency crimes. However, the seamless completion of the investigation and evidence collection relies on clarifying the real identities of the perpetrators involved in digital currency

crimes. The administrators of the Metaverse service platform or the managers of the cryptocurrency exchange where transactions are conducted must comply with requests to officially transmit recorded information to the appropriate legal authorities without face-to-face identification or verification of individuals involved in the requested transactions.

Although users have the possibility to register multiple anonymous addresses, it is imperative for the central servers of the Metaverse service platform to encrypt transaction information thoroughly and store traces of criminal activities solely in the blockchain ledger. Transactions made from blockchain ledgers can be easily detected. However, there can be challenges in determining the real identities of the individuals involved in these transactions. Various crimes such as theft, fraud, and money laundering can occur in stores opened within the Metaverse. Measures such as restricting the proximity between avatars to prevent crimes like avatars causing harm to each other have been considered. In February 2022, Meta announced the activation of a feature called "Personal Boundary" to provide avatars with secure distance protection. However, there is currently no effective measure in place specifically targeting financial crimes in the Metaverse environment. In 2012, the Dutch Supreme Court issued a conviction against two young individuals who stole a virtual amulet from another player in the online game Runescape, citing that the time and effort spent in obtaining these amulets had a value. With this decision, virtual treasures or virtual currencies used in online games became recognized as goods with real value in the Netherlands. It has been determined through text mining during this conversation that there are no court decisions in Turkey that explicitly mention the term "metaverse." However, it is expected that a settled precedent will emerge in the future as a result of cases brought before the judicial authorities. In Turkey, there are currently no specific regulations stating that "account, character, currency, and treasure information of online games must be stored as electromagnetic records on the game server. The user of the game has clear ownership rights over the account, character, currency, and treasure, and has the right to control their account, desire the protection of these digital assets, and seek compensation for them."

Cryptocurrency Crimes

Within the scope of the Metaverse, financial cybercrimes have been observed to occur on a significant scale in recent years, including large-scale theft of cryptocurrencies from exchanges and the sale of fake or suspicious cryptocurrencies (Katterbauer, 2022). The proliferation and recognition of cryptocurrencies also increase the potential for their misuse. Concerns in this regard encompass the illicit use of cryptocurrencies for activities such as illegal drug trading, theft, ransomware, financing terrorism, money laundering, circumvention of capital controls, and any other unlawful purposes (Atıcı, 2023).

Indeed, cryptocurrency crimes are more commonly observed compared to Metaverse crimes. In this regard, it can be stated that forensic accountants have a certain level of familiarity with cryptocurrency crimes (Al-Dulaimi, 2021). However, due to legal and technological delays, the analysis and investigation of crimes related to digital currencies present numerous challenges in forensic accounting. The lack of clarity in legislation concerning digital currencies necessitates an improvement in the legal perception of digital currency-related crimes. Establishing an effective investigation and evidence-gathering mechanism within judicial authorities, along with interaction with forensic accountants during the process, is believed to yield various positive outcomes. Additionally, the development of court precedents related to cryptocurrency crimes will enable forensic accountants to enhance their analyses.

Since the emergence of Bitcoin in 2009, numerous digital currencies have been created one after another. The proliferation of digital currencies and their widespread use has not only changed the rules of market transactions but has also had profound implications for traditional crimes. Private digital currencies have become a significant tool or object of crime. Changes in the form and circulation structure of digital currency have necessitated the introduction of criminal sanctions for offenses involving digital currency by also bringing about changes in the legal attributes of the currency.

It is necessary to determine that, according to the legislation in force in Turkey, Bitcoin is not recognized as legal tender, and therefore, it cannot be considered as currency under Turkish Law (Yılmaz, 2021). Bitcoin is not an economic currency; although it possesses some functions of a currency, it is essentially still a commodity due to limitations in its market size and public acceptance. Criminals often employ various methods to conceal the transactional pathway of digital currency when using it for illegal and criminal activities. While traditional crimes assist in the concealment of illicit proceeds by blending stolen money with legal currency, more complex mechanisms can be employed in cryptocurrency transactions.

