How to cite this article:
Shabanfar, A., Nematollahi, M., & Sadeghi Dehsahraei, M. (2026). The Role of Digital Currency in the Commission of Crimes with a Perspective on Iran's Criminal Policy. *Journal of Historical Research, Law and Policy, 4*(2), 1-12. https://doi.org/10.61838/jhrlp.174

Article history:
Original Research

Dates:
Submission Date: 29 September 2025
Revision Date: 21 December 2025
Acceptance Date: 28 December 2025
First Pubication Date: 29 December 2025
Final Pubication Date: 01 June 2026

The Role of Digital Currency in the Commission of Crimes with a Perspective on Iran's Criminal Policy

1. Alireza. Shabanfar[1] : Department of Law, ShK.C., Islamic Azad University, Shahrekord, Iran
2. Meysam. Nematollahi[2*]: Department of Law, ShK.C., Islamic Azad University, Shahrekord, Iran
3. Morteza. Sadeghi Dehsahraei[3]: Department of Law, ShK.C., Islamic Azad University, Shahrekord, Iran

*corresponding author's email: N.maysam1363@iau.ac.ir

ABSTRACT

Digital currencies, as an emerging phenomenon in the global financial system, despite advantages such as high transaction speed, cost reduction, technological security, and a decentralized structure, have also provided the conditions for the commission of various crimes, particularly cyber and financial crimes. Using a descriptive–analytical method, this article examines the most significant cryptocurrency-related offenses within the framework of Iranian criminal law. The findings indicate that characteristics such as decentralization, transnationality, and the anonymous or quasi-anonymous nature of cryptocurrency transactions have created serious challenges in identifying offenders, detecting crimes, and enforcing criminal prosecution. Moreover, the absence of comprehensive legislation, the fragmentation of existing regulations, and the weakness of supervisory mechanisms have intensified the potential for the criminal misuse of cryptocurrencies. Finally, emphasizing the necessity of designing a coherent and forward-looking criminal policy, the article proposes legislative, executive, and technical solutions, including the enactment of a comprehensive cryptocurrency law, the strengthening of international cooperation in combating transnational crimes, the mandatory implementation of user identification procedures (Know Your Customer – KYC) by domestic platforms, and the enhancement of public awareness among users. This study seeks, through a systematic analysis, to contribute to crime reduction and the regulation of the legal environment governing cryptocurrencies.

Keywords: *Criminal policy; digital currency; cybercrime; cryptocurrency fraud; money laundering; criminal procedure; Iranian criminal law.*

Introduction

The digital revolution and the emergence of modern financial technologies have transformed the face of the global economy. Among these developments, digital currencies, as one of the most tangible achievements of the information technology era, have attracted the attention of a wide range of economic actors, investors, and even governmental institutions by offering a decentralized, secure, and rapid model for value exchange (1-3). Nevertheless, as with any new phenomenon that brings opportunities alongside threats, cryptocurrencies are no exception. The cyberspace governing cryptocurrencies, due to features such as relative anonymity, the elimination of traditional financial intermediaries, and instantaneous cross-border transactions, has become an attractive platform for cybercriminals (4, 5). In Iran, despite the cautious and at times restrictive positions of monetary and banking authorities, the cryptocurrency market is expanding informally, with transaction volumes and the number

of users steadily increasing (6, 7). This rapid growth, in the absence of a comprehensive legal framework and a transparent criminal policy, has exposed the country to multiple security, economic, and social risks (8, 9). Crimes such as large-scale fraud (including the King Money case), theft of digital wallets, the use of cryptocurrencies for smuggling of goods and currency, money laundering, tax evasion, and even the financing of terrorist groups represent concrete manifestations of these threats (5, 10).

The principal question of this article is to examine the challenges and deficiencies confronting the criminal policy governing the cryptocurrency environment in Iran and to determine how appropriate legislative, supervisory, and procedural measures may contribute to managing these crimes and reducing vulnerabilities (5, 8). The objective of the present study is not only to identify and analyze the manifestations of cryptocurrency-related crimes, but also to evaluate the adequacy or inadequacy of existing regulations, including the Computer Crimes Act and the Anti-Money Laundering Act, as well as the associated procedural framework (6, 10).

