

Comparative Study of Criminal Protection of Digital Assets in the Metaverse in the European Union and Japan

1. Rasool Moradi Emamgheisi[✉]: Ph.D. Student, Department of Law, Na.C., Islamic Azad University, Najafabad, Iran

2. Yasin Saeedi^{✉*}: Department of Law, Isf.C., Islamic Azad University, Isfahan, Iran

3. Razie Ghasemi[✉]: Department of Law, Ti.C., Islamic Azad University, Tiran, Iran

*Correspondence: Yasinsaeedi@iau.ac.ir

Abstract

With the increasing expansion of emerging technologies and the advent of complex virtual environments such as the metaverse, digital assets have become one of the most significant forms of property within emerging platforms. This transformation has confronted criminal justice systems with novel challenges. The principal issue of this study is how digital assets in the metaverse can be protected against criminal threats and what similarities and differences exist between the approaches adopted by the European Union and Japan in this regard. The aim of this research is to conduct a comparative examination of the criminal protection of digital assets in the metaverse within two leading legal systems, namely the European Union and Japan, and to propose models for the Iranian legal system, which has thus far lacked a coherent framework in this field. The necessity of this research lies in the increasing growth of metaverse-related crimes, the inadequacy of victim protection, and the legislative vacuum within the Iranian legal system. The main research question is: "How do the criminal justice systems of the European Union and Japan protect digital assets in the metaverse, and what models can be extracted for the reform of criminal legislation in Iran?" The findings of the study indicate that Japan, through reliance on specific legislation concerning crypto-assets and newly enacted criminal regulations, and the European Union, through the adoption of innovative legal frameworks such as the Markets in Crypto-Assets (MiCA) Regulation, are advancing effective criminal protection of digital assets. In conclusion, the study emphasizes the necessity of reforming Iranian criminal laws, particularly in the fields of cybercrime and digital property. This research was conducted using a descriptive-analytical method with a comparative approach.

Keywords: Digital Asset, Metaverse, Criminal Protection, European Union, Japan, Iran, Cybercrime.

Received: 22 February 2026

Revised: 03 June 2026

Accepted: 10 June 2026

Initial Publication: 12 October 2026

Final Publication: 01 February 2027



Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Citation: Moradi Emamgheisi, R., Saeedi, Y., & Ghasemi, R. (2027). Comparative Study of Criminal Protection of Digital Assets in the Metaverse in the European Union and Japan. *Legal Studies in Digital Age*, 6(2), 1-12.

1. Introduction

Rapid developments in emerging technologies, particularly the emergence of the metaverse as one of the most important manifestations of Web 3.0, have created new challenges for legal systems across the world. In the metaverse, users can own

digital property, conduct transactions, enter into contracts, and even become victims of crime. These assets, including cryptocurrencies, non-fungible tokens, and other virtual property, have acquired considerable economic value and are comparable to traditional property in terms of their role and function. Under such conditions, criminal protection of these assets is not only a technical and legal necessity but also a fundamental requirement for ensuring criminal justice and maintaining economic security in cyberspace.

With the increasing expansion of digital interactions in the metaverse, cybercrimes related to digital assets have also increased. In many countries, particularly in developed legal systems such as the European Union and Japan, legislative and executive authorities have recognized the need to confront these crimes and have designed and implemented legal frameworks for the criminal protection of digital assets. Japan, relying on the Payment Services Act and specific supervisory regulations in the field of crypto-assets, has taken effective steps in this regard. The European Union, through the adoption of the Markets in Crypto-Assets Regulation (MiCA), also seeks to regulate the crypto-asset space and confront the criminal threats associated with it.

By contrast, in Iran, no coherent legislation has yet been enacted for the criminal protection of digital assets in the metaverse. The Computer Crimes Law adopted in 2009, although an initial step toward criminalizing unlawful activities in cyberspace, cannot provide a comprehensive response to current challenges because of its inadequate coverage of emerging digital assets, including metaverse property and tokens. The legislative vacuum in this field may increase the vulnerability of victims, expand organized digital crime, and undermine users' trust in the security of the metaverse environment.

The present study is necessary because Iran is currently on the threshold of broader engagement with emerging technologies such as the metaverse, and the increasing digitalization of assets compels the national criminal justice system to reconsider traditional concepts of property and criminal liability. A comparative examination of advanced legal systems can provide a suitable model for drafting laws aligned with the new requirements of cyberspace. Moreover, the absence of effective criminal protection for this type of asset in Iran may pave the way for new forms of economic corruption and widespread violations of users' proprietary rights. The central question of this study is:

“How do the criminal justice systems of the European Union and Japan protect digital assets in the metaverse, and what models can be used to reform criminal legislation in Iran?” This study can assist the legislative process in Iran in several respects: first, by explaining the manifestations of crimes related to digital assets and analyzing models of criminalization in Europe and Japan, it helps Iranian legislators understand the nature of emerging crimes. Second, by examining successful measures and legal challenges in these systems, it makes it possible to avoid repeating similar mistakes in Iran's criminal policy. Third, the present study can provide the basis for drafting a comprehensive legal framework for the recognition, ownership, transfer, and criminal protection of digital assets in the metaverse in a manner that ensures criminal justice in cyberspace and strengthens user security. For this reason, the findings of this research are significant not only from a theoretical perspective but also in the fields of legislation and the administration of justice.

