Identifying and Analyzing Preventive Components in Iran's Criminal Policy Toward Crimes Related to Virtual Currencies to Provide Efficient Solutions for Improved Effectiveness

1. Mohammad Ghaemi Asl: Department of Law, Ahv.C., Islamic Azad University, Ahvaz, Iran
2. Salame Abolhasani*: Department of Law, Ahv.C., Islamic Azad University, Ahvaz, Iran
3. Naghmeh Farhoud: Department of Law, Ahv.C., Islamic Azad University, Ahvaz, Iran

*Correspondence: Abolhasani070@iua.ac.ir

Abstract

This study identifies the existing capacities and challenges within Iran's criminal policy regarding the prevention of criminal activities related to virtual currencies. In this regard, legislative criminal policy—emphasizing the development of comprehensive and transparent regulations; judicial criminal policy—focusing on specialized judicial training and the establishment of dedicated branches; executive criminal policy—highlighting the supervision of law enforcement and financial institutions; and participatory criminal policy—promoting cooperation among the public, media, and private sector are examined. Furthermore, types of prevention, including social, situational, and criminal prevention, are analyzed within the framework of these four policy areas, and effective, integrated solutions are proposed to enhance the efficiency of the preventive system. The present study employs a descriptive–analytical research method. First, by using library resources and legal documents, the theoretical foundations and the current legal status are reviewed. Then, through comparative and critical analysis, the strengths and weaknesses of Iran's criminal policy in addressing cryptocurrency-related crimes are identified. Finally, targeted corrective and preventive recommendations are presented. The findings reveal that Iran's criminal policy in the field of virtual currencies lacks the necessary coherence and comprehensiveness and remains predominantly reactive rather than preventive. The novelty of this study lies in presenting a four-pronged prevention model—legislative, judicial, executive, and participatory—which integrates all dimensions of prevention while considering the specific characteristics and risks associated with financial technologies. This model can serve as a practical framework for reforming Iran's criminal policy and transitioning toward an efficient, coordinated, and future-oriented preventive system against crimes related to virtual currencies.

Keywords: criminal fault, unintentional fault, Imamiyyah jurisprudence, Public Penal Code of 1925, Islamic Penal Code of 2013, historical evolution.

Received: 11 May 2025
Revised: 25 September 2025
Accepted: 04 October 2025
Initial Publish: 18 October 2025
Final Publish: 01 December 2025

Citation: Ghaemi Asl, M., Abolhasani, S., & Farhoud, N. (2025). Identifying and Analyzing Preventive Components in Iran's Criminal Policy Toward Crimes Related to Virtual Currencies to Provide Efficient Solutions for Improved Effectiveness. *Legal Studies in Digital Age,* 4(4), 1-11.

1. Introduction

The emergence of new financial technologies and digital transformations has fundamentally reshaped the global economic and commercial landscape. One of the most important manifestations of this transformation is the rise of virtual currencies as decentralized, encrypted, and transnational financial instruments (Afzali, 2013; Mohammadzadeh, 2013). With their rapid transferability, digital security, and independence from the traditional banking system, these technologies have created significant opportunities for the development of financial markets and the facilitation of economic transactions (Navabpour, 2017). However, these same characteristics also create fertile ground for criminal activity. Money laundering, large-scale fraud, financing of illegal activities, and organized cybercrime are among the major threats associated with virtual currencies (Mousavinejad, 2012; Shambyati, 2012).

In Iran, the increasing use of virtual currencies in recent years has amplified the need for an effective response to this emerging phenomenon (Malek, 2013). On one hand, virtual currencies can contribute to economic development, enhance the flexibility of financial markets, and improve the efficiency of trade transactions (Navabpour, 2017). On the other, the absence of a robust legal infrastructure, weak specialized oversight, and the unpreparedness of judicial and executive bodies have created conditions for related criminal activities to spread rapidly (Khalili Paji, 2011). This situation demonstrates that a purely punitive and reactive approach cannot adequately counter the threats posed by virtual currencies and underscores the urgent need for preventive policies grounded in criminological analysis and modern technology (Afrasiabi, 2020; Farhadi Alashti, 2016).

