Legal Gaps in Cryptocurrency Payments and Related Crimes: Proposals for Criminalization and Legislative Reform in Iran

1. Hossein Nikbakhti: Department of Law, ShQ.C., Islamic Azad University, Shahr-e Qods, Iran
2. Massoud Alizadeh*: Assistant Professor, Department of Law, Faculty of Social Science, Payame Noor University, Tehran, Iran

*Correspondence: massoud.alizadeh@pnu.ac.ir

Abstract

The rapid expansion of cryptocurrency use has created significant challenges for legal systems whose financial and criminal regulations were primarily designed for centralized and institutionally supervised payment mechanisms. In Iran, the growing use of crypto-assets for the transfer of economic value has not been accompanied by a comprehensive and coherent legislative framework governing cryptocurrency payments, service providers, user identification, transaction monitoring, digital evidence, and asset recovery. This study aims to identify the principal legal gaps affecting cryptocurrency payments, examine the crimes arising from or facilitated by those gaps, and propose an appropriate framework for criminalization and legislative reform. Using a descriptive-analytical legal method, the study examines the legal status of crypto-assets, the fragmented regulatory environment, and the applicability of existing criminal-law rules to cryptocurrency-related misconduct. The findings indicate that the principal deficiencies concern uncertainty regarding the legal classification of crypto-assets, the absence of a unified licensing regime for cryptocurrency service providers, inadequate customer-identification and record-keeping requirements, weaknesses in transaction tracing and institutional coordination, ambiguity concerning digital evidence, and insufficient procedures for freezing, seizing, confiscating, and restituting digital assets. These deficiencies can facilitate fraud, unauthorized transfers, cyber-enabled appropriation, money laundering, unlawful financial intermediation, and the concealment or transfer of criminal proceeds. The study argues that reform should avoid indiscriminate criminalization of cryptocurrency technology and instead adopt a regulated-legality model based on technological neutrality, proportionality, and risk-based supervision. The proposed framework includes statutory recognition of crypto-assets as legally protectable economic value, clear definitions of regulated activities, licensing of professional service providers, customer due diligence, transaction-record obligations, targeted criminalization of intentional harmful conduct, recognition of blockchain evidence, specialized asset-recovery procedures, stronger institutional coordination, and enhanced technical and international cooperation.

Keywords: Cryptocurrency Payments; Crypto-Assets; Legal Gaps; Criminalization; Financial Crime; Digital Evidence; Money Laundering; Legislative Reform; Iran

Received: 15 June 2026
Revised: 17 September 2026
Accepted: 24 September 2026
Initial Publication: 25 September 2026
Final Publication: 01 June 2027

Citation: Nikbakhti, H., & Alizadeh, M. (2027). Legal Gaps in Cryptocurrency Payments and Related Crimes: Proposals for Criminalization and Legislative Reform in Iran. *Legal Studies in Digital Age,* 6(6), 1-17.

1. Introduction

The emergence of cryptocurrencies has transformed the traditional understanding of money, payment, ownership, financial intermediation, and the territorial organization of economic transactions. Unlike conventional means of payment, which are ordinarily issued, transferred, recorded, or supervised within institutional structures consisting of central banks, commercial banks, payment companies, clearing institutions, and other regulated intermediaries, cryptocurrencies may permit economic value to be transferred directly between users through distributed technological infrastructures. Their development has therefore challenged legal concepts that were originally formulated on the assumption that monetary transactions would take place through identifiable persons and institutions operating within defined territorial jurisdictions. Cryptocurrency is not simply a technological variation of electronic banking. Its architecture may alter the relationship between possession, control, identification, transfer, record keeping, and legal responsibility. Crypto-assets may function as investment instruments, speculative assets, mechanisms for storing value, methods of transferring wealth across borders, or means of payment for goods and services. This multiplicity of functions has made their legal classification difficult and has complicated attempts to subject them to conventional financial and criminal-law categories. Theoretical analyses of cryptocurrency have consequently emphasized that its significance cannot be understood solely by asking whether it constitutes "money"; rather, its economic and legal functions must be examined separately in relation to the particular transaction in which it is used (Chohan, 2021). The difficulty becomes especially pronounced where a crypto-asset performs a payment function despite not possessing the formal characteristics of sovereign currency. Regulatory frameworks that depend exclusively on classifications derived from conventional banking and securities law may therefore leave important transactions outside effective supervision (Jabotinsky, 2020).

Cryptocurrency payments present particular regulatory challenges because they combine technological decentralization with the possibility of economically significant transfers that may be completed without the traditional financial intermediaries on which regulatory systems depend. Blockchain-based systems may provide a persistent record of transfers, but the existence of a transaction record does not necessarily mean that the legal identity of the person controlling a wallet is apparent. This distinction between transactional transparency and user identification is fundamental. Public blockchains may record transfers openly while allowing participants to operate through cryptographic addresses that do not, by themselves, reveal civil identity. As a result, cryptocurrency should not be simplistically characterized as completely anonymous, but its pseudonymous structure can nevertheless impede ordinary identification practices and complicate law-enforcement investigations (Europol, 2021). The development of privacy-enhancing technologies, decentralized protocols, cross-chain transfers, mixers, non-custodial wallets, and multiple exchange environments further increases the complexity of identifying the ultimate controller and beneficiary of particular funds. Studies of cryptocurrency-related financial offenses have shown that offenders can exploit multiple stages of conversion, transfer, fragmentation, and reaggregation in order to obscure the connection between criminal proceeds and their ultimate destination (Boyko et al., 2022). These characteristics do not establish that cryptocurrency is inherently criminal, but they demonstrate why a legal framework designed around centralized financial intermediaries may not provide adequate coverage when value moves through decentralized or semi-decentralized networks.

The regulatory challenge is intensified by the legitimate economic functions of crypto-assets. A legal system cannot respond effectively merely by treating every cryptocurrency transaction as suspicious or undesirable. Financial innovation can reduce transaction costs, create new channels for investment, facilitate cross-border settlement, expand access to digital financial services, and promote new commercial models. FinTech and blockchain scholarship has repeatedly emphasized that the technological architecture underlying crypto-assets has applications that extend substantially beyond speculative trading (Rabbani et al., 2020). The broader development of blockchain-based financial services also demonstrates that regulation must account for the interaction between innovation, financial inclusion, cybersecurity, market stability, and criminal misuse (Hasan et al., 2020). Regulatory policy must therefore distinguish legitimate technological innovation from conduct that generates legally cognizable harm. An excessively restrictive model may push legitimate activity into informal or foreign markets, reduce domestic regulatory visibility, and weaken the ability of authorities to obtain transaction information. Conversely, a permissive model that leaves exchanges, custodians, payment facilitators, and other service providers without clear obligations may create opportunities for fraud, laundering, cybercrime, unauthorized financial activity, and concealment of criminal proceeds.

Regulation consequently requires a calibrated approach in which authorization, supervision, compliance duties, and criminal liability operate as complementary rather than interchangeable mechanisms.