2. The Concept and Nature of Digital Assets in the Metaverse

The metaverse can be understood as a new generation of the internet that transfers human interactions from the traditional two-dimensional web environment to three-dimensional and virtual reality environments; it is a pervasive and immersive environment in which users can interact with one another and with the digital environment through avatars, spaces, and virtual objects (Shen et al., 2023). The metaverse is a combination of advanced technologies such as augmented and virtual reality, artificial intelligence, the Internet of Things, blockchain, and Web 3.0, which together provide a platform for digital life and economic, social, and cultural interactions in three-dimensional form (Kalpokas & Kalpokiene, 2023). In this context, digital assets refer to intangible objects that are created, stored, or exchanged in virtual environments. These assets include items such as virtual lands, digital artworks, avatar wearables, decorative objects, and even digital identities that users can create, own, or trade (Damodaran, 2022).

The concept of digital assets in the metaverse can be understood within the framework of the continuous evolution of the web, from the formation of human communication in Web 1.0 and interaction with objects through the Internet of Things to machines' understanding of the meaning of data in the semantic web (Sheng et al., 2016). These developments ultimately provided the basis for the web to move toward a visual, interactive, and three-dimensional experience, which became the

foundation for the formation of the metaverse. Although the idea of the three-dimensional web is not new and technologies such as VRML had made this possibility available since 1994, they did not become widespread because of graphical and computational limitations (Li et al., 2022). By contrast, platforms such as Second Life, Roblox, and Minecraft, through cloud infrastructure and user-friendly environments, enabled users to create and own digital assets without requiring programming knowledge (Andrade et al., 2020; Han et al., 2023; Lozano-Duran et al., 2023).

Digital assets in the metaverse have functions beyond aesthetics and create independent economic and cultural identities for users. Users can buy, sell, or exchange these assets as unique items in virtual worlds. These assets have also found broad applications in fields such as education, tourism, museums, and digital galleries. For example, many museums have used the metaverse to strengthen their digital identity and present their works to a global audience (Giannini & Bowen, 2023). During the COVID-19 pandemic, these capacities also created an opportunity for virtual visits to become an alternative experience to physical visits (Cotter et al., 2022). From a cultural perspective, these spaces can play a key role in protecting historical and artistic heritage against risks such as war and climate change (Kantaros et al., 2023).

Accordingly, blockchain technology, and especially non-fungible tokens, have added a new legal and economic dimension to digital assets in the metaverse. NFTs allow artists and content producers to prove ownership of their works and sell them as unique digital assets (Damodaran, 2022). This capacity not only facilitates the authentication of ownership and the protection of moral rights but also creates new markets for the trade of digital art (Balis, 2022). In other words, by relying on NFT technology, Web 3.0, and virtual reality, the metaverse has created an innovative platform for the creation, display, and commercialization of digital assets, in which traditional concepts of ownership have been transferred to the digital realm; this corresponds to what Kalpokas describes as the dominance of digital media over all spheres of social life (Kalpokas & Kalpokiene, 2023).

2.1. The Position of Digital Assets in Property Law

In property law, digital assets, as an emerging phenomenon, have gained an increasingly important position because these forms of property exist electronically and, unlike traditional property, are inherently intangible and are stored as digital data in infrastructures such as blockchain or cloud servers (Fairfield, 2022). This feature makes digital property easily transferable on the one hand and independent of geographical borders and physical constraints on the other. Such characteristics have created the need to rethink traditional concepts of property, because digital assets do not fully correspond to existing legal structures, which have mainly been designed for tangible property.

In addition to their intangible nature, rapid transferability, and independence from location, the examples of digital property have also become highly diverse, ranging from digital currencies such as Bitcoin to non-fungible tokens that represent ownership of artworks, music, or digital data. These new forms of property make it possible to prove ownership and conduct transactions without intermediaries, yet they also create legal challenges. One of the most important of these challenges is the issue of determining actual ownership, because in the digital environment, proof of ownership relies on technical tools, which may be accompanied by ambiguity or interpretive disagreement in traditional legal systems (Ayoubi, 2024). In addition, threats such as cyber fraud, breaches of platform security, and non-compliance with digital contracts have created significant legal gaps in protecting holders of these assets.

In this regard, the position of digital assets in property law requires the development of new and coherent legal frameworks that cover the various dimensions of this type of asset. In addition to rules concerning ownership and transfer, states must enact tax regulations suited to digital assets and provide mechanisms for taxing income derived from such property. Moreover, the protection of users' rights against contractual breaches and security risks must be regarded as an inseparable component of legal policymaking. The growing global experience in the use of digital assets shows that the absence of clear regulations can lead to judicial disputes and a decline in public trust; therefore, revising the traditional principles of property law and adapting them to the requirements of the digital world is an unavoidable necessity.

3. The Impact of the Expansion of the Metaverse on the Emergence of New Crimes in Criminal Law

The expansion of the metaverse as a virtual and interactive environment in which users interact with one another and their surroundings through digital avatars has created a platform for the emergence of new crimes in the field of criminal law. This is particularly evident in crimes such as sexual harassment, which have traditionally been defined in physical space, whereas in the metaverse such crimes may occur virtually and without “physical contact.” For this reason, a conflict has emerged between traditional laws and new technologies (Kalpokas & Kalpokiene, 2023; Shen et al., 2023). This issue has caused countries to face uncertainty in dealing with crimes such as attacks against avatars, that is, users’ digital representations, even though the psychological harm caused by these virtual events may be comparable to the harm caused by similar physical crimes (Kalpokas & Kalpokiene, 2023).

Because the metaverse is built upon the physical world and supported by technologies such as augmented reality, virtual reality, blockchains, and artificial intelligence, the possibility of committing crimes in it has expanded considerably. For example, simultaneous hacking attacks against several avatars and the creation of widespread virtual violations not only increase the number of victims but also produce broader social and psychological effects through the immediate and global transmission of harmful content (Kalpokas & Kalpokiene, 2023; Kayani & Hasan, 2024). It has been predicted that by 2030, a significant portion of the global population may spend at least one hour per day in metaverse environments, which will increase both criminal opportunities and threats (Shen et al., 2023).