Criminal policy—encompassing legislative, judicial, executive, and participatory measures—plays a critical role in responding to new financial phenomena (Maddadi & Ghaemi-Kharagh, 2011). Crime prevention here does not simply mean stopping offenses through post-crime responses; it also includes structural, technical, cultural, and educational measures that reduce crime opportunities and strengthen society's capacity to manage risk (Afrasiabi, 2020; Javadi Yeganeh, 2008). In the field of virtual currencies, prevention involves developing clear and comprehensive regulations, establishing digital surveillance systems, educating and raising user awareness, improving cybersecurity, and leveraging international cooperation (Farhadi Alashti, 2016; Mousavinejad, 2012).

The inherent features of virtual currencies—such as high-speed, borderless transactions, transaction anonymity, and decentralization—have generated substantial regulatory and legal challenges (Nabavi & Saber, 2010; Shamloo & Khalili Pachi, 2010). These characteristics often allow crimes to transcend national borders and render traditional judicial responses inadequate (Izadi & Arzanian, 2019). Experiences from other countries show that purely criminal or narrowly economic regulatory approaches cannot effectively control these crimes and that preventive policies must be built upon international cooperation, advanced cybersecurity standards, and flexible legal frameworks (Golkhandan, 2022).

In Iran, the current criminal policy response to virtual currencies lacks sufficient coherence. Existing regulations are either overly general or focused mainly on economic aspects, paying insufficient attention to preventive and criminological dimensions (Maddadi & Ghaemi-Kharagh, 2011; Malek, 2013). Weak legislative frameworks, unclear judicial precedents, and institutional limitations have complicated the fight against cryptocurrency-related crimes (Khalili Paji, 2011). Moreover, the lack of coordination between regulatory, judicial, and executive bodies, legal gaps, and insufficient use of new technologies have allowed the threats associated with virtual currencies to become increasingly complex and widespread (Afrasiabi, 2020; Golkhandan, 2022).

The transnational nature of virtual currencies and their capacity to bypass geographical restrictions make it essential to design a criminal policy built on international cooperation and informed by the experiences of advanced jurisdictions (Izadi & Arzanian, 2019; Mousavinejad, 2012). This requires Iran, while preserving the autonomy of its legal system, to adopt modern international standards and create mechanisms that enable crime prevention at both the national and transnational levels (Nabavi & Saber, 2010; Shambyati, 2012). Criminal policy in this field must aim not only to react to current crimes but also to anticipate and prevent future ones (Afrasiabi, 2020).

Given current conditions, a systematic analysis of Iran's criminal policy regarding the prevention of criminal activities linked to virtual currencies is both necessary and urgent (Malek, 2013; Navabpour, 2017). Identifying the strengths and weaknesses of existing policies enables the design of theoretical and practical solutions to reinforce crime prevention and strengthen financial and cyber security (Farhadi Alashti, 2016). From a scientific standpoint, such analysis fills a clear research gap, as most Iranian studies have focused primarily on economic and financial aspects rather than criminological and preventive dimensions (Afzali, 2013; Maddadi & Ghaemi-Kharagh, 2011).

One key challenge in Iranian criminal policy is its limited emphasis on proactive and preventive measures. While reactive judicial strategies may reduce some offenses in the short term, they cannot address the long-term risks posed by emerging financial technologies (Afrasiabi, 2020). Effective prevention requires an integrated approach that combines legal, executive, educational, and cultural initiatives to both reduce crime incentives and increase institutional and societal capacity to address cyber and financial crime (Farhadi Alashti, 2016; Golkhandan, 2022). Comparative analysis of successful international experiences shows that prevention of virtual currency crimes hinges on coherence and coordination among government agencies, the judiciary, regulatory bodies, and the private sector (Izadi & Arzanian, 2019; Mousavinejad, 2012).

In Iran, the absence of such coordination has left many preventive measures fragmented and ineffective, while new and complex crimes continue to proliferate (Malek, 2013). Furthermore, insufficient public awareness and education leave both users and some implementing agencies vulnerable to cyber threats, creating opportunities for increasingly sophisticated criminal activity (Navabpour, 2017).

Accordingly, this study aims to conduct a comprehensive examination of Iran's criminal policy regarding the prevention of virtual currency crimes, to identify existing gaps and weaknesses, and to propose practical and theoretically grounded reforms (Afzali, 2013; Maddadi & Ghaemi-Kharagh, 2011). The research objectives are threefold: first, to analyze the theoretical foundations of virtual currencies and their relationship to financial and cybercrime; second, to assess the legislative, judicial, and executive dimensions of Iran's current criminal policy; and third, to formulate evidence-based recommendations to strengthen preventive strategies (Afrasiabi, 2020).

