Crimes Related to Cryptocurrencies in the Iranian Legal System and the Common Law System

1. Ehsan Sadeghi:: Department of Criminal Law and Criminology, Aras International branch, Islamic Azad University, Tabriz, Iran

2. Mohammad Javad Pourhosseini*: Department of Criminal Law and Criminology, Khorramabad Branch, Islamic Azad University, Khorramabad, Iran

3. Mehdi Nik Nafs: Department of International Relations, Tabriz Branch, Islamic Azad University, Tabriz, Iran

*Correspondence: e-mail: MJ.pourhosseini13@iau.ac.ir

Abstract

Cryptocurrencies, as an emerging phenomenon in the world of finance and technology, have attracted significant attention. These digital currencies operate based on blockchain technology and facilitate financial transactions without the need for traditional intermediaries such as banks. In the Iranian legal system, due to the novelty of the topic, there is no specific and comprehensive legislation to address crimes related to this domain. Nevertheless, some existing laws on combating money laundering and financial crimes can be extended to partially cover cryptocurrencies. The Central Bank of Iran and other financial institutions are currently in the process of formulating regulations to manage and supervise this field. On the other hand, in the common law system, which is implemented in countries such as the United States, Canada, and the United Kingdom, multiple laws have been enacted to confront crimes associated with cryptocurrencies. Institutions such as the Securities and Exchange Commission and the Financial Crimes Enforcement Network under the U.S. Department of the Treasury have developed detailed regulations to monitor and control cryptocurrency transactions. This article examines the differences and similarities in the laws and regulations related to cryptocurrencies in the Iranian and common law legal systems and analyzes the efforts of both systems in addressing the legal challenges associated with this field.

Keywords: cryptocurrencies, crimes, money laundering, Iranian legal system, common law system.

Received: 24 July 2024
Revised: 21 October 2024
Accepted: 05 November 2024
Published: 30 November 2024

Citation: Sadeghi, E., Pourhosseini, M. J., & Nik Nafs, M. (2024). Crimes Related to Cryptocurrencies in the Iranian Legal System and the Common Law System. *Legal Studies in Digital Age*, 3(4), 49-62.

1. Introduction

In recent years, cryptocurrencies have gained significant attention as an emerging phenomenon in the realms of finance and technology. These digital currencies, which operate based on blockchain technology, enable financial transactions without the need for traditional intermediaries such as banks. However, the increasing use of cryptocurrencies has also brought forth new legal challenges, especially in the areas of combating financial crimes and money laundering. In the Iranian legal system, due

to the novelty of cryptocurrencies, there are no specific and comprehensive laws addressing crimes related to this area. Nonetheless, existing laws concerning anti-money laundering and financial crimes can to some extent be extended to cryptocurrencies. The Central Bank of Iran and other financial institutions are also in the process of drafting regulations for the management and oversight of this domain. Furthermore, some judicial and legal authorities in Iran have dealt with violations and crimes associated with cryptocurrencies by referencing general laws related to cyber and financial crimes.

In contrast, the common law system, which is in effect in countries such as the United States, Canada, and the United Kingdom, has adopted a more comprehensive approach due to its advanced legal infrastructure and greater experience in handling financial crimes. In this system, various laws have been enacted to counter crimes associated with cryptocurrencies. For example, in the United States, the Securities and Exchange Commission and the Financial Crimes Enforcement Network of the U.S. Department of the Treasury have developed precise regulations for the control and monitoring of cryptocurrency transactions. Additionally, courts in these countries have addressed numerous complex cases involving cryptocurrency crimes and have established a variety of judicial precedents.

Overall, although both the Iranian legal system and the common law system experience shared challenges in addressing crimes related to cryptocurrencies, there are notable differences in their approaches and legal frameworks. Iran is striving to draft and implement specific laws in this area, whereas the common law system, with its broader experience and more comprehensive regulations, is operating more advanced mechanisms for controlling and overseeing cryptocurrency-related activities.

2. The Legal Nature and Criminal Classifications Related to Cryptocurrencies in Iranian Law

Cryptocurrencies such as Bitcoin and Ethereum, as decentralized digital monetary units based on cryptographic technologies, have introduced a new form of financial exchange that fundamentally differs from traditional financial systems. Legally speaking, cryptocurrencies still possess an ambiguous status in Iran. While they are recognized as digital financial tools, there are no explicit laws or regulations for their governance and oversight. In recent years, Iranian government bodies and the Central Bank have taken varied stances, particularly concerning transactions and commercial activities involving cryptocurrencies. The Central Bank of Iran has emphasized, in several statements, the prohibition of using cryptocurrencies for financial transactions and has imposed restrictions particularly in the areas of foreign trade and international investments. This ambiguous legal status has resulted in cryptocurrency-related activities in Iran being subject to strict and sometimes informal oversight (Sharifi, 2020).

Numerous challenges are associated with cryptocurrencies in Iran. One of the primary problems is the absence of a clear and specific legal framework governing cryptocurrency-related activities. This lack of precise legislation can lead to legal loopholes and financial abuses. Additionally, the use of cryptocurrencies for illicit purposes such as money laundering and terrorism financing is a major concern, making the supervision and control of financial activities even more difficult. These issues, along with the extreme volatility in cryptocurrency prices, have made the management and regulation of such currencies in Iran complex and problematic. In Iranian law, due to the absence of specific legislation on cryptocurrencies, the criminality of related activities is indirectly addressed through other legal provisions. Activities such as money laundering, terrorism financing, and fraud, which may be conducted using cryptocurrencies, fall under Iran's general criminal law. In particular, the Anti-Money Laundering Act and the Counter-Terrorism Financing Law directly address suspicious and illegal financial activities and are applied to cryptocurrencies within this legal framework. Moreover, fraudulent schemes related to cryptocurrency investments and similar ventures are also recognized as criminal acts under general criminal law and may be subject to prosecution. Consequently, cryptocurrencies in Iranian law face multiple challenges and an ambiguous legal standing. This situation necessitates the formulation of more precise legislation to ensure the oversight and governance of cryptocurrency-related financial activities, in order to prevent legal and financial problems and to effectively counter illicit conduct (Mohammadi, 2020).