Unfortunately, current criminal laws have largely been shaped on the basis of physical and tangible harms and have not yet been able to adapt themselves to harms arising from the virtual world. This mismatch between law and technology can encourage a wave of new crimes and endanger social stability (Kalpokas & Kalpokiene, 2023). On the other hand, the absence of an integrated international legal framework for confronting crimes in the metaverse, due to the geographical breadth of this space and differences among national laws, represents a major challenge for legislators and law-enforcement authorities (Kalpokas & Kalpokiene, 2023; Kayani & Hasan, 2024). Therefore, the need to develop modern criminal laws and international cooperation for managing metaverse crimes is strongly felt.

4. European Union Regulations on Digital Assets and Their Criminal Protection

European Union regulations on digital assets have taken shape particularly through the MiCA legal framework, which aims to ensure investor protection, preserve market stability, and facilitate innovation in the field of digital assets (European Parliament, 2023). These regulations, through a technology-neutral and activity-based regulatory approach, seek to manage the technical complexities of digital assets without restricting innovative developments in this field (Pundziene & Gadeikiene, 2023). In addition, these regulations address challenges related to security, fraud, and market integrity; because digital assets have an emerging structure, the creation of a comprehensive and harmonized framework among EU member states is especially important for ensuring market integrity and investor protection (Avci & Erzurumlu, 2023).

From the perspective of criminal protection, European Union regulations are developing mechanisms to counter crimes related to digital assets, including fraud, money laundering, and misuse of information (European Parliament, 2023). These supervisory and criminal measures are designed to promote transparency and provide reassurance to investors. Their positive effects can be observed especially in member states such as Latvia, which provides an example of national alignment with EU regulations (Burilov, 2019). Latvia, given its extensive efforts to adapt domestic laws to EU frameworks, provides a suitable context for analyzing the implementation of European regulations and their effects at the national level (Kiskis, 2024).

In addition, recent studies show that blockchain technology and asset tokenization, while creating new financial opportunities, require the development of precise legal and criminal mechanisms to protect investors’ rights and market stability (Garcia-Teruel & Simon-Moreno, 2021). Since digital assets are divisible and rapidly transferable, yet simultaneously exposed to risks such as fraud and cybercrime, EU laws seek to respond to these challenges by using hybrid and adaptable legal frameworks (Chiu & Greene, 2019; Gan et al., 2020). Therefore, European policymakers seek to strike a balance between

supporting digital innovation and ensuring investor security, a matter that requires continuous cooperation among supervisory bodies, legal experts, and market participants. This issue is discussed in greater detail below.

4.1. *The Role of MiCA in Protecting Digital Assets*

The role of MiCA in protecting digital assets as a comprehensive legal framework at the European Union level is highly crucial and decisive. These regulations were drafted to create legal harmonization among member states and fill existing legal gaps in the field of digital assets ([European Parliament, 2023](#)). One of the most important features of MiCA is its technology-neutral approach, which allows rules to be applied regardless of specific technologies such as blockchain or other tokenization tools, thereby enabling faster adaptation to technological innovations ([Pundziene & Gadeikiene, 2023](#)). This approach makes the regulations applicable to different types of digital assets while also enabling the development of new markets and increased competition.

From the perspective of investor protection, MiCA provides transparency, disclosure, and risk-management requirements for issuers of digital assets and related service providers ([Garcia-Teruel & Simon-Moreno, 2021](#)). These requirements help reduce the risks of fraud, deception, and abuse, and protect investors against dangers arising from emerging digital-asset markets. MiCA also increases the level of trust and market integrity by establishing precise standards for the issuance and trading of tokens, thereby contributing to the stabilization of financial markets based on digital assets ([Swinkels, 2023](#)).

Accordingly, the role of MiCA goes beyond the mere creation of legal order and functions as an instrument for promoting sustainable innovation in the digital economy. By providing a clear and predictable legal environment, these regulations allow member states, including Latvia, to use emerging technologies such as asset tokenization in a secure and controllable manner and thereby expand the investment environment ([Burišov, 2019](#); [Kiskis, 2024](#)). This leads to the attraction of new capital, the facilitation of financial processes, and ultimately the strengthening of the digital economy at the European Union level. Thus, by creating a coherent, transparent, and technology-oriented framework, MiCA plays a fundamental role in enhancing legal certainty, increasing investor confidence, and strengthening the infrastructure of digital-asset markets in the European Union. These regulations not only fill legal gaps but also significantly enhance investor protection by providing requirements for transparency, risk management, and supervision over digital-asset services. Furthermore, by creating a predictable legal environment, MiCA facilitates the path of innovation and the wider use of emerging technologies such as tokenization, contributing to the formation of a competitive and sustainable market in Europe's digital economy.

4.2. *Analysis of the European Union Criminal Justice System in Confronting Metaverse Crimes*

The European Union criminal justice system has taken important steps in dealing with crimes related to the metaverse and digital assets in order to provide suitable legal frameworks for confronting new digital threats. In particular, MiCA was designed with the aim of fully and comprehensively regulating services related to crypto-assets so as to increase investor security by requiring authorization from supervisory authorities and aligning national laws with EU regulations ([European Parliament, 2023](#)). However, the inherent challenge of distributed ledger technology, which restricts direct supervision by authorities, remains. The only theoretical solution would be the participation of authorities in every type of crypto-asset, which is difficult to achieve because of the decentralized nature of this technology ([European Parliament, 2023](#)).