Virtual currency possesses characteristics such as anonymity, decentralization, and globalization, which can assist criminals in money laundering. The anonymous nature of Bitcoin and the lack of oversight by a third party have made it a convenient system for criminals to conduct payment transactions (Demir, 2023). During a transaction, while the virtual currency account, transaction address, and amount can be identified, a random "public key" and "private key" pair are generated for each virtual currency transaction. As a result, it becomes difficult to determine the real IP address of the actual user and the user of the account. From virtual currency wallet addresses to network scanning records, electronic evidence becomes a kind of crime scene. The identification and reporting of electronic evidence are key to resolving virtual currency cases. Forensic accountants play a significant role in ensuring the integrity of electronic evidence, but they also need to collaborate with relevant technology companies to enhance the effectiveness of evidence collection.

The Function of Forensic Accounting in Next-Generation Financial Crimes

To investigate crimes such as money laundering and virtual theft that occur in the Metaverse, digital forensic investigations are necessary (Israfin, Imamy, & Wirawan, 2023). Due to the unique technical features of the Metaverse and the cryptocurrencies used within it, new generation financial crimes possess characteristics of privacy, complexity, and prevalence. In addition to forensic accountants being mindful of the technical risks brought about by new technologies, they also need to develop investigation technologies in line with the features of the Metaverse and cryptocurrencies. Forensic accountants should update their investigation models based on the characteristics of crimes involving the Metaverse and cryptocurrencies and collaborate with third parties, such as forensic computing experts, to strengthen their investigations.

The Metaverse represents a virtual world, while cryptocurrencies are digital forms of virtual currency. However, it can be expressed that ultimately the Metaverse and cryptocurrencies are financed with real-world currencies. The values such as Turkish Lira, US Dollars, Euros, etc., held in a regular bank account, are converted into the cryptocurrency accepted by the Metaverse platform for various purposes such as buying virtual properties, purchasing NFTs, or conducting e-commerce transactions. When this converted value is subjected to theft, fraud, or financial crimes in any way, it creates a real-world impact and victimization. During the use of the Metaverse and cryptocurrencies, people are more vulnerable to financial crimes. Using a technology does not necessarily equate to understanding or comprehending it fully. Moreover, the requirements for cybersecurity further increase the complexities of Metaverse and cryptocurrency usage. There are numerous risks involved, such as attacks on accounts, wallets, or avatars, irreversible financial transactions, fraudulent or duplicate transactions, and the exploitation of cybersecurity vulnerabilities for fraudulent activities.

Metaverse is envisioned as the living space of post-humans, giving rise to the concept of digital life, including digital humans, electronic humans, virtual humans, information humans, and more. NFTs, cryptocurrencies, and metaverse technologies are closely related to real-world rights. Forensic accountants find their field of work in addressing the grievances and ensuring justice when these rights are violated by financial crimes. Investigations into Metaverse and cryptocurrency cases are typically conducted by forensic accountants upon the request of the victim or their legal representative. Once the evidence and documents of the incident are compiled into a report, they are submitted to the judicial authorities, leading to further legal investigations and proceedings. It is crucial to take preventive measures at national, social, and individual levels before the dimensions of Metaverse and cryptocurrency crimes expand further.

TEXT MINING APPLICATION IN COURT DECISIONS

Statistical information regarding metaverse and cryptocurrency crimes in Turkey is not regularly shared with the public. However, it has been observed that the total number of crimes queried with the keyword "Bitcoin" in search engines is significantly higher than the total number of crimes queried with the keyword "digital currency." By applying text mining analysis techniques to Turkish judicial decisions, results similar to those attempted to be expressed in Table 1 have been obtained. The data in Table 1 was obtained from http.// www.lexpera.com.tr and the table was created by the authors.

When examining Table 1, it is observed that out of 176 decisions from the courts of first instance, the term "bitcoin" or "cryptocurrency" appears in the text. One decision is from 2019, one from 2020, 13 from 2021, and finally, three decisions are from 2022. By analyzing the keywords in the text using text mining techniques, it is concluded that four cases are related to Bitcoin-related