3. The Necessity of Criminalization in the Realm of Cryptocurrencies

The expansion of cryptocurrencies in Iran has highlighted the need for legal action concerning the various types of actors in this field. Although proactive approaches were initially taken, the country is lagging behind many others in terms of achieving

relative advancements. The most significant aspect of legislative intervention in Iran can be seen in the criminal dimension, which, unlike in many other countries that have treated cryptocurrencies as separate regulatory domains within anti-money laundering frameworks, has adopted a different approach by classifying them under currency smuggling. This route, while perhaps well-intentioned, could have achieved the objective of managing criminal risks associated with cryptocurrencies through the less complex route of applying anti-money laundering regulations.

In reality, it appears that there is no necessity to recognize cryptocurrencies as foreign currencies—an approach that has not been adopted by any country in practice. Most countries that have legislated on cryptocurrencies have recognized this technology as a "value" rather than money or foreign currency. Within this framework, legal recognition of cryptocurrency service providers and the imposition of certain requirements upon them have paved the way for the regulation of this area. Iran's approach of recognizing cryptocurrencies as foreign currency may lead to a theoretically stricter criminal stance, but in practice, it is not a suitable approach. On one hand, recognizing this technology as a value would have sufficed to bring it under the scope of anti-money laundering regulations and enforce the related obligations upon users and service providers. On the other hand, the global nature of cryptocurrencies—which lack backing, are highly volatile, and whose creators remain ambiguous—may strongly influence public interest in engaging with them. If the buying and selling of cryptocurrencies is complicated due to currency regulations, it can potentially criminalize a large number of individuals unnecessarily (Khalili Paji & Shamlou, 2021).

4. Crimes Related to Cryptocurrencies in the Iranian Legal System

The emergence of cryptocurrencies in the economic sphere has brought about significant transformations and changes; however, the challenges arising from their inherent nature pose substantial risks to the economy. The lack of a clear definition for digital currencies, as well as the novelty of their form, has resulted in traditional crimes—which previously required complex procedures—now being committed easily and without significant obstacles. Offenders can achieve their objectives by exploiting these types of currencies. It appears that governments and financial and economic institutions must first establish a precise definition of such digital currencies and develop appropriate regulations for processes such as their definition, exchange, and storage. Current laws are no longer effective in terms of oversight and deterrence. Considering the growing number of cryptocurrency users, the existing legal vacuum could lead to considerable harm and financial disorder across various societies at the international level.

4.1. Money Laundering in the Context of Cryptocurrency Use

Computer or cyber fraud is one of the crimes that occurs in cyberspace. In 2009, the Iranian legislature enacted the Computer Crimes Act. Article 13 of this law defines computer fraud as follows: "Anyone who, without authorization, uses computer or telecommunications systems to commit acts such as entering, altering, deleting, generating, or halting data or disrupting the system in order to obtain money, property, benefits, services, or financial privileges for themselves or others shall, in addition to returning the property to its rightful owner, be sentenced to one to five years of imprisonment or a fine ranging from twenty million rials to one hundred million rials, or both." In this article, the legislator has provided examples of behaviors that constitute computer fraud. “Entering” refers to inputting data into a computer system for processing. For instance, someone who takes another person’s debit card and empties their account via an ATM by entering the PIN is committing computer fraud through data entry. “Altering data” includes any modification—minor or major—of someone’s data. For example, altering one's bank account data to falsely show an unpaid loan as paid. Therefore, computer crimes are criminal acts with traditional characteristics that are committed using modern tools such as computers and the internet. Cyber fraud or internet fraud falls within this category (Rahimi & Amini Nia, 2021).

Given the current legal and regulatory limitations in this area, it is hoped that legislators will develop and adopt comprehensive laws aligned with international standards, considering the rapid technological developments that render national laws increasingly ineffective. Such legal development requires observing specific conditions to effectively prevent and combat cybercrime.

These conditions include:

A. Access to preventive technologies, which requires a suitable regulatory environment.

B. Awareness of potential security risks and methods to counter them.

C. The presence of substantive and procedural legal frameworks that take into account both domestic and international criminal activity.

D. Effective cooperation among all stakeholders, including users, consumers, industry sectors, law enforcement, and data protection authorities. This is essential for tracking cybercrime and ensuring public safety. Consequently, different sectors (users, consumers, industry, etc.) must act within defined roles and regulations. Governments should recognize that the needs of law enforcement may create obstacles for the industry and should take appropriate measures to minimize such barriers.

Regarding cyber theft, Chapter 3 of the 2009 Computer Crimes Act—titled “Theft and Fraud Related to Computers”—states in Article 12: "Anyone who, without authorization, steals data belonging to another shall be fined from one million rials to twenty million rials if the data remains with its owner, and otherwise shall be sentenced to ninety-one days to one year of imprisonment or fined from five million rials to twenty million rials, or both." (Izadi & Arzaniyan, 2019).

Additionally, Article 13 reiterates: "Anyone who, without authorization, uses computer or telecommunications systems to commit acts such as entering, altering, deleting, generating, or halting data or disrupting the system in order to obtain money, property, benefits, services, or financial privileges for themselves or others shall, in addition to returning the property to its rightful owner, be sentenced to one to five years of imprisonment or a fine ranging from twenty million rials to one hundred million rials, or both."

Virtual and cyber theft can also, in some cases, meet the criteria for theft punishable by hadd (fixed punishment). Nevertheless, the legislator has, contrary to traditional theft, considered cyber theft—regardless of whether it fulfills the hadd criteria—to be a tazir (discretionary punishment) offense. The general wording of Articles 12 and 13 encompasses cyber theft whether or not the hadd criteria are met and includes unauthorized data theft under offenses such as embezzlement, cyber robbery, and computer fraud. Therefore, the legislator’s general approach—especially considering the title of the chapter—implies that unauthorized appropriation of others' assets, whether framed as theft or under other offenses like embezzlement or fraud, warrants tazir penalties. There is no distinction between theft, which is traditionally subject to hadd when certain conditions are met, and other offenses involving unauthorized acquisition of property. All are subjected to discretionary punishment.