On the other hand, before the adoption of MiCA, the European Union had largely adopted a conservative approach toward financial instruments based on distributed ledger technology. Given risks such as money laundering, terrorist financing, and cybersecurity threats, various legal reforms were adopted, including the extension of the Anti-Money Laundering Directive to cryptocurrency exchanges and electronic wallet providers ([European Banking Authority, 2013](#); [European Commission, 2017](#)). Although these preliminary measures were positive steps, the rapid growth and complexity of cryptocurrency markets caused the European Union to lag behind other regions, such as the United States, in some areas ([European Commission, 2018](#)).

Accordingly, criticisms have been raised regarding the compatibility of EU environmental policies with the mining of tokens based on distributed ledger technology, because cryptocurrency mining, due to its high energy consumption and dependence

on resources that may generate pollution, may conflict with the objectives of the European Union's green transition ([European Parliament, 2023](#)). This issue, in addition to legal and regulatory challenges, has introduced environmental dimensions into the European Union criminal and regulatory system and demonstrates the need for greater policy coordination and the development of sustainable solutions in this field. From a criminological perspective, this system, by recognizing the emerging and complex nature of the metaverse—which is a potential platform for crimes such as digital fraud, money laundering, terrorist financing, privacy violations, and cyber exploitation—seeks to reduce risks arising from the anonymity of users, the absence of centralized supervision, and the instability of crypto-asset transactions through frameworks such as MiCA. From a criminal-law perspective, the European Union, by extending the scope of criminal and regulatory rules to digital-asset service providers and exchanges and requiring licensing, seeks to increase transparency and criminal accountability in decentralized environments. Nevertheless, the main challenge in the effective enforcement of criminal regulations remains the inherent difficulty of identifying perpetrators and proving crimes in decentralized virtual platforms, which, from a criminological standpoint, requires the development of advanced supervisory technologies and continuous cross-border cooperation among supervisory and criminal authorities in member states.

4.3. Enforcement Guarantees of European Criminal Laws in the Metaverse

The European Union criminal justice system has taken important steps in dealing with crimes related to the metaverse and digital assets in order to provide suitable legal frameworks for confronting new digital threats. In particular, MiCA was designed with the aim of fully and comprehensively regulating services related to crypto-assets so as to increase investor security by requiring authorization from supervisory authorities and aligning national laws with EU regulations ([European Parliament, 2023](#)). However, the inherent challenge of distributed ledger technology, which restricts direct supervision by authorities, remains. The only theoretical solution would be the participation of authorities in every type of crypto-asset, which is difficult to achieve because of the decentralized nature of this technology ([European Parliament, 2023](#)).

On the other hand, before the adoption of MiCA, the European Union had largely adopted a conservative approach toward financial instruments based on distributed ledger technology. Given risks such as money laundering, terrorist financing, and cybersecurity threats, various legal reforms were adopted, including the extension of the Anti-Money Laundering Directive to cryptocurrency exchanges and electronic wallet providers ([European Banking Authority, 2013](#); [European Commission, 2017](#)). Although these preliminary measures were positive steps, the rapid growth and complexity of cryptocurrency markets caused the European Union to lag behind other regions, such as the United States, in some areas ([European Commission, 2018](#)).

Accordingly, criticisms have been raised regarding the compatibility of EU environmental policies with the mining of tokens based on distributed ledger technology, because cryptocurrency mining, due to its high energy consumption and dependence on resources that may generate pollution, may conflict with the objectives of the European Union's green transition ([European Parliament, 2023](#)). This issue, in addition to legal and regulatory challenges, has introduced environmental dimensions into the European Union criminal and regulatory system and demonstrates the need for greater policy coordination and the development of sustainable solutions in this field ([European Parliament, 2023](#)). The enforcement guarantees of European Union criminal laws in confronting metaverse crimes, based on new legal frameworks such as MiCA, seek to strengthen accountability and responsibility in this emerging digital environment through a combination of licensing requirements, continuous supervision, and intergovernmental cooperation ([European Parliament, 2023](#)). Under these regulations, crypto-asset service providers are required to comply with security, transparency, and anti-money laundering standards, and in the event of violations, they may face sanctions and financial penalties ([European Parliament, 2023](#)). These mechanisms create effective deterrence against criminal activities in the metaverse and protect investors' rights.

On the other hand, by emphasizing cooperation among judicial and law-enforcement bodies of member states, the European Union has facilitated mechanisms for information exchange and coordination in addressing cross-border crimes related to the metaverse, because the decentralized and transnational nature of digital assets requires extensive coordination for the application of enforcement guarantees ([European Parliament, 2023](#)). In addition, preventive measures such as updating anti-

money laundering directives and strengthening customer-identification systems within the MiCA framework are key tools for tracing and combating financial crimes in the metaverse ([European Commission, 2018](#)).

The enforcement of European Union criminal laws in the metaverse faces unique challenges rooted in the virtual and often transnational nature of this environment. Although existing laws are applicable, identifying perpetrators, collecting evidence, and determining jurisdiction involve significant difficulties ([European Parliament, 2023](#)). In response to these problems, European law-enforcement bodies seek to strengthen cooperation among law-enforcement institutions of member states, universities, and the private sector, while adapting existing legal frameworks and developing innovative solutions for monitoring and combating crimes in the metaverse ([European Parliament, 2023](#)). This multilateral action plays an important role in strengthening enforcement guarantees and improving the effectiveness of criminal laws in digital environments. In addition, the use of advanced technologies in data analysis and the development of intelligent identification systems helps European law-enforcement authorities better identify offenders and track illegal activities in decentralized metaverse environments ([European Parliament, 2023](#)). Nevertheless, problems such as the protection of user privacy and the absence of clear geographical boundaries remain serious obstacles to law enforcement ([European Parliament, 2023](#)). Therefore, transnational cooperation and the development of harmonized international regulations are unavoidable necessities for ensuring effective enforcement guarantees in the metaverse ([Kayani & Hasan, 2024](#)). On the basis of the foregoing, these coordinated efforts among various institutions enable the European Union, while maintaining the security of investors and users in the metaverse, to act as a leading model in the regulation and enforcement of criminal laws for emerging technologies. Thus, given the particular limitations and opportunities of this field, the combination of legal and technological solutions and international cooperation constitutes the main strength of the European criminal justice system in confronting metaverse crimes. On the other hand, the enforcement guarantees of European Union criminal laws in the metaverse, through mechanisms such as licensing requirements for digital-asset service providers, transaction transparency, continuous supervision, and inter-institutional cooperation, play an important role in limiting metaverse-related financial crimes. These guarantees, by imposing strict obligations concerning customer identification, anti-money laundering, and compliance with cybersecurity standards, prevent offenders from operating freely in the decentralized and anonymous environments of the metaverse. Moreover, transnational coordination among judicial and law-enforcement bodies of member states and the use of modern supervisory technologies have increased the risk of identification and prosecution for perpetrators of financial crimes, such that the metaverse, despite its technological complexities, can no longer be regarded as a safe environment for money laundering, fraud, or concealing illegal assets. Consequently, these measures have created effective deterrence against the uncontrolled expansion of financial crimes in the metaverse.