The structure of the article is as follows: after this introduction, Chapter One provides a detailed examination of eight major categories of cryptocurrency-related crimes, analyzing in each case the role of cryptocurrencies, the methods of commission, and the relevant legal and judicial challenges. In Chapter Two, the Iranian legal framework is critically assessed, and finally, in the conclusion, proposed criminal policy solutions are presented. It is hoped that the findings of this research may serve as a resource for legislators, judges, researchers, and practitioners in this field.

1. Criminal Policy in the Sphere of Cryptocurrency Crimes

Digital currencies, like other financial phenomena, are not immune from criminality. From the very inception and expansion of cryptocurrencies, their becoming either the subject of crime or an instrument of crime has been unavoidable (5, 9). However, it is noteworthy that the high credibility and security of digital currencies have in no way been undermined by this reality. Just as tangible fiat currencies have always been exposed to crimes such as theft, money laundering, and fraud while still retaining public trust and acceptance, digital currencies, despite being the subject and instrument of various crimes, continue to demonstrate comparatively higher levels of security than physical currencies (1, 2).

At the same time, it must be emphasized that alongside the high level of security arising from cryptographic mechanisms, the processes of tracing and identifying offenders, determining the nature of crimes, and identifying the factors related to such crimes are considerably more complex and difficult than in the domain of conventional monetary crimes (4, 8). For this reason, some critics challenge the complete independence of cryptocurrencies from governments and other institutions and argue that a degree of oversight by domestic and international bodies is necessary (5, 6). Accordingly, the formulation and adoption of specialized procedural rules and regulatory frameworks governing cryptocurrency-related crimes appear indispensable (7, 10). Presently, governments worldwide endeavor, through legislative initiatives and focused regulatory attention, to reduce existing gaps and exert greater control over this market (2, 11).

Crimes in the Field of Cryptocurrencies

With the expansion of cryptocurrency usage in recent years, crimes associated with digital currencies have increased significantly (5, 8). Some of the principal offenses in this domain include the theft of digital assets, fraud in cryptocurrency transactions, fraud in cryptocurrency production, and the use of cryptocurrencies in illicit activities

such as drug trafficking, money laundering, and the financing of terrorism (9, 10). Cryptocurrency transactions are conducted based on blockchain technology, and if an individual succeeds in penetrating this technology, they may gain unauthorized access to the system and steal digital assets without the consent of their owners (3, 4). Moreover, certain cryptocurrencies suffer from security vulnerabilities that may result in transactional fraud and production-related fraud (12, 13). Due to the absence of centralized financial institutions in the cryptocurrency ecosystem, the tracing of crimes and the recovery of stolen assets are also more limited, a factor that further contributes to the growth of cryptocurrency-related offenses (8, 10).

Overall, as the use of digital currencies expands, the corresponding criminal activities have increased simultaneously. In order to confront these crimes, legal reform and the enhancement of security within cryptocurrency trading platforms can be effective measures (6, 7). The following section provides a detailed examination of the most significant crimes in the field of cryptocurrencies.

Digital Currency and Its Role in Computer Fraud

Fraud has long been regarded as one of the most significant and prevalent crimes against property, to the extent that some scholars have referred to it as the “crisis of the twentieth century” (5). In brief, fraud is defined as the unlawful appropriation of another’s property through the use of fraudulent means. Fraud is divided into two main types.

First, traditional fraud, in which the offender deceives another person through deceptive methods and thereby appropriates their property; in this form, a human being is deceived.

Second, computer fraud, which involves deceiving a non-human entity—such as a computer, device, mobile phone, or similar system—for the purpose of unlawfully obtaining another’s property.

Accordingly, when the deceived party is a human being, the offense constitutes traditional fraud, whereas when the deceived entity is non-human, the offense constitutes computer fraud. Furthermore, the subject matter of computer fraud is broader and more general than that of traditional fraud, as it encompasses not only property but also financial benefits and privileges (10).

Like traditional fraud, computer fraud is a result-based offense. Thus, the perpetrator must obtain property or a benefit through the abuse and deception of a computer. Until such a benefit or property is actually acquired, even if the offender has manipulated data systems and deceived the computer, the crime of computer fraud is not legally consummated (10).