While this may be legally sound in the context of embezzlement and cyber fraud, it seems inadequate in the case of cyber theft. The conditions required for hadd punishment in theft can also exist in cyber theft—perhaps even more evidently. For example, data "harz" (protected space) and the covert nature of the theft may be more pronounced in cybercrime. Therefore, from the authors' perspective, applying tazir punishment absolutely to cyber theft is not entirely appropriate. The legislature should adopt a more stringent stance, distinguishing clearly between cyber theft, cyber embezzlement, and cyber fraud. Where the criteria for hadd theft are met, cyber theft should be considered a hadd crime. In fact, due to the gravity and expansive reach of cyber theft—enabled by the borderless nature of cyberspace—penalties might even need to be more severe than those for traditional theft. Otherwise, lenient treatment of cyber theft could embolden perpetrators to operate internationally and inflict significant, unparalleled damage (Moradizadeh, 2020).

Fast transactions via virtual currencies have made money withdrawal or conversion significantly quicker than through traditional means. The speed of these transactions complicates oversight, and the blending of cryptocurrency use with other modern and traditional money laundering methods has made detection and prosecution more difficult. Criminals can use these means to transfer illicit gains to jurisdictions with weaker laws and oversight regarding money laundering and convert them into cash or other assets. Furthermore, cryptocurrencies pose a high risk of fraud. The significant increase in the value of some virtual currencies can easily mislead investors, allowing criminals to seize assets by falsely promising cryptocurrency sales. Another method involves fraudulent sales in which the seller, after receiving cryptocurrency, refuses to send the goods or provide services. An additional example is the initial coin offering (ICO), where individuals claim to create new cryptocurrencies to collect funds, only to disappear afterward (Izadi-Fard & Hosseinnajad, 2019).

In some countries, authorities have adopted a "wait and see" approach to the novel phenomenon of virtual currencies like Bitcoin, observing the approaches of other nations before determining the best regulatory path. This strategy is typically divided into three stages. Some countries have not yet enacted or implemented any cryptocurrency regulations. Others, while

acknowledging the emergence of Bitcoin as a payment system or showing readiness to accept its risks, place the burden of risk on users under the principle of assumption of risk, without engaging in regulation. In certain legal systems, Bitcoin is partially self-regulating as a payment system, which allows internal mechanisms to support enforcement against illegal activity when Bitcoin is used as a currency or payment tool (Davari & Davari, 2011).

With a 90% market growth in Bitcoin in 2016 and the rise of cryptocurrencies, legal recognition and response to this new phenomenon became necessary. Consequently, in the European Union, tax laws have been structured to exempt cryptocurrency transactions from value-added tax (VAT), while other tax obligations depend on national enforcement bodies. In anti-money laundering regulations, cryptocurrency exchanges are required to implement user identity verification and report suspicious transactions. Exchanges that convert fiat money into cryptocurrencies are treated as assets or investments. The Commodity Futures Trading Commission (CFTC) has declared Bitcoin to be a commodity akin to oil or gold. Tax regulations further state that capital gains taxes apply to profits from such investments. Anti-money laundering laws also apply fully to cryptocurrency services. Regarding the overall legal framework, laws surrounding Bitcoin differ by jurisdiction within the United States, and various forms of non-criminal, social, situational, and community-based crime prevention are used (Davari & Davari, 2011).

Money laundering in cyberspace—especially with the growth of digital technologies and the internet—is being conducted through increasingly complex and innovative methods. These methods enable criminals to hide illicit funds using modern tools and techniques, effectively evading traditional surveillance and controls. One common method involves using digital currencies. Digital currencies, particularly cryptocurrencies such as Bitcoin and Ethereum, have become popular tools for money laundering due to their relative anonymity and lack of reliance on traditional financial intermediaries. Criminals can convert illegal money into cryptocurrencies and then, through complex transactions involving multiple digital wallets, convert these assets into legitimate funds. This process becomes even more difficult to trace when techniques such as "mixing"—which combines various transactions—are used (Fallahi & Momeni, 2018; Qaemi, 2022).

Finally, the use of online platforms and e-commerce sites—especially online stores and marketplaces—allows criminals to disguise illicit funds as legitimate income through small, repeated transactions. These transactions can be deliberately executed using various accounts and reciprocal sales to effectively launder money. Overall, money laundering in cyberspace, using diverse and complex methods, requires specialized attention and oversight to effectively combat and prevent the expansion of these illegal activities.

4.2. Examination of the Crime of Computer Fraud

The crime of computer fraud is recognized as a form of cyber and financial crime in both the Iranian legal system and the common law system; however, the definition, penalties, and judicial procedures differ between the two. In the Iranian legal system, computer fraud is defined under the 2011 Computer Crimes Act. Specifically, Article 13 addresses computer fraud and defines it as the unlawful acquisition of property using computer systems. To establish computer fraud under Iranian law, it must be proven that the accused intentionally used computer and internet technologies to deceive others and unlawfully acquire property. The punishment for this offense includes imprisonment ranging from one to five years and a monetary fine equal to twice the amount of the defrauded assets. Furthermore, if the fraud results in significant damage, additional penalties such as restitution to the plaintiff may be imposed (Tofighi, 2020).

In the common law system, computer fraud is regulated under general and specialized legislation in countries such as the United States, the United Kingdom, and other common law jurisdictions. In this system, fraud is typically defined as a deceptive act committed with the intent to obtain property through misrepresentation or deceit. For example, in the United States, federal laws such as the Computer Fraud and Abuse Act (CFAA) specifically address computer fraud and categorize it as an offense involving the misuse of computers and network systems. Under this system, establishing fraud generally requires proof of intentional deception and financial harm to the victim. Penalties for computer fraud in common law jurisdictions may include long-term imprisonment, heavy fines, and restitution for damages. Overall, while the fundamental principles of fraud are similar in both legal systems, there are significant differences in the structuring and enforcement of laws, definitions of offenses, and associated penalties. The Iranian legal system places specific emphasis on computer technology and the unique aspects of fraud in this domain, whereas the common law system offers a broader and more diversified legal framework to address these offenses, often focusing on deceptive conduct and the exploitation of digital technologies (Ahmadi, 2021).

4.3. Examination of Drug-Related Crimes Using Cryptocurrencies

Drug-related crimes involving cryptocurrencies are increasingly expanding due to the unique features of this technology, particularly anonymity and lack of oversight. These platforms are effectively used for illegal transactions, including the buying and selling of narcotics.