5. Examination of Criminal Protection under Japanese Criminal Laws in the Field of Digital Assets

With reference to Fujiwara's study and the examination of Japanese criminal laws, it can be shown that Japan's experience in dealing with non-performing assets provides a suitable basis for understanding how criminal protection of digital assets has developed. Japan's financial crisis in the 1990s and the establishment of institutions such as the Resolution and Collection Corporation and the Deposit Insurance Corporation laid the foundation for supervisory and protective mechanisms that later inspired the development of legal frameworks in response to new threats, including crimes related to digital assets. Through institutions such as the Purchase Price Examination Board, the Japanese government sought to price non-performing assets transparently and fairly in order to prevent corruption and structural losses ([Fujiwara, 2023](#)). These experiences have played an important role in the development of criminal legislative institutions in the field of emerging digital assets.

The ratio of non-performing assets in Japanese banks, examined from March 1999 to September 2021, decreased in certain periods and increased during crises such as the COVID-19 pandemic ([Fujiwara, 2023](#)). These changes demonstrate the fragility of the financial system against unpredictable risks and indicate the need for supportive laws against emerging digital threats. In confronting such risks, Japan has attempted to develop suitable legal frameworks for protecting digital assets as well. One of the most important measures in this regard was the reform of the Payment Services Act and the Financial Instruments and Exchange Act in 2019, which specifically addressed the recognition and regulation of digital-asset exchanges and created requirements for customer protection and the prevention of money laundering.

On the basis of these legal reforms, digital assets have been recognized from a criminal-law perspective, and crimes such as unauthorized access, unlawful transfer of digital assets, theft of private keys, and phishing have been considered by the Japanese legislature. Moreover, under the Penal Code of Japan, individuals are subject to criminal prosecution if they commit fraudulent acts or digital forgery that result in the unfair acquisition of assets. Article 246 of this Code includes cases that can also be applied in digital environments. The experience of dealing with non-performing assets taught the Japanese government that, in order to protect the economic system, it must use a combination of supervisory mechanisms and criminal guarantees. As a result, in the field of digital assets as well, we now observe the design of a system that, from both regulatory and criminal perspectives, seeks to establish a balance between freedom of innovation and the prevention of criminal abuses. This issue is discussed further below.

5.1. The Position of Digital Assets in Japanese Criminal Law

The position of digital assets in Japanese criminal law has undergone a fundamental transformation in light of recent developments, particularly in the field of combating terrorism and organized crime. One of the most important of these developments was the adoption in 2017 of the offense of “preparation for the commission of acts of terrorism and other organized crimes” in order for Japan to accede to the United Nations Convention against Transnational Organized Crime. This new offense, with a preventive purpose, allows criminal prosecution at the planning and preparation stage, even before the principal offense is committed. This development has also created the necessary legal basis for dealing with emerging crimes such as cyberattacks, digital fraud, and the unlawful exploitation of digital assets (Fujiwara, 2023).

With the expansion of digital space, digital assets have gained importance both as instruments for committing crimes and as targets of crime. In this regard, the new Japanese law allows the criminal prosecution of individuals who use cryptocurrencies to finance terrorist groups or endanger digital infrastructures. For example, in cases where terrorist groups plan to design computer viruses and damage critical infrastructures such as electricity and water control systems, the mere commencement of the development of such viruses may be sufficient to establish criminal liability (Fujiwara, 2023). Such a preventive mechanism is designed in line with the requirements of Article 5 of the UNTOC, which emphasizes the criminalization of agreements to commit serious crimes.

At the same time, the Japanese legislature, while considering human rights concerns, has attempted to prevent possible abuses. This offense is realized only when three conditions are established: the existence of an organized criminal group, a specific agreement to commit a serious crime, and an objective act toward the implementation of the crime; merely having a “criminal thought” or a “verbal agreement” without a practical act is insufficient (Fujiwara, 2023). In addition, this offense does not include ordinary members of society who have no connection with criminal groups, and the actions of investigative bodies remain subject to judicial supervision in accordance with the rules of criminal procedure. Overall, these developments represent an important step toward adapting Japanese criminal law to international requirements in the digital age.