The significance of this work is twofold. Scientifically, it contributes to filling a research void by offering a criminological and policy-oriented perspective on virtual currencies in Iran (Mousavinejad, 2012). Practically, its findings can guide policymakers, regulators, and judicial authorities in formulating effective prevention strategies, drafting clearer laws, and enhancing security infrastructures (Golkhandan, 2022). Ultimately, addressing the challenges posed by virtual currencies demands a comprehensive and multidimensional approach that respects legal principles while leveraging technological tools, international collaboration, and preventive measures (Farhadi Alashti, 2016; Navabpour, 2017).

This integrated perspective not only reduces crime incidence but also enhances financial stability, public trust, and the integrity of the economic system (Malek, 2013). Accordingly, this study underscores the necessity of moving beyond reactive strategies and strengthening preventive infrastructure as part of a coherent and forward-looking criminal policy.

2. Research Background

Zare et al. (2021), in a study titled *Challenges of Iranian Criminal Law in Countering Crimes Related to Digital Currencies*, argue that the absence of comprehensive legislation in Iran has led to divergent judicial interpretations and inconsistent procedures in handling cryptocurrency-related cases. They emphasize that the lack of alignment between Iran's criminal policy and the recommendations of the Financial Action Task Force (FATF), coupled with insufficiently transparent regulations, increases the risk of money laundering and organized crime in the cryptocurrency sphere (Malek, 2013; Mousavinejad, 2012). This research aligns with the present thesis by underscoring the need for transparent and preventive legislation in Iran, though Zare's work is more analytical and critical of the current legal landscape.

Shamloo and Khalili Pachi (2010), in their article *The Virtualization of White-Collar Crime in the Light of Virtual Currencies*, conclude that white-collar crime has evolved alongside cyberspace and the specialized tools it provides, such that some scholars refer to it as "virtual collar crime" (Shamloo & Khalili Pachi, 2010). Their descriptive–analytical study examines the features of virtual white-collar crime and explains why offenders exploit virtual currencies to facilitate illegal

acts. Unlike their work, the present thesis goes beyond descriptive analysis and seeks to propose preventive solutions tailored to crimes associated with virtual currencies.

Nabavi and Saber (2010), in *A Comparative Study of the Challenges of the Iranian Criminal Justice System in Prosecution of Crimes Related to Virtual Currencies*, highlight the urgent need to define virtual currencies legally and determine their nature, amend and supplement existing legislation to cover unique attributes of these currencies, and establish new criminal provisions when current laws are inapplicable (Nabavi & Saber, 2010). They also advocate for international cooperation and information exchange, memoranda of understanding between public and private sectors, the use of cryptocurrency experts, and specialized judicial training. This aligns with the present thesis in recognizing structural gaps but differs by focusing primarily on prosecution rather than a broader preventive policy model.

Troutman (2022), in *The United States Regulatory System for Cryptocurrencies: A Comprehensive Review*, observes that the United States has relied heavily on enforcement—such as financial penalties, asset forfeiture, and criminal prosecution—to regulate cryptocurrencies, yet these reactive measures alone cannot sustainably curb cryptocrime (Izadi & Arzanian, 2019). This analysis parallels the present thesis by acknowledging the limitations of purely punitive strategies, though Troutman's work is situated in the U.S. institutional context, whereas this research aims to develop a preventive framework suitable for Iran. Similarly, Houben and Snyers (2018), in *Cryptocurrencies and Blockchain: The Legal Framework and Implications for Financial Crimes*, warn that blockchain technology can facilitate money laundering, tax evasion, and terrorism financing and propose multi-layered preventive policies combining criminal regulation, financial oversight, and technological–regulatory tools (Mousavinejad, 2012). Their EU-focused recommendations support the idea of structural and integrated prevention but differ from this thesis's Iran-specific approach.

3. Methodology

Given the complexity of the subject and the variables under study, this research adopts a descriptive–analytical approach (Afrasiabi, 2020). Data collection is conducted primarily through library research, including Persian and Latin academic books, journal articles, and relevant legal instruments (Malek, 2013). Information gathering also employs a questionnaire to review materials systematically. For data analysis, both quantitative and qualitative reasoning are applied, using explanatory and analytical methods consistent with the theoretical nature of the study (Javadi Yeganeh, 2008).