The first significant aspect is anonymity and privacy. Cryptocurrencies such as Bitcoin and Ethereum provide relative user anonymity, allowing transactions to occur without disclosing the actual identity of the participants. This feature enables drug sellers and buyers to conduct financial transactions without fear of identification or legal prosecution. Anonymity is particularly exploited in underground markets and the dark web, where widespread illegal activities are prevalent.

The second aspect involves the organization and management of distribution networks. Cryptocurrencies enable drug dealers to efficiently organize complex distribution networks. These networks can operate globally and use decentralized systems to facilitate financial transactions. By leveraging cryptocurrencies, dealers can transfer and relocate profits from drug sales in a secure and anonymous manner.

The third aspect is the transformation of payment and transfer methods. The use of cryptocurrencies allows drug traffickers to avoid traditional payment methods such as cash and bank accounts, instead utilizing digital wallets and blockchain transactions. This is especially useful in circumventing financial oversight and avoiding detection by legal authorities.

Finally, regulatory and legal challenges have significantly increased. With the emergence of this technology, monitoring illegal activities involving cryptocurrencies has become more complex, and many legal authorities face serious difficulties in tracking and identifying drug-related activities. These challenges include the technical complexities of blockchain, user anonymity, and the absence of adequate legal frameworks to combat such crimes. As a result, the use of cryptocurrencies in drug-related offenses has effectively increased regulatory complexities, making it essential to develop and update monitoring tools and regulatory frameworks to confront these crimes effectively (Shabani et al., 2020).

4.4. The Role of Cryptocurrencies in Committing Hacking and Theft Crimes

Cryptocurrencies play a significant role in hacking and theft crimes due to their specific characteristics, including anonymity, decentralization, and the ease and speed of transferring assets. These features attract cybercriminals to use cryptocurrencies for unlawful activities.

Anonymity and lack of transparency are key factors that allow cybercriminals to conceal their activities. Cryptocurrencies like Bitcoin and Ethereum keep users' identities relatively anonymous. While transaction data is publicly recorded on the blockchain, the real identities behind these transactions remain undisclosed. This feature allows hackers and cyber thieves to execute illegal transactions without fear of being identified. For example, when hackers gain access to digital wallets, they can easily transfer assets to other wallets, making tracking more difficult.

Phishing attacks and social engineering are also common methods used in cryptocurrency theft. Cybercriminals use phishing techniques to trick users into entering their login credentials on fake websites. Once these credentials are obtained, hackers can access victims' digital wallets and steal their cryptocurrencies. Social engineering tactics, such as fake messages or phone calls, are used to deceive users and gain access to sensitive information and digital assets.

Mixing services and organized crime networks also play a role in cryptocurrency theft. Mixing services, or “tumblers,” are designed to obscure the origin of transactions. These services allow hackers to blend stolen assets with other transactions, effectively hiding the source of the stolen cryptocurrencies and making it more difficult to trace.

Moreover, organized criminal groups can use cryptocurrencies to finance their illegal activities, thereby exacerbating legal and regulatory challenges (Naderi & Matlabi, 2021).

Online platforms and black markets are also extensively used to trade stolen cryptocurrencies. These platforms allow criminals to easily sell their digital assets and earn illicit profits. Operating on the dark web, these markets are specifically designed for exchanging and selling stolen cryptocurrencies and often use various methods to hide identities and financial locations.

The use of cryptocurrencies in hacking and theft crimes significantly increases security and regulatory complexities, making it necessary to adopt stronger measures and more advanced technologies to identify and combat such offenses effectively.

4.5. The Crime of Terrorism Financing

Terrorism financing refers to the provision of financial resources to organizations or individuals involved in terrorist activities. It is considered a serious offense both internationally and domestically, and extensive efforts have been made to identify, prevent, and prosecute individuals and entities engaged in such acts. Terrorism financing may include providing cash, convertible assets, equipment, or any other form of financial assistance that enables terrorist organizations and individuals to carry out their operations. It poses a significant threat to both national and international security. The sources of terrorist financing can originate from various avenues, including lawful activities such as charitable donations or front companies, and unlawful ones such as drug trafficking, human trafficking, and money laundering. This multiplicity of sources makes identifying and disrupting the financial chain of terrorism a major challenge for governmental and international bodies (Alidoost & Pourghahramani, 2018).

One of the primary challenges in combating terrorism financing is the obscurity of the financial routes and intermediaries used by terrorists. To address this issue, many countries have implemented strict regulations requiring banks and financial institutions to report suspicious transactions. These regulations typically include customer identity verification, monitoring large and suspicious transactions, and reporting them to financial intelligence units. International organizations such as the Financial Action Task Force (FATF) also play a crucial role in developing and promoting global standards for combating terrorism financing. Their recommendations provide countries with legal, regulatory, and operational measures to protect financial systems from terrorist abuse, including mechanisms for identifying and blocking terrorist financial resources (Alidoost & Pourghahramani, 2018).

The enforcement of counter-terrorism financing laws and regulations requires broad international cooperation. Countries must share information on suspicious transactions and collaborate in pursuing and apprehending individuals involved in terrorism financing. Such cooperation can occur through bilateral treaties, regional alliances, and international institutions like INTERPOL. In Iran, the Anti-Terrorism Financing Act of 2015 comprehensively addresses this issue. This law defines terrorism financing as a crime and prescribes severe penalties for individuals involved. Moreover, regulatory and enforcement bodies such as the Central Bank and the Financial Intelligence Unit are tasked with monitoring and controlling suspicious financial transactions to prevent the flow of resources to terrorist entities. Overall, terrorism financing is a major security threat that demands both international and domestic collaboration. Strict laws, effective monitoring of financial transactions, and international cooperation are essential for reducing this threat and ensuring global security.

4.6. Assessment of Gambling Offenses in the Context of Cryptocurrencies

With technological advancement enabling various activities without physical presence, virtual casinos have emerged as platforms offering gambling services to users without requiring their physical presence. The only difference between virtual and physical casinos is the absence of a physical location for the former; otherwise, gambling activities are identical. Therefore, the legal element of the crime of operating a virtual casino aligns with Article 708 of the Islamic Penal Code (Discretionary Punishments, 1996). The material element of the offense consists of creating a website or online platform for gambling activities, which must be established through a positive act—mere omission or failure to act does not constitute the crime.