5.2. Analysis of Laws Combating Cybercrime and Digital Assets

In recent years, with the development of blockchain technology and the emergence of digital currencies, traditional concepts in criminal and civil law have been challenged. Innovations such as the decentralized consensus mechanism based on proof of work, first introduced in the Bitcoin white paper, have played a vital role in the security and stability of decentralized networks. Despite Bitcoin’s initial dominance over the market, today thousands of different digital currencies with diverse technologies and algorithms are in circulation (Kayani & Hasan, 2024). Cryptocurrencies such as Ethereum and Ripple have structures different from Bitcoin; in particular, the Ethereum network stores not only transactions but also the updated state of the system in its blocks, and since 2022 it has achieved greater efficiency by transitioning from proof of work to proof of stake. It is necessary to note that in Japan, before the emergence of cryptocurrencies and digital assets, the country’s legal system had relatively traditional and specific definitions of “assets” and “property,” rooted in Japanese civil law and strongly influenced by German and French civil law during the Meiji period in the nineteenth century. In Japanese law, the main term for assets refers broadly to property and assets with economic value. Article 85 of the Civil Code of Japan explicitly addresses this matter. In traditional legal systems such as England, the concept of “property” has a long historical background and has always been

central to the regulation of economic and social relations. However, digital assets such as tokens, cryptocurrencies, and NFTs are new concepts that do not fit within traditional categories (Fairfield, 2022). These assets are transferable, convertible, and even divisible, but they lack physical form or material backing; these features have made it difficult in many countries, including Japan, to adapt them to classical concepts of ownership. Nevertheless, in recent years, Japan, as one of the most digitally advanced countries in Asia, has created a relatively precise legal framework for recognizing, regulating, and protecting digital assets. Following extensive cyberattacks and cryptocurrency thefts in recent years, including the Coincheck exchange incident in 2018, Japanese lawmakers revised the legal system. Under the Payment Services Act and financial-services regulations, cryptocurrencies were defined as “crypto-assets,” and strict rules were imposed on exchanges and digital wallets.

In the field of cybercrime, Japan has also adopted specific laws to combat crimes such as unauthorized access, data destruction, and digital identity theft. The Act on the Prohibition of Unauthorized Computer Access, enacted in 1999, is one of the main pillars for confronting cyberattacks, and its subsequent amendments, particularly in 2012, enabled more precise criminalization and stricter punishment. Inter-institutional and international cooperation with international police bodies and supervisory institutions such as the Financial Action Task Force has also strengthened the system for tracing suspicious transactions. Moreover, the Japanese legislature’s criminal-law approach to financial crimes related to digital assets and the metaverse is based on the principle of “no punishment without law,” which is reflected in Article 31 of the Constitution of Japan. Under the Penal Code of Japan, crimes such as computer hacking and the theft of assets have been criminalized as computer fraud under Article 246-2 of the Penal Code. Furthermore, in the Penal Code of Japan, the legislature has clearly defined the scope of application of criminal law: if the offender is Japanese, the law applies to crimes committed inside or outside Japan; however, if the offender is not Japanese, the law applies only to crimes committed in Japan. This distinction is based on the principle of determining criminal jurisdiction and preserving criminal justice.

In general, Japan has attempted to strike a balance between financial-technology innovations and legal requirements through a combination of legal reforms and modern supervisory tools. Despite these measures, several fundamental challenges remain, including proof of ownership in anonymous wallets, determination of jurisdiction in cross-border crimes, and precise criminalization of fraudulent activities in blockchain environments, all of which require the continuous development of the legal system.

From a comparative perspective, the criminal justice systems of the European Union and Japan each have distinct strengths and weaknesses in dealing with crimes and the concepts of digital property in the metaverse. The European Union, using integrated and future-oriented legal policies, has attempted over the past decade to enact comprehensive regulations on digital assets. Among the most important regulations is MiCA, which seeks to provide a coherent and broad definition of cryptocurrencies, tokens, and digital assets (European Parliament, 2023). Although this framework is new, it makes it possible to criminalize certain fraudulent behaviors such as unlawful token offerings, market manipulation, or misuse of inside information. Moreover, the use of data-protection rules and cybersecurity measures has increased the capacity to protect metaverse users against technical threats and abuses based on personal data (European Commission, 2018; European Parliament, 2023). Nevertheless, one weakness of this system is delay in implementation, because the legislative process at the EU level is complex and time-consuming and coordination among member states is difficult. In addition, many criminal-law rules remain delegated to member states, which creates inconsistency in the enforcement of laws in transnational cases such as crimes committed in the metaverse.

By contrast, Japan, with a pragmatic approach based on practical experiences, created a relatively stricter legal framework after several major security incidents in the cryptocurrency sector, such as the Coincheck hack. The Payment Services Act and the Financial Instruments and Exchange Act have defined cryptocurrencies as “crypto-assets,” and consequently, they have been subjected to certain legal requirements such as user identification, reporting of suspicious transactions, and financial supervision. In the criminal justice system as well, the Act on the Prohibition of Unauthorized Computer Access and other rules related to cybercrime provide tools through which criminal conduct in digital space and the metaverse, such as identity theft, hacking, or digital fraud, can be prosecuted and punished. Japan’s strength lies in its rapid response to technological threats and the creation of enforceable requirements for exchanges and platforms. However, one fundamental weakness of Japanese law in this field is the absence of a coherent theoretical framework regarding the nature of digital property and its position within the traditional ownership system. Moreover, the metaverse has not yet been specifically defined or criminalized in the

Japanese legal system, and criminal acts in this space must often be pursued through an expansive interpretation of traditional rules, which may lead to uncertainty in judicial decisions. Overall, the European Union has a stronger and more long-term theoretical framework but is slower in practical response, while Japan acts in a more agile and operational manner, yet faces challenges in terms of theoretical grounding and clarification of emerging concepts such as virtual assets and crimes in new environments such as the metaverse.

6. Proposal of the Best Legal Model for Iran

The reality is that personal data and virtual property, especially on digital and metaverse platforms, have become important targets for criminal behavior because of their high economic value, broad accessibility, and the weakness of traditional protection systems. Personal data, as resources with market value, create incentives for crimes such as data theft, extortion, identity forgery, cyber threats, phishing, unauthorized access, and even the illegal sale of users' information on dark markets. This situation indicates the formation of a "data-driven black economy" in which data are both instruments for committing crime and the object of crime itself.