4. Concepts of Prevention of Virtual Currency Crimes in Iranian Criminal Policy

In addressing criminal activity associated with virtual currencies, a precise and comprehensive conceptualization of *prevention* is essential because the field presents unique challenges due to its technological and transnational nature (Golkhandan, 2022). Clarifying the semantic dimensions of "prevention" in this context informs how Iranian criminal policy can adapt to emerging forms of digital financial crime and supports the development of effective, holistic preventive strategies.

4.1. Semantics of the Word Prevention

The etymological and terminological exploration of "prevention" is fundamental, as modern crime prevention has moved beyond reactive measures to include strategies that proactively eliminate opportunities for crime (Afrasiabi, 2020). This is especially crucial given the growing sophistication and variety of offenses in digital environments such as cryptocurrency networks (Farhadi Alashti, 2016).

4.2. Semantics of the Term Virtual Currency

With the rapid evolution of financial technologies, understanding the meaning and scope of "virtual currency" is critical (Afzali, 2013). Clarifying this concept helps delineate its features, potential uses, and associated risks, which are necessary for crafting robust legal and preventive frameworks (Maddadi & Ghaemi-Kharagh, 2011).

5. Fundamentals of Preventing Virtual Currency Crimes in Iranian Criminal Policy

Criminological foundations encompass the core theories and principles used to interpret and manage crime, integrating individual, social, economic, and cultural factors (Javadi Yeganeh, 2008). Several key frameworks inform prevention in the cryptocurrency sphere:

5.1. Situational Action Theory (SAT)

Developed by Per-Olof H. Wikström, SAT integrates criminological insights into a model explaining how individual morality and situational context shape criminal behavior (Afrasiabi, 2020).

5.2. Rational Choice Theory

Building on Weberian rationality and methodological individualism, rational choice theory explains how offenders weigh options and consequences to achieve goals, while also acknowledging social norms and constraints (Javadi Yeganeh, 2008).

5.3. Situational Crime Prevention

Situational crime prevention comprises 52 practical techniques designed to reduce opportunities for crime by altering pre-criminal conditions and deterring offenders (Farhadi Alashti, 2016; Golkhandan, 2022). These approaches emphasize environmental and technical interventions over purely punitive responses (Afrasiabi, 2020).

5.4. Risk-Based Prevention

Risk-based criminology, reflected in Iranian legal reforms and the adoption of risk-focused criminal policy, prioritizes proactive strategies to mitigate potential offenders' risks and recidivism (Khalili Paji, 2011). This orientation supports protecting society against evolving technological crime by emphasizing security management and forward-looking controls (Navabpour, 2017).

6. Facilitating Capacities of Virtual Currencies for Crime Prevention in Iranian Criminal Policy

In today's global economy, virtual currencies have emerged as a transformative phenomenon with the potential to facilitate transactions and reduce financial costs. Through blockchain technology and decentralized systems, they enable fast and secure transfers (Navabpour, 2017). However, alongside these advantages, virtual currencies also enable their misuse in a range of criminal activities, including money laundering, terrorist financing, tax evasion, narcotics and psychotropic drug trafficking, and human trafficking (Mousavinejad, 2012; Nabavi & Saber, 2010).

7. Structural Inadequacy of Legislative Criminal Policy in Preventing Virtual Currency Crimes

One of the fundamental structural deficiencies of Iran's legislative criminal policy is the lack of a comprehensive and specialized legal framework governing virtual currencies (Maddadi & Ghaemi-Kharagh, 2011; Malek, 2013).

7.1. Lack of Specific Criminal Regulations on Virtual Currency Financial Crimes

The absence of targeted criminal regulations for financial crimes involving virtual currencies is one of the clearest structural shortcomings of current legislation (Afzali, 2013). Cryptocurrencies, created and distributed through blockchain systems, have not yet been effectively addressed in Iran's statutory framework (Maddadi & Ghaemi-Kharagh, 2011). The only significant measure to date is the 2018 Central Bank guideline on virtual currency requirements, but it excluded major global cryptocurrencies such as Bitcoin and Altcoins, thereby leaving critical money-laundering channels unregulated (Izadi &

Arzanian, 2019). Without a clear and enforceable legal framework, supervisory bodies face obstacles in identifying and prosecuting crypto-related financial crimes. Establishing transparent, comprehensive laws would strengthen regulatory capacity and improve financial crime prevention (Mousavinejad, 2012).