The mental element of this offense involves the perpetrator's awareness that operating a virtual casino is a criminal act and their deliberate intent to commit it by launching the gambling website. Hence, if a person creates such a site merely for entertainment purposes or to increase website traffic and does not collect any monetary or material assets from participants, the elements of the crime are not fulfilled (Schopper, 2014).

Given the rise of online gambling and betting, generating income through advertising for these sites has become increasingly common. Although advertising and invitation may appear different in form, both constitute types of complicity and are independently criminalized under Article 708. Therefore, advertising or inviting people to gamble in cyberspace falls under the same legal provision. Even if a person does not name a specific gambling website but invites others to engage in online gambling, the offense is realized. The material element here is a positive physical act—invitation to online gambling cannot be carried out through inaction (Parcker, 2017).

The mental element consists of the inviter's knowledge that what is being advertised is a criminal form of gambling and their deliberate action to promote it. Therefore, if a person, unaware of the content of a gambling site and under the belief that they are promoting a computer game, invites others to participate, they likely have not committed a crime, as the requisite mental element is absent.

In the offense of aiding and abetting in running gambling houses, the material element involves providing services or assistance in any form to the operation of such establishments. Aiding may include encouraging, inciting, accounting, logistics, or cleaning—all forms of material assistance to the principal offender. These acts must be overt and positive; mere presence or observation does not constitute complicity. Any person—regardless of gender or employment status—who can be held criminally responsible may be guilty of this offense. The mental element of aiding and abetting involves general criminal intent, requiring that the accomplice knowingly and willingly participated in the commission of the crime (Danai Far, 2020).

As previously noted, gambling occurs when individuals—either physically or online—engage in games involving items such as boards, cards, coins, or nuts, and agree that the loser will pay the winner a specified asset, whether cash, property, or some benefit. If individuals act with malicious intent—meaning the belief that the winner will acquire property from the loser—they commit the crime of gambling under Article 705 of the Islamic Penal Code (Imani Shirkalai, 2000). To determine the punishment for gambling in physical spaces like casinos, one must refer to the revised Discretionary Punishments section of the Penal Code, particularly the amendments made in 2021. The amended Article 705 states: "Anyone who… commits gambling or betting in a physical space or participates in a lottery shall, in addition to the seizure of all criminal proceeds, be sentenced to a sixth-degree monetary fine or a fine equivalent to one to three times the total proceeds of the crime, whichever is greater." Based on this article, the punishment for physical gambling, such as in casinos, includes both the confiscation of criminal proceeds and a monetary fine ranging from approximately 60 to 240 million Iranian rials or one to three times the total criminal gains, whichever is greater (Ahmadi, 2023).

In conclusion, victims of cryptocurrency-related crimes require special attention and support from legal and regulatory institutions to effectively mitigate the harms resulting from these offenses and to facilitate their financial and psychological recovery.

4.7. Currency-Related Crimes Against National Security

Understanding the foundations of criminalization and the consequences of committing "currency-related crimes" is crucial due to their direct impact on a nation's foreign exchange reserves and their influence on currency exchange rates. Accordingly, the commission of various types of currency-related crimes must, under specific circumstances, be considered crimes against the "economic security" of the country. The Iranian legislature has recognized certain forms of these crimes and prescribed severe discretionary punishments, including imprisonment ranging from five to twenty years. Disruption of the foreign exchange system and currency-related crimes that lead to disturbances in the country's export system are among the most significant examples. In specific contexts, the legislature, adopting a strict criminal policy, has escalated penalties and classified some forms of these offenses as capital crimes under the category of *efsad fel-arz* (corruption on earth), for which the perpetrator is subject to the death penalty—the most severe punishment under Islamic jurisprudence and Iran's legal system. Examples of *efsad fel-arz* through disruption of the currency system include large-scale currency smuggling, misuse of proceeds from currency smuggling to finance terrorism, counterfeiting of currency, and importation of counterfeit currency. Nevertheless, it is important to note that the Iranian legislature has, at different times, employed varying criminal policies toward these crimes. While earlier phases adopted strict penal policies, subsequent phases saw a shift toward leniency, before returning once more to harsher punitive measures. A common feature across most legislative periods in Iran has been the dependence of criminal policy on governmental economic strategies (Mojahid, 2016).

5. Crimes Related to Cryptocurrencies in the Common Law Legal System

This section addresses cryptocurrency-related crimes in the United States, Canada, the United Kingdom, and Australia.

5.1. Cryptocurrency-Related Crimes in the United States

Due to the increasing use of digital currencies and blockchain technology, cryptocurrency-related crimes have become a significant issue in the U.S. legal system. These crimes include a range of offenses such as money laundering, fraud, theft, and various unlawful activities conducted via digital currencies. The decentralized and anonymous nature of these currencies poses substantial challenges for detection and enforcement. One of the most prevalent cryptocurrency-related offenses is money laundering. Criminal individuals and organizations use digital currencies to transfer illicit funds. The U.S. Department of the Treasury and other regulatory bodies have actively developed laws and regulations to combat these crimes. For instance, the Financial Crimes Enforcement Network (FinCEN) has implemented stringent rules to enhance transparency in cryptocurrency transactions (Abbasi, 2021).

Fraud and theft are also widespread. Hackers use sophisticated techniques to breach digital wallets and cryptocurrency exchanges, stealing users' assets. Moreover, fraudulent investment schemes promising high returns have lured many investors into scams. The U.S. Securities and Exchange Commission (SEC) enforces securities laws to protect investors against such fraudulent schemes. The use of cryptocurrencies in illegal activities such as drug and weapons trafficking has raised additional concerns. The U.S. Department of Justice and the FBI actively pursue and apprehend individuals who use digital currencies for illicit purposes. Numerous operations have been carried out to shut down darknet markets that facilitated illegal transactions through cryptocurrencies (Maleki, 2020).

Overall, in response to the rapid and extensive growth of digital currency use, the U.S. legal system is adapting and expanding its legal framework to combat cryptocurrency-related crimes. Regulatory and judicial bodies have undertaken significant efforts to ensure the security and transparency of the cryptocurrency market and continuously update and strengthen their legal instruments.