Table 1: In First Instance Court Decisions Regarding Bitcoin

Decision Authority	Decision Number	Subject
Bakırköy 2nd Commercial Court of First Instance	E. 2020/27 K. 2021/585, T. 10.6.2021	Claiming Compensation for Losses in Bitcoin Buying and Selling (Negative Determination of Exchange Instrument)
Bakırköy 7th Commercial Court of First Instance	E. 2019/153 K. 2019/716, T. 12.7.2019	No cryptocurrency debt belonging to the company
Ankara 3rd Intellectual and Industrial Property Rights Court	E. 2021/143 K. 2021/401, T. 9.12.2021	Regarding the inability to use the term "Bitcoin" as a trademark
Ankara 3rd Intellectual and Industrial Property Rights Court	E. 2021/142 K. 2021/397, T. 9.12.2021	Regarding the inability to use the term "Bitcoin" as a logo
Ankara 10th Commercial Court of First Instance	E. 2020/321 K. 2021/122, T. 8.3.2021	Demanding a Loss Certificate as a result of the system being hacked and Bitcoin being requested
Ankara 11th Commercial Court of First Instance	E. 2020/333 K. 2021/928, T. 7.12.2021	Demanding a Loss Certificate as a result of a Bitcoin-related cyber attack
İstanbul 21st Commercial Court of First Instance	E. 2019/1326 K. 2021/688, T. 12.10.2021	The plaintiff, who operates a hotel, engaged in Bitcoin transactions based on the guidance of an individual named "...," deposited a total of 115,000.00 TL, but after some time, couldn't access their account, and their account was emptied by a person named "..."
Bursa 3rd Commercial Court of First Instance	E. 2021/411 K. 2021/545, T. 22.6.2021	Thodex platform (… Technologies Inc.) investment company involved in Bitcoin and derivatives exchange fraud
Ankara 3rd Commercial Court of First Instance	E. 2020/562 K. 2021/239, T. 29.3.2021	Demanding a Loss Certificate as a result of a Bitcoin-related cyber attack
Ankara 14th Commercial Court of First Instance	E. 2020/582 K. 2021/39, T. 25.1.2021	Establishment of a cryptocurrency trading system
İstanbul 5th Commercial Court of First Instance	E. 2021/269 K. 2022/339, T. 12.5.2022	Gradual sale of Bitcoins in the account and conversion into Turkish Lira (TL), money laundering
İstanbul 11th Commercial Court of First Instance	E. 2021/602 K. 2022/131, T. 11.2.2022	Repetitive transactions in cryptocurrency buying and selling
İstanbul 18th Commercial Court of First Instance	E. 2021/424 K. 2021/737, T. 28.10.2021	Regarding refund fees in cryptocurrency exchanges
İstanbul 21st Commercial Court of First Instance	E. 2019/915 K. 2020/278, T. 2.7.2020	Regarding the process of refund in cryptocurrency buying and selling
İstanbul 7th Commercial Court of First Instance	E. 2021/469 K. 2021/704, T. 6.9.2021	Inaccessibility to the account for cryptocurrency transactions
İstanbul 12th Commercial Court of First Instance	E. 2020/108 K. 2021/219, T. 23.3.2021	Demanding a Loss Certificate as a result of a Bitcoin-related cyber attack
İstanbul 9th Commercial Court of First Instance	E. 2021/672 K. 2022/190, T. 22.3.2022	Unauthorized transactions in cryptocurrency trading platforms
İzmir 7th Commercial Court of First Instance	E. 2021/321 K. 2021/731, T. 30.9.2021	Bitcoin mining with illegal electricity.

Source: http.//www.lexpera.com.tr (Access Date: 01.04.2023), Created by the Authors.