In Iranian criminal law, the legal vacuum regarding the recognition of personal data as a protectable object of crime is highly evident. This vacuum arises from the absence of an explicit definition of data as property or as an object capable of being violated, and it prevents the application of many traditional crimes, such as theft, breach of trust, or fraud, to data-related situations. In fact, in the absence of a legal definition of personal data as property or as an object of crime, perpetrators of digital crimes often remain outside the scope of effective prosecution, or proceedings are conducted through expansive interpretations that may conflict with the principle of legality of crimes and punishments (Mojahed et al., 2024).

From a criminological perspective, features such as intangibility, reproducibility, and the transferability of data within anonymous digital platforms facilitate victimization. Victims often become subject to the criminal collection and exploitation of their information without being aware of it. Moreover, new platforms such as the metaverse, by providing spaces for remote interaction and anonymous identity, create new criminal opportunities for which the traditional criminal justice system is not prepared. For example, intrusion upon a metaverse user's personal data, threats or extortion through digital assets, or digital identity forgery are forms of conduct that require specific criminalization, proportionate criminal responses, and preventive policies (Esmaeili & Ghavi al-Bonieh, 2022).

On this basis, it is proposed that the best legal model for Iran in the criminal-law dimension should be a combined model that, on the one hand, like the European Union, provides specific criminal-law rules for misuse of data and unauthorized access through the adoption of laws similar to general data-protection regulations, and on the other hand, like Japan, establishes more effective criminal enforcement by enacting explicit laws concerning "data" and "crypto-assets." Japan, by reforming the Act on the Prohibition of Unauthorized Computer Access enacted in 1999 and extending it to data-driven crimes, has developed an approach based on preventive control, punishment, and inter-institutional cooperation, which can serve as a suitable model for Iran. Especially in circumstances where personal data have exchange value and economic effects, the failure to criminalize their criminal exploitation leads to public distrust, the expansion of cybercrime, and an increase in hidden victimization. Therefore, it is proposed that the Iranian legislature amend the Computer Crimes Law and adopt a comprehensive law on the protection of personal data, criminalizing conduct such as unlawful collection, sale, unauthorized disclosure, threats, and financial exploitation of individuals' data as independent criminal offenses. It is also necessary to design specific criminal titles for crimes related to digital assets in environments such as the metaverse and to provide enforcement measures such as seizure of digital assets, blocking access, or cooperation with international platforms. Ultimately, incorporating emerging concepts such as "data ownership," "criminal liability of platforms," "personal cybersecurity," and "digital victimization" into Iran's criminal policy is not only a theoretical necessity but also a practical requirement; without it, citizens' vulnerability in digital space will seriously increase.

7. Conclusion

With humanity's entry into a new era of digital technologies, the metaverse, as one of the most important emerging platforms for human, economic, and social interactions, has acquired a special position. In this environment, users engage in economic activities, exchange, and investment through tools such as cryptocurrencies, non-fungible tokens, and other virtual assets. This

structural transformation in the concept of ownership has created the need to rethink legal protections, particularly criminal protections, for digital property.

In the first part of this study, by examining the concept and nature of digital assets in the metaverse, it was shown that this type of property, despite lacking a physical manifestation, has real economic value and the capacity for ownership. From the perspective of property law, although digital assets still lack a clear position in many legal systems, their nature requires protections similar to those afforded to traditional property. The expansion of the metaverse has led to the formation of new methods of committing crimes, including digital identity theft, data manipulation, token fraud, and cyberattacks against digital wallets, which traditional legal systems are unable to confront effectively.

In the comparative analysis, the examination of European Union regulations showed that the Union, by adopting MiCA, has systematically regulated digital financial activities and introduced new concepts of virtual property into its legal structure. These regulations play an important role in clarifying the legal status of digital assets, imposing licensing requirements on platforms, and drafting criminal protective rules. On the other hand, the analysis of the European Union criminal justice system shows that, through instruments such as data-protection rules, anti-money laundering directives, and cross-border judicial cooperation, the possibility of confronting metaverse crimes is expanding. EU judicial practice, although still limited, also contains signs of acceptance of the concept of digital assets as protectable property.

In the Japanese legal system, it is observed that the legislature, by precisely defining digital assets in criminal and financial laws, including the Payment Services Act and financial-asset laws, especially after widespread cyberattacks against exchanges, has reconstructed the legal structure. In this country, criminal action against cyber offenders is pursued seriously, and supervisory institutions also have extensive duties in preventing, detecting, and prosecuting crimes related to digital assets. The comparison of Japanese judicial approaches with Iran and the European Union shows that Japan has also moved toward developing criminal protections appropriate to the metaverse environment. Accordingly, the comparative analysis between the European Union and Japan, in light of the examination of the Iranian legal system, showed that Iran's legal system still suffers from gaps in the conceptual definition of digital assets, their recognition within property law, and the explicit criminalization of metaverse crimes. While the European Union and Japan are expanding the scope of criminal protections for digital assets through modern legal instruments, Iran remains dependent on outdated laws that are not aligned with digital developments, such as the Computer Crimes Law adopted in 2009.