In the realm of cryptocurrencies, fraud is likewise among the most important and prevalent offenses (5, 8). Digital currencies may constitute both the subject of traditional fraud and the subject of computer fraud. For example, an individual who falsely presents himself as an employee of an exchange and persuades another person to transfer their digital assets to his wallet for conversion into fiat currency commits traditional fraud, with digital assets constituting the object of the crime. In the context of computer fraud, a perpetrator may manipulate the data of an individual’s digital wallet, impersonate the wallet owner, and by deceiving the computer system transfer digital assets into his own account. In such a case, the abuse of computer systems, interference with data, and deception of the system constitute the material elements of the crime, while the digital assets are the object of the offense (8, 10).

Another increasingly widespread example in this field is the creation of fictitious and unsupported cryptocurrencies by opportunistic actors. After extensive promotion and the dissemination of false promises and

hopes, they attract large numbers of investors, sell substantial quantities of these assets, and subsequently conduct what is known as an “exit scam,” whereby the price of the asset abruptly collapses to zero. This form of fraud constitutes one of the most significant and common types of cryptocurrency-related fraud (12, 13). Consequently, prior to purchasing or trading any digital currency, it is essential to investigate its backing, creators, and history and to refrain from acquiring unknown or newly issued assets.

One of the largest fraud projects that has occurred in Iran involved the cryptocurrency known as King Money (symbol: KIM), with an estimated value of approximately 4,500 billion tomans. This asset was introduced in 2019 as a payment instrument for marketing commissions by the network company Badran. Shortly thereafter, a large number of the company’s users and other individuals began trading this cryptocurrency. The project’s documentation falsely claimed features such as mining via mobile phones and operational mechanisms similar to Bitcoin. Contrary to these assertions, however, King Money lacks a blockchain, an anomalous characteristic for any genuine digital currency. It also lacks transparency—one of the most fundamental features of cryptocurrencies—and its codes and operations are private and closed. This means that King Money is not, in reality, a cryptocurrency, but merely a representation of fabricated and deceptive numerical values. Its price and value were determined not by market mechanisms but by its creators, who artificially generated price fluctuations to encourage investment. The price reportedly rose from 4 euros to several thousand euros, and once thousands of individuals had invested their assets, the King Money website became inaccessible and the value of holdings collapsed by 100 percent, resulting in massive fraud. The King Money case remains ongoing, with numerous plaintiffs, and the defendants are scheduled to appear in court in June 2020.

Computer fraud in the cryptocurrency domain remains a persistent threat to participants in this market. As previously noted, it represents the most frequent and significant category of offenses in this field. Accordingly, market participants and those intending to enter the cryptocurrency sector must, through careful study, investigation, consultation with knowledgeable experts, and reliance on informed guidance at the outset, prevent victimization or at least substantially reduce the risk of becoming victims of cryptocurrency-related crimes (5, 8).

Digital Currency and Its Role in Computer Theft

Computer theft is addressed in Article 12 of the Computer Crimes Act. In computer theft, what is stolen is “data,” regardless of whether such data has financial value or lacks financial value. Computer theft is a purely cyber offense, and the actus reus, similar to non-computer theft, consists of the act of taking. However, there are differences between these two forms of theft, including the fact that in computer theft, the identical data that is stolen may still remain in the possession of its owner; by contrast, such a situation is not conceivable in traditional (non-computer) theft, because if the object remains under the owner’s control, the offense of theft is not realized (14).

With respect to digital currencies, because each unit of cryptocurrency can exist only within a single wallet and cannot be copied or “taken” while simultaneously remaining in the owner’s wallet, computer theft in practice becomes closely analogous to conventional theft. Nevertheless, theft occurs where the offender transfers the stolen cryptocurrency to their own account or to a designated person. If the offender transfers the digital assets to an unknown personal wallet, then, since the property has exited the victim’s ownership yet has not been transferred to the offender’s account or to a person designated by the offender, it appears that the offense would more closely align with computer data destruction. Given the distinctive nature of cryptocurrencies, if these assets are stolen, recovery and tracing can be extremely difficult and, in some instances, effectively impossible. Accordingly, the most

effective approach is prevention and the use of preventive tools, including the selection of an appropriate wallet and the protection of personal passwords and passphrases. Some of the most important measures for preventing the theft of digital currencies are as follows (6).