The Iranian legal system faces this problem in a particularly complex context. The expansion of cryptocurrency use has not been accompanied by a single comprehensive legislative framework that clearly determines the legal position of crypto-assets, the permissible scope of payment activities, the licensing status of relevant intermediaries, the rights and obligations of users, and the circumstances in which crypto-related misconduct constitutes an independent criminal offense. Studies of Iranian criminal policy have identified fragmentation and inconsistency as recurring characteristics of the domestic approach to cryptocurrency-related conduct (Bakhshi, 2025). Iranian policy has developed through a combination of monetary restrictions, administrative decisions, rules concerning mining and energy use, general criminal law, cybercrime provisions, anti-money-laundering regulations, and institutional measures affecting exchanges and financial services. Such a structure may address particular manifestations of cryptocurrency activity without resolving the larger question of how cryptocurrency payments should be legally characterized and governed. Research focusing specifically on Iranian legislative and judicial criminal policy has similarly identified tension between the growing economic reality of crypto-assets and the absence of a fully coherent legislative response (Mirmojidi, 2024). This creates difficulties not only for law enforcement but also for legitimate users, courts, businesses, investigators, exchanges, financial institutions, and regulatory authorities attempting to determine which legal rules govern a particular transaction.

The problem becomes more serious when existing criminal offenses are applied to conduct involving cryptocurrency. Traditional criminal law may already prohibit fraud, unauthorized access, theft-like appropriation, money laundering, financing of criminal activity, unlawful acquisition of property, and various forms of cybercrime. The use of cryptocurrency does not necessarily require the creation of a new offense whenever one of these conventional crimes is committed through digital means. A fraudulent seller who induces a victim to transfer cryptocurrency, for example, may engage in conduct that is functionally comparable to fraud involving conventional money. Similarly, obtaining control of another person's wallet through unauthorized access may fall within existing cybercrime rules. The legislative difficulty arises where the technological structure of cryptocurrency creates conduct that does not correspond neatly to existing statutory concepts or where the absence of regulation makes harmful behavior difficult to classify. Criminal policy must therefore distinguish between technological neutrality, under which existing offenses remain applicable regardless of the medium used, and genuine regulatory gaps, in which the elements of existing offenses fail to capture the specific harm produced by cryptocurrency-based conduct. Contemporary analysis of cryptocurrency-related cybercrime supports this distinction because digital currencies often facilitate or modify existing criminal practices rather than creating entirely new categories of criminality (Haghi et al., 2025).

Financial crime provides one of the clearest illustrations of the regulatory problem. Cryptocurrencies may be used to transfer proceeds from fraud, extortion, cyberattacks, illegal commerce, and other predicate offenses. They may also function as intermediate assets through which funds are moved before conversion into conventional currency. The risk does not arise merely from the existence of cryptocurrency but from the possibility of combining decentralized transfers, jurisdictional fragmentation, poorly supervised service providers, and techniques designed to reduce traceability. International analysis has therefore increasingly treated virtual assets and virtual-asset service providers as components of the broader anti-money-laundering and counter-financial-crime framework (Financial Action Task, 2022). Research concerning the laundering risks of disruptive financial technologies similarly demonstrates that legal systems must address both current methods of misuse and the possibility that offenders will adapt quickly when new regulatory controls are introduced (Akartuna et al., 2022). The legislative problem is consequently dynamic. Rules designed around a particular cryptocurrency, exchange model, or transaction technology can rapidly become obsolete.

The international regulatory trend has moved away from the assumption that cryptocurrency can be effectively controlled through simple prohibition. Comparative scholarship shows considerable diversity, but an increasing number of legal systems have attempted to regulate entry points between decentralized networks and the formal economy by licensing service providers, requiring customer identification, preserving transaction records, imposing suspicious-transaction reporting duties, and authorizing the freezing or confiscation of criminal assets (Houben & Snyers, 2020). Other jurisdictions have experimented with broader classifications that distinguish payment tokens, utility tokens, securities-like assets, and other forms of digital assets according to their economic function (Huang et al., 2020). These experiences do not provide a model that can be transplanted mechanically into Iranian law, but they indicate that effective regulation normally depends on functional definitions, institutional responsibility, risk-sensitive obligations, and enforceable mechanisms of accountability. The issue is therefore not simply whether cryptocurrency should be permitted or prohibited. The more important question is how the law should identify those activities that require authorization, those risks that require preventive regulation, and those forms of misconduct that justify criminal sanction.

The present article seeks to identify the principal legal gaps affecting cryptocurrency payments in Iran, analyze the offenses that arise from or are facilitated by those gaps, and formulate a legislative framework for appropriate criminalization and regulation. The central premise is that cryptocurrency itself should not constitute the object of indiscriminate criminalization. Criminal policy should instead concentrate on identifiable harmful conduct, deliberate evasion of regulatory safeguards, unauthorized control over digital assets, fraudulent payment practices, laundering and concealment mechanisms, and the knowing facilitation of serious criminal activity. The research therefore separates the regulatory status of cryptocurrency payments from the criminal status of particular conduct performed through those payments. It also distinguishes criminalization from administrative regulation. Licensing violations, technical compliance failures, and failures of record keeping should not automatically receive the same criminal response as intentional fraud, laundering, theft, or participation in organized criminal finance. The objective is to establish a coherent model in which private economic activity remains legally predictable while harmful conduct can be effectively detected, attributed, investigated, and punished.

Methodologically, the study adopts a descriptive-analytical legal approach. It examines the characteristics of cryptocurrency payments, the fragmented position of crypto-assets within Iranian law, relevant criminal risks, and the relationship between regulatory gaps and difficulties of prosecution. Comparative and international materials are employed only insofar as they illuminate possible legislative solutions for the Iranian context. The article does not attempt to reproduce the broader international survey commonly found in studies of cryptocurrency regulation; rather, it uses international standards to identify regulatory functions that domestic legislation should perform. Existing research on Iranian and comparative criminal policy demonstrates the importance of combining substantive criminal law with regulation of exchanges, customer identification, technical tracing mechanisms, and institutional cooperation (Faghih et al., 2025). The article accordingly proceeds from the view that effective criminalization cannot operate independently of regulatory infrastructure. A criminal prohibition that cannot identify relevant actors, establish ownership or control, obtain records, preserve digital evidence, or freeze assets may possess formal validity while remaining practically ineffective. The central legislative challenge is therefore to design a regime in which definitions, licensing, preventive duties, criminal offenses, procedural powers, evidentiary standards, asset-recovery measures, and institutional competence function as an integrated system.

2. Cryptocurrency Payments and Their Position in the Iranian Legal System

The legal analysis of cryptocurrency payments must begin by separating the technological concept of cryptocurrency from the legal function performed in a particular transaction. A crypto-asset may be purchased as a speculative investment, retained as a store of value, transferred as collateral, used to obtain another digital asset, exchanged for sovereign currency, or delivered as consideration for goods and services. The same technological asset may therefore perform different legal and economic functions at different moments. This functional variability explains why attempts to classify all cryptocurrencies exclusively as “currency,” “commodity,” “security,” or “property” are often inadequate. Jabotinsky describes the regulatory difficulty as one arising from the location of cryptocurrencies between the conceptual categories of currency and financial product (Jabotinsky, 2020). Giudici, Milne, and Vinogradov likewise emphasize that crypto-assets constitute a heterogeneous market whose economic characteristics cannot be reduced to a single model (Giudici et al., 2020). For criminal and payment law, this distinction is important because the legal consequence of a transaction should depend on what the asset is doing within the transaction rather than on an abstract classification detached from its use. Where cryptocurrency is tendered and accepted in satisfaction of a commercial obligation, it performs a payment function even if the state does not recognize it as legal tender.