Table 2: Bitcoin in Appeals and Supreme Court Decisions

Decision Authority	Decision Number	Subject
Samsun Regional Court of Justice, 1st Civil Chamber	E. 2020/1488 K. 2020/1799 T. 19.11.2020	...gave 105,000 TL to the close friend, who has been a friend for 15 years, to be invested in Bitcoin, along with a certain amount of gold and a small sum of cash.
Bursa Regional Court of Justice, 5th Civil Chamber	E. 2021/2349 K. 2022/781 T. 6.6.2022	Bitcoin mining was conducted using company resources, but the profits generated were not transferred to the company accounts.
Istanbul Regional Court of Justice, 14th Civil Chamber	E. 2020/1588 K. 2020/1107 T. 22.10.2020	The total profit and principal amount from Bitcoin trading amounted to 165,025.76 USD. The debtor defaulted on the payment, and the password used was changed.
Court of Cassation, 6th Criminal Chamber	E. 2020/1158 K. 2020/2598 T. 7.7.2020	The forcible acquisition of computer password and its use in Bitcoin transactions.
Istanbul Regional Court of Justice, 27th Civil Chamber	E. 2019/501 K. 2020/1218 T. 10.6.2020	Termination of employment contract due to placing the devices used for Virtual Currency Mining (Bitcoin) in the information processing server room.
Ankara Regional Court of Justice, 22nd Civil Chamber	E. 2023/94 K. 2023/153 T. 17.2.2023	Seizure of Bitcoin accounts.
Istanbul Regional Court of Justice, 3rd Civil Chamber	E. 2023/308 K. 2023/869 T. 21.3.2023	Bitcoin and cryptocurrency trading platform fraud..
Izmir Regional Court of Justice, 17th Civil Chamber	E. 2022/727 K. 2022/864 T. 12.5.2022	Loss incurred due to the disappearance of bitcoins purchased through the company's website in the digital realm and inability to sell them.
Istanbul Regional Court of Justice, 17th Civil Chamber	E. 2023/148 K. 2023/191 T. 16.2.2023	The right to reject advertising requests from a country where advertising for cryptocurrencies is not permitted.
Ankara Regional Court of Justice, 20th Civil Chamber	E. 2020/1093 K. 2022/379 T. 25.3.2022	The prohibition of using the term "cryptocurrency" as a registered trademark.
Ankara Regional Court of Justice, 20th Civil Chamber	E. 2020/70 K. 2021/1164 T. 30.9.2021	The prohibition of using the term "cryptocurrency" as a registered trademark.
Ankara Regional Court of Justice, 21st Civil Chamber	E. 2023/141 K. 2023/220 T. 22.2.2023	Imposing interim measures on accounts related to cryptocurrencies, electronic money, etc.
Istanbul Regional Court of Justice, 19th Civil Chamber	E. 2021/1963 K. 2021/1628 T. 17.9.2021	Freezing the funds in the company's account due to cryptocurrency trading transactions.
Izmir Regional Court of Justice, 11th Civil Chamber	E. 2022/625 K. 2022/602 T. 12.4.2022	Engaging in unfair competition by featuring other cryptocurrency advertisements.
Istanbul Regional Court of Justice, 12th Civil Chamber	E. 2022/1073 K. 2022/915 T. 16.6.2022	Engaging in repeated transactions in cryptocurrency buying and selling.
Istanbul Regional Court of Justice, 19th Civil Chamber	E. 2021/3166 K. 2021/2411 T. 21.12.2021	Inability to access the account in cryptocurrency buying and selling.
Istanbul Regional Court of Justice, 13th Civil Chamber	E. 2023/522 K. 2023/491 T. 23.3.2023	Making cryptocurrency buying and selling transactions worth 700,000 USD with commission payment.
Istanbul Regional Court of Justice, 37th Civil Chamber	E. 2022/2128 K. 2023/826 T. 22.3.2023	Failure to reimburse the amount paid for cryptocurrency asset purchases and sales.
Istanbul Regional Court of Justice, 44th Civil Chamber	E. 2021/1354 K. 2021/1325 T. 4.11.2021	Making various commitments regarding cryptocurrencies, collecting substantial amounts of money from customers, but failing to fulfill the commitments.

Source: http.//www.lexpera.com.tr (Access Date: 01.04.2023), Created by the Authors.

cyber attacks, one case is related to Bitcoin mining with illegal electricity, five cases are related to Bitcoin trading fraud, and one case is related to money laundering. The search was conducted using the common keywords "Bitcoin," "cryptocurrency," and "digital currency." The data in Table 2, obtained from http://www.lexpera.com.tr, is created by the authors of the table.

According to the analysis of Table 2, it is concluded that there are 19 decisions, with 4 decisions made in 2020, 4 decisions in 2021, 5 decisions in 2022, and 6 decisions in 2023. When the words in the decisions were examined using text mining techniques, it was observed that 1 decision involved robbery, 1 decision involved unfair competition, and 1 decision involved trademark usage, while the remaining decisions were related to buying and selling transactions.

CONCLUSION

In today's world, communication, transportation, software, the internet, artificial intelligence, and computer technologies are rapidly advancing. While these advancing technologies bring beneficial outcomes for humanity, they also create opportunities for criminals. The Metaverse or virtual world is a relatively new technological ecosystem compared to cryptocurrencies. Measures to prevent financial crimes that can be committed in the Metaverse world, fighting against criminals, and conducting crime investigations do not yet have a well-defined methodology. In contrast, there is a relatively more established structure regarding financial crimes related to cryptocurrencies since they are more commonly observed. The currency that is valid in the Metaverse world is cryptocurrency.