7.2. Lack of Specific Criminal Law on Terrorist Financing in the Cryptocurrency Space

The absence of a clear criminal statute addressing terrorist financing through cryptocurrency networks creates significant vulnerabilities (Navabpour, 2017). In practice, the lack of an explicit and cohesive legal instrument allows criminals to exploit virtual currencies for covert transfers without detection (Shambyati, 2012). This gap hinders banks and financial institutions from effectively conducting customer due diligence and transaction monitoring, increasing exposure to terrorism financing and complex laundering schemes (Mousavinejad, 2012).

7.3. Lack of Explicit Criminal Provisions on the Use of Cryptocurrencies in Economic Crimes

Another major weakness is the absence of explicit legal provisions criminalizing the use of cryptocurrencies in economic offenses (Afzali, 2013). Although money laundering has been partially addressed in Iran's amended anti–money laundering law, virtual currencies remain insufficiently integrated into statutory definitions (Izadi & Arzanian, 2019). This legislative ambiguity fosters uncertainty for enforcement agencies and facilitates illicit capital flows. Comprehensive, cryptocurrency-specific regulations would close loopholes and provide clarity for regulators and prosecutors (Maddadi & Ghaemi-Kharagh, 2011).

7.4. Lack of a Specific, Transparent Legal and Tax System for Cryptocurrency Transactions

Another manifestation of legislative inadequacy is the lack of a coherent tax and reporting framework for cryptocurrency activities (Khalili Paji, 2011; Navabpour, 2017). Virtual currency transactions—especially in informal or illicit contexts—generate significant financial flows that remain largely invisible to the traditional tax apparatus (Malek, 2013). Without a law defining the legal nature of these digital assets and establishing tax obligations, enforcement agencies cannot track gains, verify ownership, or prevent large-scale tax evasion (Mousavinejad, 2012). This legal vacuum allows capital owners to transfer or store wealth through peer-to-peer networks without disclosure, undermining both fiscal security and anti–money laundering efforts (Golkhandan, 2022).

7.5. Lack of a Clear Definition of Virtual Currency Ownership in Criminal Law

A further challenge is the absence of a precise definition of ownership of virtual currencies under Iran's criminal code (Malek, 2013). Traditional property concepts fail to capture the intangible and borderless nature of digital assets. This ambiguity complicates the attribution of ownership rights and criminal liability, creating opportunities for fraud and asset misappropriation (Maddadi & Ghaemi-Kharagh, 2011). It also undermines investor protection and public trust in digital financial technologies (Navabpour, 2017). Developing legally sound, technology-oriented definitions of digital asset ownership is critical for both crime prevention and market stability.

7.6. Ambiguity in Applying the Legal Title of Theft to Virtual Data and Assets

Finally, the application of theft statutes to virtual data and cryptocurrency remains uncertain (Malek, 2013). The digital environment allows for hacking and unauthorized transfers that cause real financial harm but may not fit neatly within traditional definitions of theft (Maddadi & Ghaemi-Kharagh, 2011). Without explicit legislative clarification, enforcement against virtual asset theft remains inconsistent and ineffective, leaving both private users and institutional actors vulnerable.

8. Challenges in the Status and Validity of Cryptocurrencies in Contract Law and Banking Law

An examination of the legal status and validity of cryptocurrencies in Iranian contract and banking law shows that the only formal legislative instrument concerning their use is the resolution of the Cabinet of Ministers dated August 27, 2019 (05/06/1398), enacted under Article 138 of the Constitution. This six-article, seven-note resolution provides a limited regulatory foundation but does not fully clarify the contractual and banking treatment of cryptocurrencies (Mohammadzadeh, 2013). From a contract law perspective, Articles 1 and 2 of the resolution state that cryptocurrency use by private parties is not protected or guaranteed by the government or the banking system and that domestic transactions with cryptocurrencies are generally prohibited. The sole exception concerns cryptocurrency mining, which is permitted under license from the Ministry of Industry, Mines, and Trade. Under banking law, the Central Bank retains authority to regulate the use and supply of cryptocurrencies, but this oversight remains subject to the general monetary and banking laws of the Islamic Republic (Malek, 2013).