A cryptocurrency payment may therefore be understood as a transfer of control over a crypto-asset that is intended by the parties to satisfy, wholly or partially, an economic obligation. Such a definition avoids the unnecessary conclusion that cryptocurrency must first be legally recognized as sovereign money before payment-related rules can apply. It also permits legal analysis to focus on the transfer of economic value. The regulatory literature increasingly recognizes that crypto-assets can perform money-like functions without acquiring the complete legal status of money (Chohan, 2021). This approach is particularly important in private transactions because parties may voluntarily assign exchange value to a digital asset even where public law restricts its use within the official monetary system. The law must consequently distinguish legal tender status from economic functionality. Failure to make this distinction creates a conceptual gap: a transaction may clearly transfer economically valuable assets and expose parties to substantial loss, yet the applicable rules may remain uncertain because the asset does not fit traditional monetary categories.

The technological mechanics of cryptocurrency payments further differentiate them from ordinary bank transfers. In a conventional payment system, account ownership, institutional records, customer identification, reversal procedures, centralized compliance controls, and judicial access to financial records are generally embedded within the architecture of the payment system. In a blockchain transaction, control of a cryptographic key may effectively determine the capacity to transfer an asset. A transaction may be technically irreversible once confirmed, even if it resulted from fraud, coercion, unauthorized access, or mistake. The legal owner and the technical controller may therefore be different persons. This separation between legal entitlement and technological control requires criminal law to articulate how ownership, possession, appropriation, transfer, and restitution operate in relation to digital assets. Europol has emphasized that cryptocurrency investigations require the ability to link blockchain activity to persons, services, devices, accounts, and off-chain information (Europol, 2021). Chainalysis likewise demonstrates that the practical investigation of crypto-related crime frequently depends on tracing transactional patterns and connecting them to identifiable intermediaries or conversion points (Chainalysis, 2022). The law must consequently recognize that blockchain records are important evidence but are not, by themselves, a complete legal determination of ownership or criminal responsibility.

Iran's regulatory position has developed incrementally rather than through a unified cryptocurrency statute. The resulting framework reflects different governmental concerns at different stages, including monetary sovereignty, capital movement, energy consumption associated with mining, unauthorized economic activity, cybercrime, money laundering, and financial security. Research on Iranian criminal policy identifies this fragmented development as a central weakness because administrative, financial, and criminal measures have not always been organized around a consistent legal definition of cryptocurrency or a unified regulatory objective (Ghaemi Asl et al., 2024). Mirmojidi similarly points to a divergence between legislative and judicial responses in the Iranian treatment of digital assets (Mirmojidi, 2024). Fragmentation becomes especially problematic in the field of payments because the legal consequences of transferring cryptocurrency can vary depending on whether the issue is viewed through monetary regulation, contract law, criminal law, cybercrime law, anti-money-laundering regulation, or rules governing unauthorized economic activities.

A comprehensive legal system does not necessarily need to classify cryptocurrency identically for all purposes. Functional differentiation may in fact produce greater legal precision. An asset could be treated as property for purposes of ownership and restitution, as a financial asset for disclosure or supervisory purposes, and as a payment instrument when used to discharge an obligation. The difficulty arises where legislation provides no clear rule for determining which classification applies to which context. Ibrahim argues that the rapid expansion of cryptocurrency activity has made regulatory clarification unavoidable because legal ambiguity increases risks both for users and for supervisory authorities (Ibrahim, 2024). Comparative regulatory studies also show that definitional precision is essential because the scope of licensing, reporting, consumer protection, and criminal enforcement depends on the terms used to identify regulated assets and services (Houben & Snyers, 2020). Iranian legislation would therefore benefit from a general statutory concept of “crypto-asset” or “virtual asset,” supplemented by functional categories that identify payment activities, exchange activities, custodial services, token issuance, and other relevant services.

The position of cryptocurrency exchanges is particularly important because exchanges constitute a major interface between decentralized assets and identifiable economic actors. Where users purchase cryptocurrency with fiat money, convert crypto-assets into sovereign currency, or transfer assets through custodial accounts, exchanges may possess information that is unavailable on the blockchain itself. Regulating exchanges therefore serves multiple objectives simultaneously: consumer protection, market integrity, customer identification, anti-money-laundering compliance, tax transparency, and criminal investigation. FATF standards place particular emphasis on virtual-asset service providers because these entities can perform functions analogous to financial intermediaries and can therefore become crucial regulatory gateways (Financial Action Task, 2022). Fletcher, Larkin, and Corbet argue that the risks associated with Bitcoin do not justify abandoning the technology but support regulatory intervention aimed at reducing laundering and financing risks (Fletcher et al., 2021). In the Iranian context, uncertainty concerning the legal status, licensing requirements, and compliance duties of crypto-asset service providers weakens the regulatory chain. If an exchange handles economically substantial transactions but its legal obligations are not equivalent to the risks associated with those functions, law enforcement may face difficulty identifying users, preserving records, freezing assets, and obtaining reliable transaction histories.

Non-custodial activity presents a different problem. A legal framework focused exclusively on centralized exchanges cannot fully regulate peer-to-peer transfers, self-hosted wallets, decentralized exchanges, or transactions in which no domestic intermediary participates. This does not mean that every person maintaining a private wallet should be treated as a regulated financial institution. Such an approach would be disproportionate and practically unenforceable. Regulation should instead identify points at which professional or commercial actors provide services to others. The distinction between personal use and regulated service provision is crucial because criminal and administrative obligations should attach to conduct that creates identifiable public risks. International standards typically concentrate on persons engaged as businesses in exchange, transfer, custody, or similar activities involving virtual assets (Financial Action Task, 2022). The Iranian framework should adopt comparable functional distinctions while adapting them to domestic institutional structures.

The payment dimension also requires protection of users against fraud and operational misconduct. Cryptocurrency transactions may expose users to fake payment platforms, fraudulent token representations, false confirmations, compromised wallets, impersonation, phishing, deceptive investment schemes, and unauthorized transfers. Bakhshi identifies unauthorized transactions and cybercrime as major components of the criminal-policy problem surrounding cryptocurrencies in Iran (Bakhshi, 2025). Haghi and colleagues similarly describe digital currencies as instruments capable of facilitating cybercrime when offenders exploit technological complexity and user unfamiliarity (Haghi et al., 2025). The legal response should not assume that every such event requires a new crypto-specific offense. In many cases the substance of the conduct remains fraud, unlawful access, deception, or unauthorized appropriation. However, legislation must make clear that digital assets constitute legally protectable economic value and that unlawful acquisition or transfer can satisfy the property-related elements of relevant offenses. Otherwise, defendants may exploit conceptual ambiguity concerning whether a crypto-asset qualifies as property, money, data, or another legally protected interest.