Forensic accounting is an effective forensic discipline in the investigation of financial crimes. It can be observed that various fields such as law, auditing, criminology, psychology, and graphology have a perspective closely related to the science of accounting. Forensic accounting comes into play when accounting analysis is required in legal cases. In the resolution of metaverse and cryptocurrency financial crimes, significant responsibilities lie with forensic accountants. In the virtual world of the metaverse, forensic accountants can be consulted in cases involving the theft, fraud, manipulation, corruption, and misuse of digital assets known as NFTs. Furthermore, in the perpetration of new generation digital financial crimes such as fraud and money laundering using cryptocurrencies, forensic accountants can be sought for assistance in analyzing the incidents.

Whether the rules designed by the Metaverse are consistent with legal norms in the real world is yet to be determined, as there are currently no detailed legislative regulations specifically addressing Metaverse and crypto-related crimes. It is expected that regulations will be established regarding information security, identity verification, the valuation of crypto assets, and determining which behaviors constitute crimes. The digital identity represented by avatars in the metadata repository serves not only as an online account holder for users in the Metaverse but also grants ownership rights due to its facilitation of transactions such as crypto and NFT trading. It is crucial to establish clear guidelines for determining the value of digital assets and defining the crimes and penalties associated with offenses related to digital assets.

REFERENCES

Akturan, K.E. (2023). Metaverse'ün Yapım Sektöründeki Etkilerinin İncelenmesi, İstanbul Kültür Üniversitesi, Lisansüstü Eğitim Enstitüsü, Yüksek Lisans Tezi, İstanbul, 5-6.

Al-Dulaimi, A.F.T.A. (2021) Kripto Para: Muhasebeleştirilmesi Ve Kripto Para Dolandırıcılığının Tespitinde Adli Muhasebenin Rolü, Erciyes Üniversitesi, Sosyal Bilimler Enstıtüsü, Yüksek Lisans Tezi, Kayseri. 103-104

Altaylı, E. (2022), Adli Muhasebe-Adli Müşavirlik Kapsamında Hile Araştırmacılığı, Regresyon (Bağlanım) Modeli İle Analizi Ve Raporlanması, Hacı Bayram Veli Üniversitesi, Lisansüstü Eğitim Enstitüsü, Yüksek Lisans Tezi, Ankara, 31-32.

Arıcı, S.T. (2023), Çağımıza Global Köy Olarak Bakmak, Metaverse Yaşamlar, Başkent Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara, 87-88.

Atak, M.C. (2022), Metaverse'ün Çalışma Hayatı Üzerine Etkisi: Bir Delphi Çalışması, Başkent Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara, 40-41.

Atıcı, G. (2023), Dijital Ekonomi Blokzinciri ve Finansal Sistem, Nobel Yayınevi, Ankara, 58.

Aytekin, M.İ., (2022), Adli Muhasebe Kapsamında Uzman Tanıklık (Bilirkişi Tanıklığı), Dava Destekleri, Hile, Yolsuzluk Ve Suistimal Denetçiliği: Karaman İlinde Bir Araştırma, Karamanoğlu Mehmetbey Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Karaman, 30-31.

Baltacıoğlu Ş. (2023), Metaversede Mülkiyet Sahibi Olan Ve Olmayan Kişilerin Psikolojik Ölçeklerle Değerlendirilmesi Ve Karşılaştırılması, Cumhuriyet Üniversitesi, Aile Hekimliği Anabilim Dalı, Yüksek Lisans Tezi, Sivas, 7-8.

Başoğlu, R. (2023), Siyasal İletişimde Metaverse'ün Kullanılma Potansiyeli: Fırsatlar ve Tehditler, Hasan Kalyoncu Üniversitesi, Lisansüstü Eğitim Enstitüsü, Yüksek Lisans Tezi, Gaziantep, 43-44.

Beşinci, E. (2023), Metaverse'te Pazarlama Ve Vrchat'te Bir Pazarlama Deneyimi Tasarımı, Işık Üniversitesi, Lisansüstü Eğitim Enstitüsü, Yüksek Lisans Tezi, İstanbul, 39-40.

Bil, H. (2023), Ekonomide Kripto Para Kullanım Tercihi: Siirt Üniversitesi Örneği , Siirt Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Siirt, 14-15.

Cheong, B.C. (2022), Avatars in the Metaverse: Potential Legal Issues and Remedies, Int. Cybersecurity Law Rew. 3, 467-494.

Çağlar, O.B. (2022), Dijital Varlık Ekonomisi Atıl Kaynakların Blokzincir İle Finansal Varlığa Dönüşümü, Pusula Yayıncılık, İstanbul, 144.