8.1. Legalization Challenges in the Decentralized World of Blockchain and Virtual Currencies

The decentralized architecture of blockchain technology complicates legislative control and exemplifies the structural inadequacies of current criminal policy. Because blockchain operates globally and is not confined to a single jurisdiction, national legal frameworks cannot easily govern its activities (Maddadi & Ghaemi-Kharagh, 2011). This gap allows criminals to exploit transnational anonymity and carry out illegal operations without fear of detection (Mousavinejad, 2012). The lack of clear, comprehensive legislation thus reduces transparency and undermines regulatory bodies' ability to identify and pursue suspicious activities. Effective legislative reform should integrate technology-aware provisions and international standards to secure financial and banking systems against blockchain-enabled crime (Afrasiabi, 2020).

8.2. Silence of the Islamic Penal Code Regarding Cryptocurrency Crimes

The 2013 Islamic Penal Code and its subsequent amendments were enacted before blockchain and cryptocurrencies had gained a defined role in Iran's economy. As a result, the Code does not directly address the definition, legal nature, or criminalization of cryptocurrency transactions or offenses (Maddadi & Ghaemi-Kharagh, 2011; Malek, 2013). This silence leaves courts without statutory guidance and weakens the preventive and punitive capacity of the legal system.

8.3. Ambiguity of the Legal Nature of Virtual Currencies

Iran's monetary and banking laws clearly define currency and foreign exchange, but these definitions predate the emergence of digital assets. Under the Law on Combating Smuggling of Goods and Currency and the Monetary and Banking Law, "currency" refers to foreign banknotes, coins, or financial instruments; buying and selling currency outside authorized channels is treated as smuggling. However, these provisions do not explicitly classify virtual currencies (Navabpour, 2017). The lack of legal clarity about whether cryptocurrencies are "currency," "property," or a distinct asset class creates interpretive confusion, obstructs enforcement, and fosters opportunities for fraud and abuse (Maddadi & Ghaemi-Kharagh, 2011).

9. Structural Requirements of Legislative Criminal Policy in Preventing Virtual Currency Crimes

At the legislative level, criminal policymakers must anticipate technological threats and provide coherent frameworks to regulate emerging digital assets (Afrasiabi, 2020; Shamloo & Khalili Pachi, 2010). The following structural requirements are particularly critical:

9.1. Developing Specific Laws for Suspicious Cryptocurrency Transactions in Money Laundering

Explicit anti–money laundering provisions addressing cryptocurrency transactions are essential because current Iranian law does not clearly cover these activities (Afzali, 2013; Maddadi & Ghaemi-Kharagh, 2011).

9.2. Passing Special Legislation to Monitor and Block Transactions Related to Terrorist Financing

Preventing terrorism financing requires robust access controls, customer due diligence, and mechanisms to intercept suspicious transfers (Mousavinejad, 2012). Enacting specialized legislation would equip banks and financial institutions to identify high-risk cryptocurrency users and disrupt funding flows (Malek, 2013).

9.3. Situational Measures to Reduce the Attractiveness of Financing Terrorism

Applying rational choice theory to legislative design can raise the cost of engaging in crypto-based terrorism financing (Farhadi Alashti, 2016). Techniques such as increasing transaction traceability and imposing reporting duties on exchanges discourage offenders by reducing potential rewards.

9.4. Situational Prevention by Reducing Provocation and Incentives

Legislation can also integrate situational prevention methods that limit environmental and motivational triggers for financial crime (Afrasiabi, 2020). Reducing systemic opportunities and provocation lowers the incentive to misuse cryptocurrencies for terrorism or laundering.

9.5. Developing Supplementary Regulations to Combat Cryptocurrency Use in Smuggling

Although Iran's anti-smuggling and economic crime laws offer a basic framework, they lack digital-asset-specific measures (Maddadi & Ghaemi-Kharagh, 2011; Navabpour, 2017). Supplementary rules should define cryptocurrencies as potential smuggling instruments, impose reporting thresholds, and establish interagency and international cooperation mechanisms (Golkhandan, 2022).

9.6. Determining Criminal Enforcement Guarantees for Exchanges and Virtual Currency Services

Because cryptocurrency exchanges, wallet providers, and related fintech actors serve as bridges between virtual and fiat economies, legislation should impose compliance duties and liability for failure to monitor suspicious transactions (Khalili Paji, 2011; Malek, 2013). Mandating identity verification, suspicious activity reporting, and cooperation with authorities would strengthen prevention and enforcement capacities.