The legal status of transactions is also significant for victims seeking restitution. A criminal justice system that recognizes an offense but lacks effective procedures for securing and returning digital assets may fail to provide meaningful protection. Crypto-assets may move rapidly across wallets, exchanges, chains, and jurisdictions. Their value may also fluctuate significantly while proceedings are pending. Authorities therefore require rules governing seizure, preservation, custody, conversion where necessary, and eventual restitution or confiscation. The development of regulatory responses in other jurisdictions demonstrates that digital assets require technical procedures different from those applied to conventional bank balances (Huang et al., 2020). Investigators may need to secure private keys or transfer assets to government-controlled wallets, while courts require methods for proving control, ownership, transaction history, and valuation. The absence of detailed procedural rules may produce inconsistent practices and increase the risk of asset loss.

Iran's position should consequently be understood as one of partial regulation rather than complete legal absence. Existing laws can address important forms of misconduct, particularly where cryptocurrency functions merely as the medium through which an already criminalized act is performed. Anti-money-laundering rules, cybercrime provisions, fraud-related offenses, and general principles governing criminal proceeds may all remain relevant. Faghih, Barzegarzadeh, and Safaei conclude that the central weakness lies in the lack of comprehensive and coordinated regulation rather than the absolute absence of any legal mechanism (Faghih et al., 2025). Similarly, Namamian's analysis of Iranian and comparative approaches emphasizes inconsistency and lack of clarity in the domestic regulation of cryptocurrencies (Namamian, 2024). This distinction matters because legislative reform should not unnecessarily duplicate existing criminal offenses. It should instead identify where traditional rules can be explicitly extended to digital assets, where procedural adaptation is needed, and where genuinely new offenses or duties are justified.

Another significant issue concerns institutional competence. Cryptocurrency payments simultaneously engage monetary policy, financial supervision, cybersecurity, commerce, taxation, criminal justice, data regulation, consumer protection, and international cooperation. Fragmentation among competent authorities can therefore create overlapping mandates or regulatory gaps. A transaction may attract attention from one authority because it involves an unauthorized exchange, another because it involves suspected laundering, and another because it involves cyber intrusion. Without clear rules for information exchange and institutional coordination, each authority may possess only part of the evidentiary picture. Faghih and colleagues identify institutional coordination as an important difference between more developed regulatory models and the Iranian system (Faghih et al., 2025). The regulatory design should therefore assign primary supervisory responsibility for service providers while requiring structured cooperation with law-enforcement, judicial, cybersecurity, and financial-intelligence bodies.

The desired legal position is neither unrestricted recognition of cryptocurrency as equivalent to sovereign money nor categorical denial of its economic reality. A coherent framework should recognize crypto-assets as forms of transferable digital economic value and regulate payment-related conduct according to function and risk. Such a framework would provide legal certainty regarding ownership, contractual transfer, intermediary obligations, professional service provision, consumer risks, suspicious transactions, criminal proceeds, and asset recovery. The recognition of economic value would not require the state to surrender control over legal tender or monetary policy. It would instead ensure that transactions already occurring in practice are brought within a predictable legal structure. This distinction is especially important because legal ambiguity does not eliminate cryptocurrency activity; it may instead relocate that activity to less visible channels. Effective law should therefore make legitimate conduct identifiable and regulated while increasing the legal and operational costs of criminal misuse.

3. Legal Gaps in Cryptocurrency Payments and Crimes Arising from Them

The most significant legal gap in cryptocurrency payments is the absence of a comprehensive and internally consistent statutory definition of the object and activities being regulated. Criminal liability depends on legality, certainty, and foreseeability. Individuals must be able to determine in advance what conduct is prohibited, and courts must be able to identify the elements of an offense without relying on expansive analogy. Where cryptocurrency is not clearly classified as property, transferable economic value, a payment asset, or another legally protected object, uncertainty may arise in cases involving appropriation, deception, loss, confiscation, and restitution. Jabotinsky's analysis of cryptocurrency regulation demonstrates how classification problems can affect the choice of applicable legal regime (Jabotinsky, 2020). The same difficulty appears in Iranian criminal policy, where studies have identified uncertainty concerning the legal nature of crypto-assets and the consequences of that uncertainty for criminal enforcement (Mirmojidi, 2024). The first legislative gap is therefore conceptual. Without stable definitions, subsequent rules concerning payment, licensing, custody, seizure, and criminal misuse remain vulnerable to inconsistent interpretation.

The second gap concerns the distinction between lawful personal transactions and professional payment-related services. Cryptocurrency activity exists on a spectrum ranging from occasional transfers between private users to commercial exchange platforms processing transactions for large numbers of customers. Regulatory obligations should increase with the scale, professional character, custody function, and risk of the service provided. Where the law does not clearly define which services require authorization, market participants may operate in a grey zone in which users assume a degree of legal protection that does not actually exist. Bakhshi's examination of Iranian criminal policy toward cryptocurrency-related cybercrime and unauthorized transactions emphasizes the consequences of regulatory incompleteness for enforcement and prevention (Bakhshi, 2025). A similar issue has been observed internationally, where regulatory responses increasingly focus on service providers rather than attempting to prohibit decentralized technology itself (Houben & Snyers, 2020). The absence of a comprehensive licensing model can facilitate unregulated exchange services, informal brokerage, custody of customer assets without adequate safeguards, and payment intermediation without minimum compliance requirements.

Such regulatory gaps create conditions favorable to fraud. Cryptocurrency-related fraud may take conventional forms, such as false representation, deceptive inducement, and misappropriation, but the technological setting can increase both reach and complexity. A fraudulent operator may establish an apparently legitimate exchange or payment service, obtain customer funds, falsely represent that assets are being purchased or held, and subsequently disappear. Other schemes may involve fabricated tokens, misleading investment returns, false wallet interfaces, phishing pages, or manipulated transaction information. Chainalysis has documented the continuing importance of scams and other illicit activities within crypto markets (Chainalysis, 2022). Haghi and colleagues also identify fraud as one of the cybercriminal activities facilitated by digital currencies (Haghi et al., 2025). The principal legal issue is not whether fraud should be criminalized—it already is—but whether the legal system clearly recognizes cryptocurrency as an object capable of being obtained, transferred, misappropriated, or lost through fraudulent conduct and whether investigators possess the tools required to trace and secure the relevant assets.

Unauthorized transfer of digital assets raises an analogous problem. A person may obtain another user's private key through malware, phishing, unauthorized access, coercion, insider misconduct, or exploitation of a service provider. Once the key is obtained, the offender may transfer assets to another wallet. Traditional property offenses were developed around tangible objects, while cybercrime legislation often focuses on unauthorized access to data or systems. Cryptocurrency theft may involve both dimensions: the unauthorized access is informational, but the ultimate harm is economic deprivation through transfer of a valuable digital asset. Boyko, Dotscenko, and Dolia identify unauthorized appropriation and movement of cryptocurrency as part of the broader pattern of crypto-enabled financial crime (Boyko et al., 2022). The law should therefore avoid a gap in which unauthorized access is punishable but the transfer of the digital asset is not clearly recognized as a property-related harm. Explicit statutory recognition of crypto-assets as property or transferable economic value for purposes of criminal law would reduce this ambiguity.