5.2. Cryptocurrency-Related Crimes in Canada

As one of the leading countries in adopting and regulating digital currencies, Canada has faced various challenges related to cryptocurrency-related crimes. The increasing use of digital currencies such as Bitcoin and Ethereum for financial transactions and investment has led to the emergence of several criminal activities, prompting the Canadian legal system to manage these challenges through detailed laws and regulations. One of the most significant issues is money laundering. Criminals exploit the anonymous and untraceable nature of cryptocurrency transactions to transfer and launder illicit funds. In response, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has enacted anti-money laundering and anti-terrorist financing regulations. These include requirements for financial institutions and cryptocurrency exchanges to report suspicious transactions and verify customer identities (Mohammadi, 2020).

In addition to money laundering, fraud and theft are other common cryptocurrency-related crimes in Canada. Hackers use advanced techniques to breach users' digital wallets and cryptocurrency exchanges, stealing their funds. Regulatory authorities such as the Ontario Securities Commission and the British Columbia Securities Commission enforce strict rules to enhance transparency and security in digital currency markets and prevent such crimes. Furthermore, the use of digital currencies for illegal activities like drug and weapon trafficking remains a challenge. The Royal Canadian Mounted Police (RCMP) and other security agencies actively cooperate with international organizations to identify and arrest individuals engaged in such activities. Several operations have been conducted to dismantle darknet markets that rely on cryptocurrencies for illegal transactions.

Overall, in light of the rapid and widespread adoption of digital currencies, Canada's legal system is evolving to address cryptocurrency-related crimes. Regulatory and judicial efforts aim to strengthen legal frameworks to prevent criminals from exploiting legal loopholes, ensuring market integrity and public safety.

5.3. Cryptocurrency-Related Crimes in the United Kingdom

The United Kingdom, a leader in financial technologies and digital currencies, has encountered numerous challenges in addressing crimes involving cryptocurrencies. The decentralized and relatively anonymous nature of cryptocurrency transactions has made this technology attractive to criminals. Consequently, the UK legal system continuously develops and

updates its regulatory framework to combat such offenses. One of the most pressing issues is money laundering, where criminals use digital currencies to move and launder illegal funds. The UK's Financial Conduct Authority (FCA) and the National Crime Agency (NCA) enforce strict regulations to oversee digital financial activities and combat money laundering. These include mandatory registration for cryptocurrency exchanges and the requirement to report suspicious transactions.

Fraud and theft are also common. Hackers infiltrate digital wallets and exchanges to steal users' assets. UK regulatory authorities implement robust security and oversight measures to prevent such crimes. Additionally, the Metropolitan Police Service plays an active role in investigating and apprehending hackers and cybercriminals operating in this domain. The use of digital currencies for illegal activities such as drug and weapons trafficking has also been observed in the UK. British police, in cooperation with international agencies and through advanced technologies, work to identify and suppress such crimes. For example, darknet markets that facilitate illegal transactions using cryptocurrencies are often the focus of enforcement operations (Zarei, 2018).

In summary, the UK legal system is continuously updating and strengthening its laws and regulations to combat cryptocurrency-related crimes. By establishing strong legal and regulatory infrastructure, the UK aims to support financial innovation while preventing criminal exploitation, ensuring security and transparency in digital currency markets.

5.4. Cryptocurrency-Related Crimes in the Australian Legal System

Australia, as one of the leading countries in embracing and regulating digital currencies, has encountered various challenges related to cryptocurrency crimes. Due to their unique features such as anonymity and rapid transferability, digital currencies have become highly attractive to criminals. In response, the Australian legal system has implemented comprehensive laws and regulations to combat these offenses. One of the most prominent crimes involving cryptocurrencies in Australia is money laundering. Criminals use digital currencies to transfer and launder illicit funds. The Australian Transaction Reports and Analysis Centre (AUSTRAC) has established strict regulations to combat money laundering and the financing of terrorism. These include requirements for digital currency exchanges to register, report suspicious transactions, and conduct customer identity verification.

Fraud and theft are also common in the cryptocurrency sphere. Hackers penetrate users' digital wallets and cryptocurrency exchanges to steal their assets. The Australian Securities and Investments Commission (ASIC) enforces stringent security and regulatory measures to prevent such crimes. In addition, the Australian Federal Police actively investigates and apprehends cybercriminals operating in this domain. The use of cryptocurrencies in illegal activities, such as the trade of narcotics and weapons, has also been reported. Australian law enforcement collaborates with international agencies and leverages advanced technologies to identify and suppress such offenses. For example, several operations have been launched to dismantle darknet markets that facilitate illegal transactions through digital currencies (Qasemi, 2019).

Overall, the Australian legal system is continually updating and strengthening its legal framework to address cryptocurrency-related crimes. By developing robust legal and regulatory infrastructures, the country seeks to support financial innovation while preventing criminal abuse and ensuring the security and transparency of digital currency markets.

6. Criminal Prosecution of Cryptocurrency Crimes

In legislating financial and currency-related crimes, key features include addressing legal deficiencies, ensuring public acceptance of laws, implementing flexible sentencing systems, and empowering early warning mechanisms. In the judicial sphere—where cases are handled by national courts and judicial institutions—there is an emphasis on the appropriate application of penalties and criminal enforcement mechanisms to deter offenders and prevent future crimes. Judicial authorities must be meticulous and technically informed in their assessments, ensuring proportionality between the offense and the punishment, and individualizing sentences to enhance the preventive function of criminal justice. Judges should incorporate expert perspectives, especially in financial crimes, and minimize judicial errors through professional and specialized training, thereby fostering public trust in the judiciary. Without such integrity, the credibility of judicial rulings may erode, reducing public motivation to refrain from criminal acts and potentially allowing real offenders to evade justice while innocent individuals are punished (Forghandoust Haghighi & Nadaf, 2023).

7. Procedures for Filing Complaints Related to Cryptocurrency Crimes

Filing complaints regarding cryptocurrency crimes involves navigating complex legal processes due to the distinct characteristics of digital currencies. These crimes may include financial fraud, digital theft, and other illicit activities. The first step is gathering evidence and documentation. Victims must collect all relevant data about the suspicious or illegal activity, including details of suspicious transactions, email communications, and information about encrypted accounts. Maintaining detailed transaction records is critical, as such evidence plays a key role in advancing the legal case.