First, selecting an appropriate digital wallet. Various wallets exist for storing digital currency, including hardware wallets, software wallets, mobile wallets, online wallets, and even paper wallets. The security of these wallets differs; for example, an online wallet generally provides less security than an offline wallet. In general, hardware wallets offer higher security. Hackers may steal cryptocurrencies through counterfeit wallets and, for this purpose, use names that resemble those of authentic wallets. To avoid such problems, the application should be downloaded from the wallet's official website.

Second, protecting private keys. The password and recovery phrase provide the owner of the cryptocurrency with personal credentials for accessing their assets and must never be disclosed to others.

Third, avoiding phishing attacks. Phishing attacks aim to trap users and compromise a digital wallet by creating similar-looking and fraudulent websites. Users should strictly refrain from clicking on untrustworthy links in order to remain protected from phishing attacks.

Fourth, countering malware. In this method, hackers install malicious software on a user's mobile phone or laptop and, when a transfer is initiated, substitute their own wallet address so that the user unknowingly sends digital currency to the hacker. Where malware is suspected, the most effective response is to cleanse the system and change passwords.

Digital Currency and Its Role in Smuggling

In legal terminology, smuggling refers to bringing goods into or out of a country in violation of governmental regulations, and engaging in the transfer, purchase, or sale of such goods in an unauthorized and prohibited manner. Under paragraph (a) of Article 1 of the Law on Combating Smuggling of Goods and Currency, any act or omission that results in the violation of legal formalities related to the import or export of goods or currency—and which, under that law or other laws, is deemed smuggling and subject to punishment—constitutes smuggling at border entry points or anywhere within the country, including the place of distribution within the domestic market (15).

Digital currencies can serve both as the subject of the offense of smuggling and as an instrument facilitating smuggling. As the subject of the offense, what is "smuggled" is the transfer of digital currencies out of the country, or their entry into the country, without observing the regulations governing the import and export of currency. The outflow of currency through digital assets is a matter that, in the absence of monitoring and control, may create significant problems for the national economy, because the export of digital currencies effectively entails an outflow of national foreign-exchange and dollar resources. For this reason, the Central Bank has consistently sought measures and mechanisms through which it can exercise maximum oversight over foreign-exchange transactions and the volume of currency purchases and sales by each individual, for example by determining limits on how much currency each person may obtain through their national identification code. The NIMA system is another measure adopted by the government and the Central Bank to enhance the transparency of foreign-exchange transactions and the inflow and outflow of currency. Accordingly, in the absence of oversight and control by the Central Bank and other economic institutions, digital currencies may become the subject of smuggling offenses and generate foreign-exchange and economic difficulties for the state (8).

On the other hand, digital currencies can function as tools for smuggling by facilitating the illicit import and export of goods. Because smugglers consistently face obstacles in making foreign-currency payments for purchasing goods abroad and importing them illegally, the procurement and transfer of large foreign-currency sums is complex and difficult; however, by using instruments such as digital currencies, such transfers can be conducted far more easily. For example, smugglers may purchase cryptocurrency in Iran and transfer it conveniently to a seller of goods in China, thereby completing their transactions. Setting ceilings on the daily purchase volume per person can constitute one practical measure to address this phenomenon (7).

In conclusion, with the advancement of computers and technology, geographical borders are becoming increasingly less salient, and preventing or prohibiting global connections will become progressively more difficult over time. Accordingly, rather than suppressing or obstructing the use of new tools and global developments in the communications and technology sphere, it is necessary to adopt policies and diverse measures to guide such progress in a proper and constructive direction.

Digital Currency and Its Role in Money Laundering

With the increased use of digital currencies, money laundering offenses facilitated by these assets have also expanded. Money laundering refers to any act that gives an appearance of legality to funds derived from unlawful and illegitimate activities. It is a process in which illicit funds obtained from criminal activity are “cleaned” in such a manner that they appear to originate from lawful sources. Money laundering is among the most significant financial crimes and can have severely destructive effects on the economy and society. It may be committed through numerous methods, and any activity that, in some manner, makes crime-derived funds appear lawful may fall within the scope of money laundering. The use of digital currencies in money laundering is facilitated by the lack of a need to identify the holders of such assets and by the absence of centralized financial institutions. In this process, individuals purchase digital currency using illicit funds and subsequently sell those assets through cryptocurrency trading platforms (10).