Therefore, this study proposes that the Iranian legislature, by drawing on successful legal systems, particularly MiCA and Japan's legal structure, should enact a comprehensive law on the recognition of digital assets, determination of their position in property law, criminalization of new forms of crime in the metaverse, and design of enforcement guarantees appropriate to cyberspace. Such an action would not only enhance the legal security of Iranian users in the metaverse but could also contribute significantly to trust-building and the development of the digital economy at the national level.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

- Andrade, B. D., Poplin, A., & Sena, I. S. D. (2020). Minecraft as a tool for engaging children in urban planning: A case study in Tirol Town, Brazil. *Isprs International Journal of Geo-Information*, 9, 170.
- Avci, G., & Erzurumlu, Y. O. (2023). Blockchain tokenization of real estate investment: A security token offering procedure and legal design proposal. *Journal of Property Research*, 40, 188-207.
- Ayoubi, S. (2024). *Transformation of Attitudes toward Property in the Digital Context* [Doctoral dissertation, University of Mazandaran]. Mazandaran.
- Balis, J. (2022). How brands can enter the metaverse. <https://hbr.org/2022/01/how-brands-can-enter-the-metaverse>
- Burilov, V. (2019). Regulation of crypto tokens and initial coin offerings in the EU. *European Journal of Comparative Law and Governance*, 6, 146-186.
- Chiu, I. H. Y., & Greene, E. F. (2019). The marriage of technology, markets and sustainable (and) social finance: Insights from ICO markets for a new regulatory framework. *European Business Organization Law Review*, 20, 139-169.
- Cotter, K., Crone, D., Rodriguez-Boerwinkle, R., Boerwinkle, M., Silvia, P., & Pawelski, J. (2022). Examining the flourishing impacts of repeated visits to a virtual art museum and the role of immersion. *Behavioral Sciences*, 12, 500.
- Damodaran, A. (2022). From non-fungible tokens to metaverse: Blockchain-based inclusive innovation in arts. *Innovation and Development*, 1-20.
- Esmacili, M., & Ghavi al-Bonieh, A. (2022). Reconsideration of the Rules Related to Public Property Based on the Transformation of the Theory of Private Ownership. *Justice Law Journal*, 86(120), 179-199.
- European Banking Authority. (2013). *Warning to Consumers on Virtual Currencies* (EBA/WRG/2013/01). <https://www.eba.europa.eu/sites/default/files/documents/10180/598344/b99b0dd0-f253-47ee-82a5-c547e408948c/EBA%20Warning%20on%20Virtual%20Currencies.pdf>
- European Commission. (2017). *Report on the Assessment of the Risks of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities*. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017DC0340>
- European Commission. (2018). *FinTech Action Plan: For a More Competitive and Innovative European Financial Sector*. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0109>
- European Parliament. (2023). *Regulation (EU) 2023/1114 on Markets in Crypto-assets*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02023R1114-20240109>
- Fairfield, J. A. (2022). Tokenized: The law of non-fungible tokens and unique digital property. *Indiana Law Journal*, 97, 1261.
- Fujiwara, B. (2023). *A Study on Non-Performing Assets Cases and Cryptocurrency in Japan*. City University of Hong Kong.
- Gan, J., Tsoukalas, G., & Serguei, N. (2020). Initial coin offerings, speculation, and asset tokenization. *Management Science*, 67, 914-931.
- Garcia-Teruel, R. M., & Simon-Moreno, H. (2021). The digital tokenization of property rights: A comparative perspective. *Computer Law and Security Review*, 41, 1-16.
- Giannini, T., & Bowen, J. P. (2023). Global cultural conflict and digital identity: Transforming museums. *Heritage*, 6, 1986-2005.
- Han, J., Liu, G., & Gao, Y. (2023). Learners in the metaverse: A systematic review on the use of Roblox in learning. *Learning in the Metaverse*, 12, 296.
- Kalpokas, I., & Kalpokiene, J. (2023). *Regulating the Metaverse*. Routledge Taylor and Francis.
- Kantaros, A., Ganetsos, T., & Petrescu, F. I. T. (2023). Three-dimensional printing and 3D scanning: Emerging technologies exhibiting high potential in the field of cultural heritage. *Applied Sciences*, 13, 4777.
- Kayani, U., & Hasan, F. (2024). Unveiling cryptocurrency impact on financial markets and traditional banking systems: Lessons for sustainable blockchain and interdisciplinary collaborations. *Journal of Risk and Financial Management*, 17, 58.
- Kiskis, M. (2024). Private law framework for blockchain. *Frontiers in Blockchain*, 7, 1205461.
- Li, T., Liu, J., & Xu, Y. (2022). Simulation research and development of new marine simulator based on Videotrace. In *Applied Mathematics, Modeling and Computer Simulation* (pp. 58-64). IOS Press.
- Lozano-Duran, A., Rudolphi-Solero, T., Nava-Baro, E., Ruiz-Gomez, M., & Sendra-Portero, F. (2023). Training scientific communication skills on medical imaging within the virtual world Second Life. *International journal of environmental research and public health*, 20, 1697.
- Mojahed, M., Rajabzadeh, A., & Elahi, M. (2024). Examining the Legitimacy of Virtual Assets with Emphasis on Digital Currency (Cryptocurrency). *Law and Political Science*, 5(2), 1-16.
- Pundziene, A., & Gadeikiene, A. (2023). Digital ecosystems for sustainable society: Current developments and future research pathways. 2023 IEEE International Conference on Technology and Entrepreneurship (ICTE), Kaunas, Lithuania.
- Shen, J., Zhou, X., Wu, W., Wang, L., & Chen, Z. (2023). Worldwide overview and country differences in metaverse research: A bibliometric analysis. *Sustainability*, 15, 3541.
- Sheng, B., Zhang, C., Yin, X., Lu, Q., Cheng, Y., Xiao, T., & Liu, H. (2016). Common intelligent semantic matching engines of cloud manufacturing service based on OWL-S. *International Journal of Advanced Manufacturing Technology*, 84, 103-118.
- Swinkels, L. (2023). Empirical evidence on the ownership and liquidity of real estate tokens. *Financial Innovation*, 9, 45.