The next step involves reporting the crime to relevant judicial and law enforcement agencies. Victims should approach legal authorities such as the Cyber Police (FATA) or local police departments to file their complaints. In Iran, FATA is the designated authority for handling cyber and computer-related crimes, including cryptocurrency offenses. Filing a complaint involves completing specific forms and submitting the collected evidence to the appropriate authority. Legal proceedings then begin with the formation of a case and investigation by the judiciary. Prosecutors and courts, recognizing the technical nature of cryptocurrency crimes, often consult technology and legal experts to conduct detailed case analyses. Collaboration with IT specialists and analysts may be required to present technical and legal information to the judiciary. In some cases, international cooperation and the use of cross-border legal channels may also prove useful (Naderi & Matlabi, 2021).

Given the global and transnational nature of cryptocurrencies, pursuing justice may necessitate cooperation with international organizations such as INTERPOL or international tribunals. This cooperation may include sharing information and evidence and requesting assistance from the judicial authorities of other countries.

8. Criminal Liability of Legal Entities for Cybercrimes

The criminal liability of legal entities for cybercrimes has become a significant and debated topic in many legal systems, particularly in recent decades. With the rapid expansion of digital technologies and the growing prevalence of cybercrimes such as hacking, online fraud, and privacy violations, the issue has gained greater prominence. Criminal liability of legal entities refers to the legal responsibility of corporations and non-natural persons for crimes committed by their employees or representatives. In cybercrimes, this liability can involve the use of corporate IT infrastructure or computer systems to engage in illegal activities.

In several legal systems, including Iran's, legal entities can be prosecuted for violating cyber laws, including data breaches, malware distribution, and participation in online fraud. Under Iran's Islamic Penal Code, specific attention is paid to the criminal liability of legal entities. Article 7 of the Penal Code (Discretionary and Deterrent Punishments) stipulates that if a crime is committed by employees or directors in connection with the legal entity's activities, the entity itself will bear criminal responsibility. Penalties may include monetary fines, suspension of commercial operations, and mandates for corrective or preventive actions (Rezavi Fard & Mousavi, 2016).

Due to the technical and organizational complexities of cybercrimes, determining the criminal liability of legal entities requires specialized and detailed assessments. It must be proven that the crime resulted from intentional misconduct or negligence in fulfilling legal and security obligations. This may involve analyzing internal corporate procedures, security systems, and managerial oversight mechanisms.

9. Challenges and Solutions for the Adoption of Digital Cryptocurrencies in the Legal Systems of Iran and Common Law

A comparative study of the challenges and solutions related to the adoption of digital cryptocurrencies in the legal systems of Iran and Common Law jurisdictions reveals significant differences and similarities in the management and regulation of these emerging instruments. In the Iranian legal system, the primary challenges associated with cryptocurrencies pertain to concerns about economic security and legal ambiguity. Due to fears of economic risk and the potential adverse effects on the financial and economic systems, Iran has implemented restrictive measures to limit the use of cryptocurrencies. The Central Bank of the Islamic Republic of Iran closely monitors cryptocurrency-related activities and has adopted actions such as prohibiting banks and financial institutions from engaging with cryptocurrencies in order to prevent money laundering and terrorist financing. This conservative approach is particularly evident in the strict regulations imposed on exchanges and

financial entities associated with cryptocurrencies. However, such restrictive measures may lead to market instability and reduce the country's ability to harness the potential benefits of this technology (Sadeghi & Nasir, 2021).

In contrast, Common Law systems—especially in developed countries like the United States and the United Kingdom—take a different approach. These countries have sought to leverage the advantages of digital assets while mitigating their risks by developing clear and comprehensive regulatory frameworks for managing cryptocurrencies. In the United States, agencies such as the Securities and Exchange Commission (SEC) and the Financial Crimes Enforcement Network (FinCEN) have established regulatory measures aimed at monitoring cryptocurrency activities, particularly focusing on anti-money laundering and counter-terrorism financing. Similarly, the United Kingdom, through the Financial Conduct Authority (FCA), has created frameworks to regulate the cryptocurrency environment and mitigate associated risks.

Proposed solutions for Iran include enhancing and strengthening cryptocurrency-related laws and regulations, establishing clear and supportive legal frameworks, and employing advanced technologies for risk monitoring and management. Moreover, Iran should align itself with international standards to benefit from the economic opportunities presented by cryptocurrencies while minimizing potential threats. In Common Law jurisdictions, strategies involve the continuous updating and improvement of financial and economic regulations, expanding international cooperation for regulating and overseeing cryptocurrencies, and enhancing the use of modern technologies for managing and supervising digital economic activities. This approach seeks to balance the utilization of cryptocurrency advantages with the protection of the financial and economic system against associated risks. In summary, while Iran emphasizes heavy restrictions and strict oversight, Common Law countries aim to develop coherent and adaptable legal structures to manage cryptocurrencies and mitigate their risks.

10. Conclusion

Cryptocurrencies, as an emerging phenomenon in the world of finance and technology, have brought about major transformations in the conduct of financial transactions. However, the growing use of these digital currencies has also introduced new legal challenges. An analysis of the legal systems of Iran and Common Law jurisdictions reveals that while both face similar issues, they have adopted markedly different approaches.

In Iran, due to the novelty of cryptocurrencies and the absence of comprehensive legal provisions, there are significant challenges in addressing crimes related to this domain. Nevertheless, financial institutions and lawmakers in Iran are currently working to draft regulations to manage and monitor this sector. These efforts reflect an awareness of the importance of creating appropriate legal frameworks to prevent misuse and financial crimes associated with cryptocurrencies. On the other hand, Common Law systems, benefiting from more developed legal infrastructures and greater experience with financial crimes, have adopted more comprehensive approaches. The existence of multiple laws and robust regulatory bodies such as the SEC and FinCEN has enabled countries within this legal tradition to possess more effective tools to combat cryptocurrency-related crimes. This highlights the importance of having a coherent and efficient legal framework to control and supervise cryptocurrency-related activities.