Money laundering is often committed in an organized and transnational manner. For this reason, identifying and tracing money-laundering offenders and the funds subject to laundering requires international cooperation and engagement with international organizations and institutions. Accordingly, combating money laundering requires coordinated international action aimed at prevention and enforcement. International treaties and the establishment of international organizations constitute part of the measures undertaken by the international community to address money laundering.

Iran, in parallel with other countries, has placed the fight against money laundering on its policy agenda. The Anti-Money Laundering Act of 2008 is the country’s most significant legislative measure in this regard. Additional Central Bank measures, implemented through by-laws and circulars, constitute other steps taken to counter money laundering. The establishment of the High Council for Combating Money Laundering, chaired by the Minister of Economic Affairs and Finance pursuant to Article 4 of the Anti-Money Laundering Act, represents an important measure aimed at preventing money laundering.

The relationship between money laundering and cryptocurrencies arises insofar as digital currencies become instruments for committing money laundering offenses. The creation of multiple wallets and accounts by offenders and the transfer of crime proceeds into them, transferring funds abroad, rendering such funds untraceable through digital currencies, and converting these proceeds into assets such as real estate and vehicles through digital

transactions inside and outside the country are among the many methods through which money laundering may be facilitated both domestically and transnationally. Money laundering has become one of the central concerns in the cryptocurrency sphere, and given the broad destructive impacts of money laundering on national economies and the outflow of substantial foreign-exchange assets, it is necessary to adopt suitable and effective criminal policies and to legislate in this field in order to combat and prevent this phenomenon (16).

To prevent money laundering through digital currencies, it is necessary to define money-laundering rules and regulations specifically applicable to digital assets and to require cryptocurrency trading platforms to implement such rules. In addition, the use of identity-verification mechanisms for asset holders can contribute to reducing money-laundering offenses involving digital currencies.

Digital Currency and Its Role in Phishing

The term “phishing” literally refers to “fishing,” and this label has been adopted due to the complexities and subtle techniques employed in this crime. Phishing is a type of cyberattack in which malicious actors, for the purpose of deceiving individuals and collecting important and sensitive information such as email passwords, usernames, credit card details, and the like, impersonate legitimate businesses, entities, or institutions. Phishing is one of the methods used by cybercriminals to steal sensitive information from internet users. With the growing use of digital currencies in financial transactions, some offenders also employ digital currencies and related processes to facilitate phishing schemes.

Phishing involves psychological manipulation and relies on human error; for this reason, it is classified as a form of social engineering. Phishing attacks most commonly occur when an offender uses forged or fraudulent emails and persuades the victim to enter sensitive information into fraudulent websites. Requests such as changing passwords “for greater security,” entering credit-card information to “extend validity,” and links to gambling and betting websites are among the common phishing techniques. In addition, some offenders use malicious software to steal encrypted keys from users and, through them, gain access to user accounts and transfer digital currencies to their own accounts (3).

Since 2020, phishing has been among the most prevalent attacks carried out by cybercriminals. In the field of digital currencies, phishing also has numerous victims. For example, cyber offenders may counterfeit the main website of an exchange or websites associated with a particular digital currency and deceive users into believing they are operating on legitimate platforms; by embedding their own wallet addresses on those sites, they steal users’ assets. The creation of counterfeit wallets and making them available on Google Play, Bazaar, or other widely used application-download platforms is another phishing method in the cryptocurrency domain (1).

To prevent phishing in connection with digital currencies, it is advisable to consistently use secure and reputable websites for financial transactions and exchanges, to refrain from disclosing personal and sensitive information in unknown or fraudulent messages, and to use updated antivirus software. Required software should be downloaded exclusively from reputable websites and sources, and users should avoid clicking on unknown or suspicious links.