Payment fraud can also arise without unauthorized access. A debtor may falsely claim to have made a cryptocurrency payment by providing manipulated screenshots, fabricated transaction identifiers, or information relating to a transaction that was never confirmed or was directed to another wallet. A merchant may accept payment and subsequently deny receipt despite verifiable blockchain evidence. The technical characteristics of blockchain transactions may assist proof in some circumstances, but courts must understand confirmation, address control, chain reorganizations, custody structures, and the distinction between a transaction appearing on-chain and the legal identity of the parties. Europol's analysis of cryptocurrency tracing demonstrates that blockchain information can support criminal investigation while requiring specialist interpretation and linkage to external data (Europol, 2021). A legal framework that does not specify the evidentiary status of blockchain records may produce unnecessary uncertainty concerning authentication, expert testimony, and proof of control.

Money laundering represents one of the most significant criminal risks associated with regulatory gaps in cryptocurrency payments. Crypto-assets may be used to receive criminal proceeds, transfer them through multiple addresses, exchange them into other assets, move them across borders, or convert them into conventional currency. Azadbakht's analysis of digital currencies and money laundering emphasizes the challenges created by cross-border transactions and gaps between national regulatory systems (Azadbakht, 2024). Kapsis likewise identifies money laundering as a major field in which the characteristics of crypto-assets interact with organized financial crime (Kapsis, 2023). The problem should nevertheless be stated carefully. Public blockchain transactions may be traceable, and cryptocurrencies do not automatically provide complete anonymity. The laundering risk often arises from the combination of pseudonymous addresses, unregulated services, privacy-enhancing techniques, cross-jurisdictional transfers, and conversion through institutions that do not adequately identify customers. The legal response should therefore focus on the points at which identity, custody, exchange, and conversion can reasonably be regulated.

The absence of effective customer identification is a central vulnerability. Traditional financial institutions are expected to identify customers, maintain records, understand certain aspects of customer activity, and report suspicious transactions. Virtual-asset service providers performing comparable economic functions can become attractive alternatives if they are not subject to comparable risk-based duties. FATF standards therefore extend anti-money-laundering expectations to relevant virtual-asset service providers (Financial Action Task, 2022). Rashidi's analysis also emphasizes customer identification and stronger supervisory mechanisms as important components of an effective response to cryptocurrency-related laundering and financing risks (Rashidi, 2024). In Iran, a fragmented regulatory environment can result in inconsistent identification requirements across exchanges and service providers. This weakens the evidentiary chain because investigators may identify a blockchain address connected to suspected criminal funds but remain unable to link it to a verified person.

Another gap concerns beneficial ownership and control. The individual opening an account or interacting with an exchange may act on behalf of another person. Criminal organizations may use intermediaries, nominees, money mules, or compromised accounts to distance themselves from transactions. Esoimeme's study of money mules demonstrates how individuals may be recruited to move illicit funds, sometimes without fully understanding their role in the laundering process (Esoimeme, 2020). Cryptocurrency can add another layer to such arrangements because assets can be transferred rapidly between multiple addresses before reaching a centralized exchange. Regulation should therefore distinguish basic customer identification from the broader obligation to identify the person who ultimately owns or controls assets in higher-risk situations. Failure to address beneficial control leaves an important weakness even where formal identification procedures exist.

The cross-border nature of cryptocurrency payments creates jurisdictional difficulties. A user in Iran may send assets to an address controlled abroad through software operated by a decentralized network, using an exchange incorporated in another jurisdiction and infrastructure distributed across multiple countries. Traditional concepts of territorial jurisdiction may therefore intersect with nationality, effects, location of victims, location of service providers, and location of criminal proceeds. Ghavami and Mahmoudi emphasize that the transnational nature of digital-currency crimes requires stronger international legal cooperation (Ghavami & Mahmoudi, 2024). Ghavampour Sarshkeh and Mahmoudi similarly address the importance of international instruments in responding to business-related crimes involving digital currencies (Ghavampour Sarshkeh & Mahmoudi, 2023). Domestic legislation should accordingly articulate jurisdictional connecting factors for crypto-related offenses rather than leaving courts to resolve novel transnational configurations entirely through general rules.

Jurisdictional fragmentation is particularly problematic for evidence and asset recovery. Blockchain transactions may be visible globally, while information identifying the users behind those transactions may be held by an exchange in another state. Obtaining that information can require mutual legal assistance or other forms of cooperation. During the resulting delay, assets may be transferred repeatedly. Criminal policy must therefore combine formal international cooperation with mechanisms for rapid preservation of information and provisional restriction of assets. Koshulovich emphasizes that law-enforcement intelligence concerning cryptocurrency-related criminal networks depends on effective collection and interpretation of data across technical and jurisdictional boundaries (Koshulovich, 2023). The legal framework should therefore authorize expedited preservation requests and establish procedures for cooperation with foreign service providers where permitted by applicable law.

The regulation of privacy-enhancing technologies presents another difficult issue. Privacy is a legitimate interest, and the use of privacy-preserving technology should not in itself be treated as evidence of criminal intent. Yet tools designed to break transaction traceability may also be used to conceal criminal proceeds. The legislative challenge is to avoid criminalizing technology merely because it can be misused while addressing deliberate services designed or operated for unlawful concealment. Akartuna and colleagues show that emerging technologies can create new criminal opportunities but also caution against static approaches that fail to distinguish legitimate innovation from harmful applications (Akartuna et al., 2022). A proportionate approach should therefore focus on knowledge, intention, professional facilitation, and demonstrable risk rather than on the mere possession or use of a privacy-related tool.

Terrorist financing is one of several serious criminal purposes for which cryptocurrency can potentially be used, although its role should not be exaggerated. Dyntu and Dykyj analyze the characteristics that may make cryptocurrency attractive in terrorist-financing contexts, particularly speed and cross-border transferability (Dyntu & Dykyj, 2021). Kapsis likewise treats terrorism financing as one of the principal financial-crime risks examined in the crypto-asset literature (Kapsis, 2023). Iranian research has focused extensively on this subject, with Namamian emphasizing the difficulties of applying existing counter-financing measures to cryptocurrency transactions (Namamian, 2024). For the purposes of the present article, however, terrorist financing is relevant as an example of a broader legislative problem: the law must ensure that prohibitions governing the provision, collection, transfer, or concealment of assets for criminal purposes apply irrespective of whether the asset takes conventional or cryptographic form. The technology should not create a loophole in the material scope of an existing financing offense.

The same principle applies to other illegal markets and cybercrime. Cryptocurrency may be demanded as payment in ransomware attacks, used in illicit online commerce, or transferred as proceeds of hacking, extortion, and fraud. Europol has described the role of cryptocurrencies in cybercrime ecosystems while also emphasizing the increasing capacity of investigators to trace transactions (Europol, 2021). Noronha Rodrigues, Bhattacharya, and Cabete situate digital cybercrime and illicit financial movements within a broader set of threats affecting contemporary economic systems (Noronha Rodrigues et al., 2025). Effective criminal policy should therefore ensure that payment in cryptocurrency does not alter the legal characterization of the underlying offense. At the same time, specialized aggravating circumstances may be justified where sophisticated concealment techniques, organized criminal structures, or deliberate interference with tracing significantly increase the seriousness of the conduct.