Çekmen, Y. (2022), Muhasebede Yapılan Hatalar, Hileler Ve Adli Muhasebe, İksad Yayınevi, Ankara, 65.

Demir, N. (2023), Kripto Para Ve Kara Para Aklama İlişkisi, Fırat Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Elazığ, 42-43.

Güngör, İ. (2022), Metaverse'de Influencer Pazarlamaya Yönelik Bir İnceleme, TOBB Ekonomi Ve Teknoloji Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara, 58-59.

Gürbüz, R. (2023), Yenilikçi Finansal Yatırım Aracı Olarak Kripto Para Ve Kripto Para Yatırımcılarının Ekonomi Okuryazarlıkları Üzerine Bir Araştırma, Muğla Sıtkı Koçman Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Muğla, 17-18.

Güven, İ. (2022), Metaverse'te Arsa Değerini Belirleyen Faktörler, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul, 34-35.

Gönülal, M. (2022), Marka İletişimi Açısından Yeni Bir Kanal Olarak Metaverse, Bolu Abant İzzet Baysal Üniversitesi, Lisansüstü Eğitim Enstitüsü, Yüksek Lisans Tezi, Bolu, 31-32.

Israfin, N. N.,Imamy, S.N. & Wirawan A.R.,(2022), Potential of Money Laundering in the Metaverse Era, The 4 th Open Society Conference OSC 2022 Faculty of Law, Social and Political Sciences, 112-121.

Katterbauer, K., Syed, H. & Cleenewerck, L. (2022), Financial Cybercrime in the Islamic Finance Metaverse, Journal of Metaverse, V.2(2), 56-61.

Kaya, E. (2022), Metaverse Meta İnsana Hazır Mısın?, Nemesis Kitap, İstanbul, 28.

Koç, F. N. (2023), Dijital Pazarlamanın Metaverse Fenomenine Sunduğu Fırsatlar Ve Sınırlılıklar: Tekstil Sektörü İncelemesi, İstanbul Gelişim Üniversitesi Lisansüstü Eğitim Enstitüsü, Yüksek Lisans Tezi, İstanbul, 17-18.

Özkul, F. (2022), Kripto Varlıklar Muhasebesi Blokzincir Teknolojisi İle Muhasebe Dünyasında Paradigma Değişimine Doğru, Hümanist Yayınevi, İstanbul, 70.

Özer, İ. (2022), Adli Muhasebe Boyutunda Bilirkişilik Mesleği Ve Meslek Mensuplarının Algı Düzeylerinin Demografik Özelliklere Göre Tespiti, Batman Üniversitesi, Lisansüstü Eğitim Enstitüsü,Yüksek Lisans Tezi, Batman, 3-5.

Qin, H. X.,Wang, Y. & Hui,P. (2022), Identity, Crimes, and Law Enforcement in the Metaverse, arXiv:2210.06134v2, 1-13.

Seo, S., Seok, B. & Lee, C. (2023), Digital Forensic Investigation Framework For The Metaverse, J Supercomput 79, January 2023, 9467–9485.

Smaili, N. & Raymond, A.R. (2022), Metaverse: welcome to the new fraud marketplace, Journal of Financial Crime, 21 July 2022, https://doi.org/10.1108/JFC-06-2022-0124, 1-15.

Tekin, Z. (2022), Metaverse 101, Scala Yayıncılık, İstanbul, 1-3.

User, E. (2022), Metaverse, Cinius Yayınları, İstanbul, 66-67.

Yılmaz, A.(2021), Kripto Para Birimi Bitcoin ve Bitcoin'in Türk Sermaye Piyasası Hukuku Açısından Değerlendirilmesi, On İki Levha Yayıncılık, İstanbul. 43-44.

Yüksel, H. (2022), Hile, Etik Davranış Ve Kalite Kavramına, Adli Muhasebe Ve Adli Müşavirlik Çerçevesinde Genel Bir Bakış: Giresun İlindeki Banka Çalışanları Üzerinde Bir Alan Araştırması, Giresun Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Giresun, 104-105.

Zhang, Q. (2022), Rule of the Metaverse, Metaverse, V.3 (1), 1-6.

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z., (2023), Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities, IEEE Open Journal of the Computer Society, 2023, V: 4, 37-49.

http.//www.lexpera.com.tr (Access Date: 01.04.2023).