Digital Currency and Its Role in Tax Evasion

The decentralized nature of digital currencies and the absence of an organization or institution responsible for them make the monitoring and control of transactions and invested capital more difficult. In many countries, taxation constitutes a major source of government revenue. Individuals often seek, through various means, to evade taxes

or to minimize their tax burden. Undoubtedly, tax evasion through digital currencies may also occur. For example, if a seller acquires digital currencies at prices above their actual value and fails to pay the required tax, that person may be regarded as engaging in tax evasion. In addition, some individuals may attempt to conceal income derived from the sale of digital currencies and refrain from paying taxes on such income. However, through appropriate regulation and accurate, continuous follow-up by tax authorities, tax evasion by cryptocurrency users can be reduced to a minimum.

Governments set specific tax obligations for different occupations and sectors and use various methods to assess income levels and, consequently, the taxes due. For example, the total amounts paid monthly through point-of-sale terminals may serve as an effective indicator for estimating a person's monthly income and the taxes they should pay. Some individuals, however, engage in tax-evasion practices such as pressuring customers to pay in cash, because cash receipts are less readily identifiable and calculable for taxation purposes. It is evident that digital currencies can substantially facilitate tax evasion at the macro level, particularly for large and significant sums. Rapid high-value payments without fees and taxation, while regarded as a strength of digital currencies, can—if broadly adopted—sharply reduce government revenues and inflict severe harm on national economies.

Digital Currency and Its Role in Terrorist Financing

Pursuant to Article 1 of the Law on Combating the Financing of Terrorism, the intentional and knowing provision and collection of funds and assets by any means, whether or not they have a lawful origin, as well as the expenditure of all or part of financial resources obtained from sources such as currency smuggling, the solicitation of financial and monetary support, donations, money transfers, the purchase and sale of financial and credit instruments, the direct or indirect opening of accounts, the provision of credit, or the conduct of any economic activity by a person for themselves or for another, for the purpose of providing them to terrorists or terrorist organizations that commit one of the acts set forth in the remainder of that article, constitutes terrorist financing and is a criminal offense. "Terrorist financing" refers to activities that provide financial support to individuals or groups engaged in terrorism. Where a government maintains a list of terrorist organizations and groups, it correspondingly enacts laws to prevent the laundering of funds that are used to finance such organizations (4).

Definitions and manifestations of "terrorism" vary across countries and are shaped by macro-level policies and interests. Allied countries often attempt, through various strategies, to label their adversaries as terrorists. For example, certain Western countries classify Hezbollah in Lebanon and the Islamic Revolutionary Guard Corps as terrorist groups and take measures against them. Conversely, Iran classifies Israel as a terrorist entity and has engaged in direct and indirect confrontations with it. Therefore, there is no universally agreed-upon global definition or fixed instance of terrorism. Terrorist financing has attracted heightened international attention in recent decades, particularly after the September 11 attacks. Through legislation and criminalization measures in this area, states have sought to prevent support for terrorism and terrorist groups.

Cryptocurrencies have, to a significant extent, facilitated the financing of various groups, from academic and research groups to terrorist organizations. This "double-edged sword" has, in many cases, supported scientific and knowledge-based initiatives, assistance to patients and older persons, and other humanitarian purposes by enabling global fundraising and sustained activity. Conversely, violent, criminal, and terrorist actors have also exploited this opportunity and have been able, through digital currencies, to receive substantial support from states or sponsoring networks.

In light of the above, the advantages of using digital currencies and their ease of broad access have at times resulted in improper and harmful uses, underscoring for all stakeholders the necessity of deliberation and policy planning to control and improve cryptocurrency usage. Any negligence or inattention in this field may lead to harmful and irreparable consequences. The enactment of the Law on Combating the Financing of Terrorism, along with other measures such as blocking and confiscating terrorist assets, mandatory reporting of suspicious terrorism-related transactions, strengthening operational cooperation with other countries in investigating financial sources of terrorism, requiring substitute systems for money transfer and banking exchanges to comply with regulatory standards, tightening anti-money-laundering rules, intensifying customer identification measures in smart transfers at domestic and international levels, and reforming laws and regulations to ensure that so-called charitable and non-profit organizations are not used to finance terrorism, are among the anti-terrorism measures attributed to the Islamic Republic of Iran.