A further legal gap concerns the criminal liability of service providers and legal persons. An exchange may be an innocent intermediary used by offenders, a negligent institution with inadequate controls, or an active participant deliberately facilitating illegal transactions. These situations must not be treated identically. Criminal liability should ordinarily require a level of fault appropriate to the offense, while regulatory sanctions may address lesser compliance failures. Koster's analysis of European anti-money-laundering implementation shows that effectiveness depends not merely on formal obligations but on institutional capacity and meaningful enforcement (Koster, 2020). Where Iranian law fails to distinguish administrative noncompliance, grossly deficient supervision, knowing facilitation, and intentional participation, enforcement can become either excessively punitive or ineffective. Clear attribution rules are therefore required for managers, compliance officers, employees, and the legal person itself.

Finally, a major gap lies in the absence of detailed digital-asset seizure and confiscation procedures. Criminal law may authorize confiscation of proceeds generally, yet crypto-assets require specific technical measures if those powers are to be effective. A wallet cannot be secured in the same manner as physical cash, and an order directed at a decentralized blockchain cannot itself prevent the person controlling a private key from moving assets. Authorities may need to obtain credentials, compel regulated custodians to restrict withdrawals, or transfer assets into secure government-controlled storage. Alrasheed emphasizes the potential role of advanced technologies in cryptocurrency tracking and financial-crime prevention (Alrasheed, 2025). The legislative gap is therefore procedural as well as substantive. Without rules governing identification, freezing, custody, valuation, preservation, confiscation, and restitution, the state may successfully prove an offense yet fail to recover the proceeds or compensate victims.

These gaps demonstrate that cryptocurrency crime cannot be addressed through the creation of a single new offense. The problem is systemic. It involves legal classification, licensing, identification, evidentiary standards, jurisdiction, intermediary obligations, cybercrime, financial crime, asset recovery, and institutional cooperation. A sound legislative response must distinguish conduct already punishable under existing criminal law from behavior that genuinely requires new criminalization. The principle of legality requires precision, while the principle of necessity requires restraint. Criminal legislation should intervene where identifiable harms cannot be adequately addressed through existing offenses or administrative regulation. The next stage is therefore not to criminalize cryptocurrency payments generally, but to construct a coherent legislative framework that makes lawful payment activity transparent, regulates professional intermediaries, closes specific loopholes, and creates targeted offenses for conduct that deliberately defeats essential safeguards.

4. Proposed Criminalization and Legislative Framework for Cryptocurrency Payments

A coherent legislative response should begin with the principle that criminalization is only one element of cryptocurrency governance. The objective of legislation should be to establish a structured environment in which lawful use is distinguishable from prohibited conduct and in which regulators and investigators can obtain the information necessary to respond to genuine criminal risks. Overcriminalization would be counterproductive because it could drive transactions away from regulated domestic platforms and toward informal peer-to-peer markets or foreign services beyond effective national supervision. Ghaemi Asl and colleagues argue for an optimal criminal-policy approach capable of balancing regulatory control with the realities of virtual-currency use (Ghaemi Asl et al., 2024). Comparative analysis similarly suggests that regulatory systems are generally more effective when they establish legal channels for compliant activity while concentrating criminal sanctions on deception, laundering, unauthorized professional activity, deliberate evasion, and other harmful conduct (Faghih et al., 2025). Criminalization should therefore follow the principles of legality, necessity, proportionality, culpability, technological neutrality, and ultima ratio.

The first legislative requirement is the enactment of clear definitions. Iranian law should adopt a broad definition of a crypto-asset or virtual asset as digitally represented value that can be transferred or stored electronically through distributed or comparable technological systems and that may be used for investment, exchange, payment, or other economic purposes. The definition should be technology-neutral so that it does not become obsolete when specific blockchain protocols change. Cryptocurrency intended or used as a medium of exchange can then be treated as a functional subset for payment-related provisions. Separate definitions should cover custodial wallets, non-custodial wallets, crypto-asset exchanges, transfer services, brokerage, custody, conversion services, and other virtual-asset service providers. FATF's functional approach to virtual assets and service providers provides a useful reference because it focuses on economic activities rather than product names (Financial Action Task, 2022). Such definitions would also prevent offenders from escaping regulation merely by describing a service using terminology not contemplated by older legislation.

The legislation should explicitly recognize crypto-assets as legally protectable economic value for purposes of criminal law, civil restitution, seizure, and confiscation. This recognition need not grant cryptocurrency the status of legal tender. It should simply make clear that digital assets capable of economic transfer can constitute property or assets for purposes of offenses involving deception, unlawful appropriation, criminal proceeds, and damage. Jabotinsky's analysis demonstrates that regulatory recognition can be separated from the question of whether a crypto-asset is formally treated as currency (Jabotinsky, 2020). This approach would reduce uncertainty in cases involving stolen private keys, unauthorized transfers, fraudulent acquisition, or concealment of digital wealth. It would also strengthen victim remedies by removing unnecessary disputes over whether the object of the offense falls within protected property concepts.

A second major component should be a comprehensive licensing regime for professional cryptocurrency service providers. Persons who professionally exchange crypto-assets for sovereign currency, exchange one crypto-asset for another, transfer digital assets on behalf of customers, hold customers' private keys, operate custodial payment services, or otherwise exercise control over customer assets should be required to obtain authorization. Licensing requirements should be proportionate to the activity performed and the level of risk created. Ibrahim emphasizes the necessity of regulatory frameworks capable of bringing cryptocurrency activity within identifiable legal boundaries rather than leaving it in an uncontrolled environment (Ibrahim, 2024). A licensing regime would enable authorities to impose minimum governance requirements, cybersecurity obligations, segregation of customer assets, complaint procedures, record keeping, and financial-crime controls. It would also create an identifiable population of service providers subject to inspection and enforcement.

The law should distinguish unlicensed commercial activity from private use. A person who transfers cryptocurrency from a personal wallet to another individual should not commit an offense merely because the payment is decentralized. Criminalizing ordinary ownership or transfer would be disproportionate and practically impossible to enforce. By contrast, a person who operates a professional exchange, custody platform, or payment business without required authorization may reasonably be subject to sanctions. The primary response to minor or technical licensing violations should normally be administrative, including warnings, corrective orders, suspension, financial penalties, or withdrawal of authorization. Criminal liability should be reserved for deliberate and serious unauthorized operation, particularly where the person handles customer assets, conceals the activity from regulators, continues after prohibition, or exposes the public to substantial financial risk. This graduated approach reflects the distinction between regulatory noncompliance and criminal wrongdoing.