10. Structural Requirements of Criminal Judicial Policy in Preventing Virtual Currency Crimes

The establishment of specialized judicial mechanisms is an essential structural requirement for strengthening Iran's criminal judicial policy and improving its capacity to prevent and address crimes related to virtual currencies (Maddadi & Ghaemi-Kharagh, 2011; Malek, 2013).

10.1. Establishment of Special Cyber Branches

Creating dedicated cybercrime branches within the judiciary is a vital measure to effectively manage virtual currency–related offenses. The increasing complexity of cryptocurrency crime, combined with blockchain's features such as cross-border transferability, relative anonymity, and rapid asset mobility, makes adjudication in ordinary public courts technically challenging and procedurally inefficient (Nabavi & Saber, 2010). Specialized cyber branches with trained judges and technical staff would provide the expertise necessary to interpret complex digital evidence, apply appropriate legal frameworks, and issue timely rulings.

10.2. Reducing Workload and Facilitating Proceedings

Another crucial requirement is reducing the burden on general courts to expedite cryptocurrency-related cases. The high volume and complexity of these cases often overwhelm ordinary judicial branches, resulting in backlogs, delays, and reduced legal effectiveness (Golkhandan, 2022). Establishing dedicated cyber branches would distribute caseloads more evenly, improve case-flow management, and enable faster, more consistent adjudication.

10.3. Issuance of Uniform Procedural Decisions by the Supreme Court

Issuing unified procedural guidelines and decisions by the Supreme Court is essential to avoid contradictory rulings on cryptocurrency crimes (Afrasiabi, 2020). Because the legal framework for digital assets remains incomplete and sometimes ambiguous, divergent interpretations by lower courts undermine predictability and public trust. Supreme Court guidance can clarify the definition of crypto-related offenses, establish consistent standards of evidence, and provide clear directions for determining liability. Such uniformity enhances judicial coherence, accelerates case resolution, and strengthens the deterrent impact of criminal law (Malek, 2013).

10.4. Equipping the Judicial System with Independent and Impartial Technical Experts

Providing the judiciary with access to specialized, impartial technical experts is indispensable for effective prevention and adjudication (Farhadi Alashti, 2016). Expertise in blockchain analysis, digital forensics, and cryptocurrency transaction tracing enables courts to interpret complex evidence and detect criminal patterns early. Rapid, reliable technical assessments support prosecutors and judges, reduce procedural delays, and increase transparency. Incorporating expert analysis into the judicial process not only improves the accuracy of rulings but also builds an intelligence base that can inform preventive strategies (Golkhandan, 2022; Mousavinejad, 2012).

11. Conclusion

Virtual currency is a form of digital asset created and managed electronically, typically utilizing blockchain technology to ensure security and transparency. These currencies are generally classified into two broad categories: centralized and decentralized. Centralized currencies are supervised by designated institutions, whereas decentralized currencies operate independently without central oversight. They may also be categorized according to convertibility, usability, and value stability.

The unique characteristics of virtual currencies—such as transaction speed, ease of transfer, decentralization, and the anonymity afforded to users—have made them an appealing tool for criminal activity. The use of digital wallets without intermediaries and the inherent privacy and security gaps create additional challenges for preventing and combating virtual currency–related crimes.

Criminal policy, understood as a set of principles and strategies for preventing, controlling, and combating crime to preserve social order and security, consists of four key dimensions. Legislative criminal policy involves formulating laws and sanctions; judicial criminal policy determines how cases are adjudicated and legal decisions are issued; executive criminal policy focuses on enforcing laws and supervising crime-related activities; and participatory criminal policy emphasizes cooperation between institutions and the public in prevention efforts.

Criminological and legal foundations are vital for strengthening the prevention of crimes committed through virtual currencies. Theories such as situational action and rational choice provide insight into offender decision-making and behavioral drivers. Preventive strategies, including situational and risk-based approaches, reduce crime opportunities and increase control over high-risk environments. Legally, principles such as the legality of crime and punishment and the state's responsibility to protect digital public order help establish an effective framework for combating cyber-financial crime.

The enabling features of virtual currencies significantly facilitate offenses such as money laundering, terrorism financing, smuggling, fraud, theft, and tax evasion. In money laundering, offenders conceal illicit origins by converting assets into digital currencies and then back into seemingly legitimate forms. Key methods include using unauthorized exchanges, mixing

cryptocurrencies to obscure fund sources, fraudulent investment schemes, and exploiting informal platforms. Gambling and online betting can further integrate illegal funds into legitimate financial channels.