Although there are substantial differences between Iran and Common Law jurisdictions in addressing cryptocurrency-related crimes, both systems are progressing and striving to tackle the legal challenges of this field. The adoption of more comprehensive approaches and the establishment of international cooperation can enhance regulatory effectiveness and reduce financial crimes associated with cryptocurrencies. It appears essential for both Iran and Common Law systems to enact specific and comprehensive legislation for the regulation and supervision of cryptocurrencies. Such legislation should include detailed provisions on transaction transparency, customer identification, anti-money laundering practices, and the reporting of suspicious transactions. Furthermore, international collaboration between regulatory and judicial bodies can play a crucial role in combating cryptocurrency-related financial crimes.

One of the main challenges in this area is the rapid pace of change and innovation in cryptocurrency technologies. Therefore, legal frameworks must be designed with sufficient flexibility to adapt to these rapid developments. Additionally, public education and awareness-raising regarding the risks and benefits of using cryptocurrencies can contribute to reducing misuse and financial crimes. Ultimately, cooperation and coordination among various domestic and international institutions in the areas of oversight and law enforcement will be key to successfully combating cryptocurrency-related financial crimes. The

experience of Common Law systems can serve as a valuable model for developing countries like Iran, enabling them to improve their legal systems and establish suitable legal frameworks for managing and supervising cryptocurrencies.

In summary, while cryptocurrencies offer significant opportunities for innovation and economic growth, they also pose considerable challenges. The development and implementation of appropriate laws, public education and awareness, and international cooperation are among the key actions that can effectively help counter financial crimes associated with cryptocurrencies. By adopting comprehensive approaches and fostering international partnerships, the legal systems of Iran and Common Law jurisdictions can establish a secure and trustworthy environment for the use of cryptocurrencies.

Ethical Considerations

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

Acknowledgments

Authors thank all individuals who helped us do 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

Abbasi, A. (2021). *Laws and regulations of cryptocurrencies in the United States*. Tehran: University of Tehran Press.
Ahmadi, A. (2023). *Financial and currency crimes: Analysis of victims and countermeasures*. Tehran: University of Tehran Press.
Ahmadi, H. (2021). *Cyber criminal law*. Tehran: Islamic Azad University Press.
Alidoost, S., & Pourghahramani, B. (2018). Financing cybercrime and Iran's criminal policy towards it. *Journal of Jurisprudence and Islamic Law Foundations*, *63*, 5-38.
Danai Far, M. (2020). *Internet gambling and betting in Iranian and English criminal law* Master's thesis, Criminal Law and Criminology, Payame Noor University, South Tehran Branch].
Davari, M. R., & Davari, M. (2011). Electronic money laundering and technical and international countermeasures. *Journal of Non-Combat Defense*, *1*(4), 45-65.
Fallahi, M., & Momeni, A. (2018). Examination of financial and tax laws combating money laundering concerning virtual currencies: A study of the European Union and the United States. National Conference on New Approaches in Management, Economics, and Accounting,
Forghandoust Haghighi, K., & Nadaf, R. (2023). A review of cryptocurrencies: Opportunities and threats. *New Research Approaches in Management and Accounting*, *9*, 150-184.
Imani Shirkalai, K. (2000). *Gambling and related crimes in Iranian criminal law* Master's thesis, Criminal Law and Criminology, University of Tehran].
Izadi-Fard, A., & Hosseinnajad, S. M. (2019). The nature of virtual thefts (Critique of Articles 12 and 13 of the Cyber Crimes Law). *Studies in Jurisprudence and Islamic Law*, *11*(21), 50-76.
Izadi, Z., & Arzaniyan, N. (2019). Preventing money laundering and fraud in the context of global cryptocurrency usage. *Journal of Crime Prevention Approaches*, *2*(1), 37-56.
Khalili Paji, A., & Shamlou, B. (2021). Criminalization in the realm of cryptocurrencies. *Journal of Criminal Law Teachings*, *21*, 29-68.
Maleki, N. (2020). *Legal analysis of cyber crimes in the United States*. Tehran: Samt Publishing.
Mohammadi, H. (2020). *Comparative analysis of criminal law in the United States and Iran regarding cryptocurrencies*. Tehran: Shahid Beheshti University Press.
Mojahid, M. (2016). Typology of currency crimes as crimes against the economic security of the country. *Horizons of Security Journal*, *9*(33), 1-30.
Moradizadeh, K. (2020). Criminal examination of the dimensions and elements of computer fraud. *Scientific-Legal Journal of Lawyar*, *4*(15), 795-821.
Naderi, S., & Matlabi, M. (2021). Examination of legal solutions for extracting and trading digital and virtual currencies: Legal gaps and proposed solutions. *Legal Civilization Journal*, *4*(9), 7-18.
Parcker, J. D. (2017). *Gambling or Gaming: Entertainment or Exploitation?* https://www.churchofengland.org/sites/default/files/11-Gambling%20Policy.pdf
Qaemi, S. (2022). *Money laundering with digital currencies: Challenges and solutions*. Tehran: Islamic Azad University Press.
Qasemi, P. (2019). *Legal challenges in the world of digital currencies*. Tehran: Jungle Publishing.

Rahimi, A., & Amini Nia, A. (2021). Cryptocurrencies, challenges, and related crimes. *Lawyar Journal*, *5*(18), 225-244.
Rezavi Fard, B., & Mousavi, S. N. (2016). Criminal liability in cyberspace under Iranian law. *Criminal Law Research*, *5*(16), 29-45.
Sadeghi, M., & Nasir, M. (2021). Comparative study of challenges and solutions for using digital cryptocurrencies in the legal systems of Iran and the United States. *Journal of Private Law Studies*, *51*(2), 275-293.
Schopper, M. D. (2014). Internet Gambling, Electronic Cash & Money Laundering: The Unintended Consequences of a Monetary Control Scheme. *Chapman Law Review*, *5*, 303. https://www.chapman.edu/law/files/publications/CLR-5-mark-schopper.pdf
Shabani, A. M., Mohseni Dehkalani, M., & Ebrahimi, S. (2020). Comparative study of Bitcoin legislation. *Comparative Law Research Journal*, *4*(5), 209-238.
Sharifi, H. (2020). *Economic criminal law*. Tehran: University of Tehran Press.
Tofighi, S. (2020). *Cyber crimes and information security*. Tehran: University of Tehran Press.
Zarei, M. (2018). *International criminal law and new technologies*. Tehran: Allameh Tabatabai University.