Digital Currency and Its Role in Cyber Extortion (Ransomware Attacks)

Cyber extortion is one of the most prevalent forms of cyberattacks and can also be carried out through the use of digital currencies. Extortion in cyberspace is primarily conducted through ransomware. One of the major threats facing individuals active in cryptocurrency trading and users of digital wallets is the loss of their assets through ransomware attacks. Ransomware constitutes a category of highly dangerous malware that infiltrates the systems of individuals and institutions and restricts access to systems or files, including financial data. This restriction of access is typically achieved through encrypting files or data. Ransomware may infiltrate users' systems through deceptive links such as emails, websites, and text messages. The attacker then demands payment from the victim in exchange for providing the decryption key. Ransomware was first observed in Russia, but it has gradually expanded to many countries, including the United States, Australia, and Iran, and has claimed numerous victims. One of the most common methods of cyber extortion is the use of encryption software, whereby hackers encrypt users' files and subsequently demand payment to unlock them. The demanded payment is typically requested in the form of digital currency, and in order to avoid financial tracking, attackers often rely on cryptocurrencies such as Bitcoin. The victim is therefore compelled to pay a sum in order to recover their files and data. Another method of cyber extortion using digital currencies involves deceiving users through fraudulent emails or counterfeit websites (5).

In this method, hackers send fraudulent emails or construct counterfeit websites that prompt users to disclose sensitive information such as usernames and passwords, which are then used to gain access to the users' cryptocurrency wallets. The sums demanded by cyber extortionists are usually collected in ways that are difficult or impossible to trace or recover, and in this regard, digital currencies have become the most significant instrument of extortion for perpetrators of this crime. The fundamental characteristics of digital currencies, which constitute their principal strengths, can also be exploited by opportunistic offenders. The untraceability of transactions and the anonymity of wallet holders are among these characteristics, which significantly facilitate the commission of cyber extortion crimes (11).

The primary reason for the success of ransomware attacks is that most systems lack adequate protection against cyber threats. Most victims never anticipate becoming targets of ransomware and therefore fail to implement effective preventive measures. In order to prevent cyber extortion via digital currencies, it is strongly recommended to use antivirus and anti-spam software. Furthermore, to prevent hackers from accessing sensitive information,

users should employ strong passwords and never share their credentials with others. Simple measures such as avoiding unknown or suspicious links and regularly updating operating systems can significantly reduce the success of ransomware attacks. Providing widespread public education in this field is also a critical necessity that should not be neglected by responsible authorities.

Conclusion

The examination of cryptocurrency-related crimes in this article demonstrates that this emerging technology, despite all of its advantages and positive economic potential, has—due to its inherent characteristics (decentralization, semi-anonymity of transactions, speed, and transnational nature)—created a vulnerable and crime-prone environment. The analysis of eight major categories of offenses, ranging from fraud and theft to money laundering and terrorist financing, indicates that offenders have effectively exploited these features and devised increasingly sophisticated methods to achieve their criminal objectives.

The principal challenge in confronting these crimes is twofold. On the one hand, significant legislative gaps and deficiencies are evident. Existing laws, such as the Computer Crimes Act and the Anti-Money Laundering Act, were largely enacted before the widespread emergence of cryptocurrencies and have not been able to address this innovative phenomenon in a specific and effective manner. The absence of a comprehensive and specialized statute governing cryptocurrencies—covering both their civil and economic dimensions as well as their criminal aspects—constitutes one of the most serious obstacles to the effective control of crimes in this domain. On the other hand, procedural and enforcement challenges persist. The relative anonymity of the parties to transactions, the transnational character of offenses, the difficulty of tracing financial flows on the blockchain, and the lack of sufficient expertise within judicial and law-enforcement authorities have collectively complicated the detection, prosecution, and adjudication of offenders.

In response, the criminal policy framework proposed in this article is based on several core pillars. First, comprehensive legislation: the necessity of drafting and enacting a “Comprehensive Law on the Regulation of Digital Currencies and the Combatting of Related Crimes,” in which the legal definition and status of cryptocurrencies, the regulatory framework governing exchanges and platforms, the specification of specialized offenses, and the enhancement of penalties are clearly articulated. Second, strengthening supervision and identity verification: mandating all platforms operating in Iran to strictly implement Know Your Customer (KYC) requirements and suspicious transaction reporting (STR), and establishing a national system for registering cryptocurrency transactions as a major step toward market transparency. Third, enhancing the specialized capacity of judicial and law-enforcement bodies: creating specialized cryptocurrency crime units and dedicated courts staffed with judges and experts trained in blockchain technology and digital currencies. Fourth, expanding international cooperation: concluding extradition treaties and judicial cooperation agreements with other countries, particularly in transnational cases where cryptocurrencies play a significant role. Fifth, public education and awareness: designing educational campaigns to inform users about security risks, common fraud methods (such as phishing and Ponzi schemes), and effective strategies for protecting digital assets.