Customer identification and record keeping should form the third major pillar. Licensed service providers should be required to identify customers to a level proportionate to the risk and nature of the transaction. FATF standards make customer due diligence and record preservation central components of the virtual-asset regulatory framework (Financial Action Task, 2022). Rashidi likewise emphasizes identification and transaction monitoring as necessary mechanisms for reducing laundering risks in virtual currencies (Rashidi, 2024). Iranian legislation should require regulated entities to verify identity, preserve account and transaction information, identify beneficial ownership in appropriate circumstances, and maintain records for a defined statutory period. The purpose should not be indiscriminate surveillance of every user but the creation of a lawful evidentiary trail for professional financial services.

The reporting of suspicious transactions should be integrated into this framework. Cryptocurrency service providers are often better positioned than law-enforcement authorities to observe unusual patterns involving repeated deposits, rapid conversion, movement through multiple accounts, interaction with known high-risk addresses, or attempts to circumvent verification thresholds. Service providers should therefore be required to implement risk-based monitoring and report legally defined suspicious transactions to the competent financial-intelligence authority. Koster's analysis of anti-money-laundering frameworks demonstrates that reporting systems are effective only when regulated entities understand their obligations and authorities possess sufficient capacity to analyze the information received (Koster, 2020). The Iranian framework should consequently avoid a purely formal compliance model in which large volumes of low-quality reports are produced without effective analysis. Reporting duties should be supported by guidance, typologies, feedback, and technical standards.

The deliberate evasion of identification requirements should be addressed carefully. Ordinary use of a self-hosted wallet should not be criminalized. However, knowingly providing false identity information to a regulated service, using forged documentation, deliberately structuring transactions to defeat statutory identification thresholds, or commercially providing services designed to circumvent mandatory customer due diligence may justify specific sanctions. The mental element is crucial. Criminalization should target intentional evasion rather than accidental noncompliance. This is consistent with the broader principle that criminal liability should attach to culpable conduct rather than to technological choices alone.

The criminal law should also expressly cover unauthorized transfer and appropriation of crypto-assets. Existing cybercrime offenses may address the method of gaining access, but legislation should clarify that intentionally transferring another person's crypto-assets without authorization, with the purpose of depriving the lawful controller or obtaining unlawful benefit, constitutes punishable appropriation. Where the conduct is already fully covered by theft, fraud, breach of trust, or computer-related offenses, the preferable legislative technique may be an interpretive provision stating that digital assets fall within the object of those offenses rather than creating multiple overlapping crimes. Bakhshi's analysis of cybercrimes involving cryptocurrencies illustrates the importance of aligning general criminal offenses with the distinctive characteristics of digital assets (Bakhshi, 2025). This approach would preserve coherence while preventing defendants from relying on the intangible character of cryptocurrency as a technical defense.

Payment-specific fraud should likewise be explicitly encompassed by existing fraud legislation. False representation that cryptocurrency has been transferred, manipulation of digital payment interfaces, fabrication of transaction records, deliberate alteration of wallet addresses, and deceptive substitution of payment destinations should be treated as fraud where the ordinary elements of deception, causation, unlawful benefit, and victim loss are established. Haghi and colleagues show that digital currencies can facilitate numerous forms of cyber-enabled fraud (Haghi et al., 2025). The technological mechanism should therefore not alter the fundamental criminal-law analysis. However, sentencing rules may treat large-scale automated victimization, organized activity, abuse of professional position, or sophisticated concealment as aggravating circumstances.

Money laundering legislation should expressly state that crypto-assets fall within the concept of property, funds, proceeds, or assets covered by laundering offenses. This clarification would eliminate arguments that anti-money-laundering rules apply only to conventional money or bank-based assets. Fletcher and colleagues support regulatory treatment of Bitcoin within anti-money-laundering frameworks because the relevant concern is the concealment and movement of value rather than its technological form (Fletcher et al., 2021). Azadbakht similarly emphasizes that digital currencies can function as vehicles for laundering where legal systems fail to integrate them into existing controls (Azadbakht, 2024). Criminal liability should continue to require the mental element specified by laundering law, such as knowledge or legally defined forms of awareness concerning the criminal origin of assets. Mere receipt of cryptocurrency should never create a presumption of laundering.

A parallel clarification is required for criminal financing offenses. Where Iranian law prohibits supplying, collecting, transferring, or making assets available for specified criminal purposes, the statutory concept of assets should expressly include crypto-assets. Malakoutikhah's analysis of criminalization in Iranian terrorist-financing law demonstrates the importance of aligning the material scope of financing offenses with contemporary forms of economic value (Malakoutikhah, 2020). Namamian also identifies the expansion of cryptocurrency as a reason to reassess existing financing controls (Namamian, 2024). The legal principle should be technology-neutral: if transferring conventional funds for a specified criminal purpose constitutes an offense, transferring cryptocurrency with the same intent should not escape liability merely because the asset is digital.

Corporate and managerial liability should be defined with similar precision. A regulated exchange should not become criminally responsible simply because a customer uses its services for an offense that the company could not reasonably detect. Such a rule would discourage legitimate service provision and produce excessive defensive compliance. Liability should depend on attribution standards such as intentional participation, knowing facilitation, deliberate concealment, or serious breaches of legally defined duties where the legislature determines that criminal punishment is justified. Administrative penalties can address ordinary deficiencies in compliance programs. More serious conduct, such as intentionally processing transactions for known criminal organizations or falsifying compliance records to conceal illegal activity, should attract criminal liability. Faghih and colleagues emphasize that effective crypto-related criminal policy requires both clear regulatory duties and meaningful enforcement (Faghih et al., 2025). The distinction between institutional failure and intentional criminal facilitation should therefore be embedded in the statute.

Investigative powers must also be modernized. Investigators should have express authority, subject to judicial safeguards, to obtain relevant records from licensed exchanges, preserve customer data, identify wallet information held by service providers, and use blockchain-analysis techniques. Alrasheed highlights the potential of artificial intelligence and technological tracking tools to improve detection of cryptocurrency-related financial crime (Alrasheed, 2025). Europol similarly illustrates the growing role of blockchain tracing in criminal investigations (Europol, 2021). These powers must remain subject to legality, necessity, proportionality, and judicial oversight. Technical capacity cannot substitute for procedural rights. The objective is to enable lawful investigation of identified criminal conduct rather than to authorize unrestricted monitoring of all blockchain users.

Digital evidence requires explicit procedural recognition. Blockchain transaction data, wallet records, exchange logs, device information, and cryptographic evidence should be admissible where authenticity, integrity, relevance, and chain of custody are established. Courts should have access to qualified expert assistance when technical interpretation is necessary. The law should recognize that a blockchain address alone does not prove legal identity; attribution ordinarily requires additional evidence connecting a person to the wallet or transaction. Koshulovich's discussion of intelligence challenges in cryptocurrency investigations reinforces the need to combine blockchain information with conventional investigative evidence (Koshulovich, 2023). A statutory evidentiary framework would reduce inconsistency and prevent both overreliance on technological evidence and unwarranted rejection of reliable digital records.