Virtual currencies also simplify terrorism financing by enabling anonymous international transfers, fundraising through digital donations, and purchasing illicit equipment or services on the dark web. Smuggling networks benefit from cryptocurrencies by settling transactions outside regulatory oversight and leveraging cross-border, untraceable payments. Fraud is enabled through Ponzi schemes, fake exchanges, phishing tactics, and price manipulation practices such as pump and dump schemes. Theft of digital assets frequently occurs through hacking wallets and exchanges, malware attacks, and exploiting vulnerabilities in smart contracts or decentralized applications. Finally, tax evasion is facilitated by concealing income from cryptocurrency transactions, avoiding reporting through unauthorized platforms, and rapidly converting wealth into digital assets to escape detection.

Despite the scale and sophistication of these threats, Iran's criminal policy for preventing cryptocurrency-related crime remains underdeveloped. Legislative gaps include the absence of clear criminal provisions for financial offenses using virtual currencies, no specialized law addressing terrorism financing through cryptocurrency, and ambiguous regulation of virtual assets in economic crime contexts. Additional weaknesses include the lack of a clear legal definition of digital asset ownership, uncertainty about criminal classifications for cryptocurrency fraud, and silence in core penal codes regarding crypto-related offenses. Furthermore, inadequate frameworks for identity verification and reporting obligations undermine effective enforcement.

These deficiencies highlight the urgent need for systematic reform to strengthen Iran's preventive criminal policy. Addressing them will not only improve the country's ability to confront emerging cyber-financial threats but also reduce societal vulnerability to complex digital crimes. By identifying and analyzing these structural gaps, this research provides a foundation for legal and policy innovation. The findings can inform future legislative reforms, support the judiciary and enforcement bodies, and promote a coherent, integrated approach to preventing virtual currency crimes. Ultimately, reforming Iran's criminal policy in this area is essential to increase legal clarity, protect economic security, and build public trust in digital financial systems.

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

Afrasiabi, A. (2020). Paradigms governing situational crime prevention. *Journal of Crime Prevention Studies*(17).

Afzali, R. (2013). Review of jurisprudential rulings on virtual currency: A case study of Bitcoin. *Journal of Economic Jurisprudence Studies*(4).

Farhadi Alashti, Z. (2016). *Situational Prevention of Cybercrimes: Solutions and Challenges*. Mizan.

Golkhandan, S. (2022). Executive and sociological challenges of situational crime prevention and solutions to face it. *Journal of Political Sociology of Iran*(20).

Izadi, Z., & Arzanian, N. (2019). Prevention of money laundering and fraud crimes in the context of the use of global cryptocurrencies. *Quarterly Journal of Prevention Approach*(1).

Javadi Yeganeh, M. R. (2008). A sociological approach to rational choice theory. *Journal of Cultural Strategy*(3).

Khalili Paji, A. (2011). Risk-based criminal policymaking against virtual currency technology. *Journal of New Technology Law*(3).

Maddadi, M., & Ghaemi-Kharagh, M. (2011). Legal Jurisprudential Research on the Issue of Legalizing "Cryptocurrencies". *Majles and Strategy Quarterly*(28).

Malek, H. (2013). Criminal Policies Regarding Dealing with Criminal Activities Related to Virtual Currencies. *Journal of Jurisprudence and Modern Law*(13).

Mohammadzadeh, A. (2013). Comparative Study of Cryptocurrencies from the Perspective of Contract Law and Banking Law. *Journal of Legal Studies in Cyberspace*(7).

Mousavinejad, S. F. (2012). Digital currencies, money laundering and strategies to combat it in international law. *Journal of Sociology of Iran*(11).

Nabavi, S. M., & Saber, M. (2010). A comparative study of the challenges of the Iranian criminal justice system in the trial of crimes related to virtual currencies. *Comparative Law Research*(1).

Navabpour, A. (2017). Designing a conceptual framework for virtual currency policymaking in the Iranian economy. *Journal of Public Policy*(4).

Shambyati, H. (2012). Preventing Terrorism Financing and Money Laundering by Using Customer Risk Identification. *Journal of Legal Studies*(50).

Shamloo, B., & Khalili Pachi, A. (2010). The virtualization of white-collar crime in the light of virtual currencies. *Justice Law Journal*(110).