Ultimately, it must be acknowledged that a purely repressive approach and total prohibition are neither practical nor effective. Global experience indicates that intelligent regulatory governance and controlled acceptance, combined with investment in advanced supervisory technologies (such as blockchain analytics), provide a more effective pathway for harnessing the economic opportunities of cryptocurrencies while simultaneously containing

their criminal threats. The present article aspires, through its in-depth analysis of crimes and existing challenges, to contribute to the formation of scholarly discourse and practical action by policymakers toward shaping a balanced, effective, and forward-looking criminal policy in the complex and dynamic realm of cryptocurrencies.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adheried in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Dibrova A. Virtual currency: new step in monetary development. Social and Behavioral Sciences. 2016:42-9. doi: 10.1016/j.sbspro.2016.07.112.
2. Matsuura JH. Overview of Digital Currency Regulations and Legal Implications. Legal Civilization. 2018;1(1):149-67.
3. Yousefi A. Application of Blockchain in Businesses. Tehran: Adabestan; 2021.
4. Cekerevac Z, Cekerevac P. Blockchain And The Application Of Blockchain Technology. MEST Journal. 2022;10(2). doi: 10.12709/mest.10.10.02.02.
5. Varasi G. Criminal Policy and Dimensions of Crime Prevention in the Field of Digital Currencies. Ghanoon Yar. 2021;5(19).
6. Khodaverdi Hossein M, Razavi A, Montazer M. Legal Pathology of Government Regulation in the Field of Cryptocurrencies. Modern Research in Administrative Law. 2023(14):67-88.
7. Ghaderi A, Ashtiani Moghaddam A, editors. Investigating the Legal Regime Governing Cryptocurrency and Digital Currency. The 1st International Conference on Law, Political Science, Islamic Politics and Islamic Jurisprudence; 2024; Sari.
8. Foghahazadeh N, Rafieipour K. Challenges of Iran's Judicial Justice System Regarding Crimes Related to Digital Currency. Judicial Law Research Quarterly. 2023;4(7):447-66.
9. Sales-Moayed AA, Siahbidi K, Kouhestani. Legal Analysis of Digital Currency and Its Impact on National Security. Security Research. 2020;19(69):59-80.
10. Nabavi SM, Saber M. Comparative Study of Challenges in Iran's Criminal Justice System in Prosecuting Crimes Related to Virtual Currencies. Comparative Law Research. 2020;24(1):179-208.

11. Hapsari AA, Puspitasari DM. The influence of financial technology on the advancement of financial inclusion in micro, small, and medium enterprises (MSMEs) in West Java. Accounting Studies and Tax Journal (COUNT). 2024;1(1):48-60. doi: 10.62207/5v4t9q48.
12. Satpolson A. Bitcoin and Cryptocurrency Trading for Beginners. Jahantighi M, editor. Karaj: Roham Andisheh; 2022.
13. Allaf Salehi N. Complete Training on Digital Currencies. Tehran: Atrān; 2021.
14. Haji Ghiasi Fard MH, Nikomaram H. Pathology of Transaction Mechanisms in the Global Currency Market (Forex) and Proposing a Structured Currency Market Model Based on the Country's Economic Reality. Financial Engineering and Securities Management (Portfolio Management). 2019;10(39):135-69.
15. Soltanifard J, Mohammadi A. A Jurisprudential Reflection on the Possibility of Transactional Usury in "Coins" and "Tokens" Exchanges. Majlis and Strategy. 2024. doi: 10.22034/mr.2024.15980.5616.
16. Madadi M, Ghaemi Kharagh M, Shafiei G. Jurisprudential and Legal Essay on the Issue of Legalizing "Cryptocurrencies". Majlis and Strategy. 2021;28(105):303-34. doi: 10.22034/mr.2021.444.