Freezing, seizure, confiscation, and restitution should receive dedicated legislative treatment. Regulated custodians should be legally obliged to comply with judicial freezing orders. Where investigators obtain lawful control of private keys associated with suspected criminal assets, procedures should authorize secure transfer to designated government wallets. Detailed rules should govern documentation, cybersecurity, access controls, valuation, preservation, conversion where legally justified, and final disposal. Asset management is particularly important because crypto-assets may fluctuate significantly in value. Legislation should determine when preservation in the original asset is appropriate and when conversion may be authorized to protect value or prevent technical loss. Chainalysis demonstrates that crypto-asset tracing increasingly enables authorities to identify and recover digital proceeds where appropriate investigative capacity exists (Chainalysis, 2022). Legal authority and technical capacity should therefore develop together.

Institutional architecture should be simplified. One regulator should have primary responsibility for licensing and supervision of cryptocurrency service providers, while formal mechanisms should connect that authority with the central bank, financial-intelligence structures, law enforcement, prosecutors, cybercrime units, and courts. Fragmented authority creates duplicated responsibilities and information gaps. Bakhshi identifies the absence of institutional coherence as a weakness in Iranian cryptocurrency criminal policy (Bakhshi, 2025). Faghih and colleagues similarly emphasize coordination as an important condition of regulatory effectiveness (Faghih et al., 2025). Legislation should therefore establish mandatory information-sharing channels, joint investigative procedures for major cases, and clearly allocated responsibilities.

The framework should also adopt a risk-based approach. Not all cryptocurrency activities create identical risks. Small-scale personal transactions differ significantly from institutional custody, high-volume exchange activity, privacy-enhancing commercial services, or cross-border payment businesses. FATF's model emphasizes risk-based regulation rather than uniform treatment of every transaction (Financial Action Task, 2022). Vucinic's analysis of FinTech and financial stability similarly demonstrates that financial innovation produces both benefits and differentiated risks requiring proportionate regulatory responses (Vucinic, 2020). Iranian law should therefore allow regulators to impose stronger controls on higher-risk activities while simplifying requirements for low-risk services.

International cooperation is indispensable because digital assets can move across borders without the physical movement of property. Domestic legislation should authorize legally appropriate exchange of information, preservation requests, mutual assistance, recognition of foreign freezing and confiscation measures where statutory conditions are met, and cooperation in identifying digital assets. Ghavami and Mahmoudi emphasize the importance of international instruments in responding to digital-currency crime (Ghavami & Mahmoudi, 2024). Financial crime regulation also increasingly depends on cooperation between public authorities and private service providers operating across jurisdictions (Financial Action Task, 2020). Iran's legislative framework should therefore ensure that competent domestic authorities possess a clear legal basis for requesting and providing assistance while preserving applicable procedural safeguards.

Consumer education and professional training should complement criminal law. Judges, prosecutors, investigators, financial-intelligence analysts, and regulators require specialized knowledge concerning blockchain architecture, wallet control, transaction tracing, custody, decentralized services, and digital evidence. Users also need clear information concerning irreversible transfers, phishing, fraudulent platforms, custody risks, and the legal status of service providers. Noronha Rodrigues and colleagues emphasize the evolving relationship between digital financial technologies and cybercrime risks (Noronha Rodrigues et al., 2025). Prevention through knowledge may reduce victimization more efficiently than punishment after loss has occurred. Regulatory agencies should therefore publish guidance, maintain registries of licensed providers, issue warnings concerning identified fraudulent schemes, and establish accessible channels for reporting crypto-related offenses.

The overall model should be one of regulated legality. Cryptocurrency payments should not be prohibited simply because they create enforcement challenges. Nor should technological innovation be allowed to operate outside the general principles of financial accountability and criminal responsibility. The law should recognize digital economic value, regulate professional intermediaries, establish customer-identification and record-keeping duties, clarify the application of fraud and property offenses, explicitly include crypto-assets within laundering and criminal-financing provisions, create proportionate sanctions for intentional regulatory evasion, modernize evidentiary and investigative procedures, establish digital-asset recovery mechanisms, and coordinate competent institutions. Such a framework would transform the current fragmented response into an integrated system in which criminalization is targeted at harmful and culpable conduct rather than at the technology itself.

5. Conclusion

Cryptocurrency payments represent a structural challenge for legal systems because they separate the transfer of economic value from many of the institutions through which payment law, financial supervision, and criminal enforcement have traditionally operated. Their significance does not arise from the proposition that cryptocurrencies are inherently criminal or necessarily anonymous. The central difficulty is that a technologically decentralized payment can perform economically significant functions without passing through the centralized intermediaries on which conventional identification, monitoring, record keeping, freezing, and reporting mechanisms depend. Consequently, the development of cryptocurrency payments requires legal systems to reconsider how they define property, payment activity, financial intermediation, custody, evidentiary attribution, proceeds of crime, and regulatory responsibility.

The examination of the Iranian framework demonstrates that the principal weakness is not the complete absence of legal rules capable of responding to cryptocurrency-related misconduct. Existing criminal law can already address numerous forms of fraud, cybercrime, unauthorized access, money laundering, illicit financing, and acquisition of criminal proceeds. The deeper problem is fragmentation. Cryptocurrency has developed across several areas of law without being incorporated into a comprehensive legal architecture. Regulatory measures concerning mining, financial transactions, economic activity, cybercrime, and criminal finance respond to particular risks but do not collectively provide a clear and predictable framework for cryptocurrency payments. This fragmentation creates uncertainty concerning the legal classification of crypto-assets, the status of payment transactions, the licensing of professional service providers, customer identification, institutional competence, digital evidence, cross-border jurisdiction, and the seizure and restitution of digital assets.

The appropriate legislative response should begin with conceptual clarification. Crypto-assets should be expressly recognized as transferable forms of digital economic value capable of constituting legally protected assets. Such recognition does not require their classification as legal tender and does not weaken the state's authority over the official monetary system. It simply reflects the economic reality that persons can possess, transfer, lose, steal, conceal, exchange, and use digital assets to satisfy obligations. Once that point is established, the law can distinguish between personal ownership and transfer, which should remain generally lawful unless associated with independent criminal conduct, and professional service activities that justify licensing and supervision.

A comprehensive statutory framework should therefore define crypto-assets, cryptocurrency payments, exchanges, custodial wallets, transfer services, and other relevant intermediaries according to their functions. Professional service providers should be subject to authorization proportionate to the services they perform and the risks they create. The framework should establish governance, cybersecurity, record-keeping, customer-identification, beneficial-ownership, and suspicious-transaction reporting obligations while avoiding the assumption that every private wallet user should be regulated as a financial institution. This distinction is essential for proportionality and enforceability.

Criminalization should be targeted rather than technology-based. The mere use, possession, or transfer of cryptocurrency should not constitute criminal conduct. The criminal law should instead focus on intentional acts that produce identifiable harm or deliberately defeat essential regulatory protections. Serious unauthorized operation of a professional cryptocurrency service, fraudulent acquisition of digital assets, intentional unauthorized transfer of another person's assets, deliberate concealment or laundering of criminal proceeds, knowing facilitation of prohibited financing, falsification of regulatory information, and intentional circumvention of legally mandatory identification mechanisms can justify criminal sanctions where existing offenses do not already provide adequate coverage. Minor licensing failures, procedural deficiencies, or ordinary compliance mistakes should ordinarily remain within administrative enforcement unless accompanied by aggravating circumstances or culpability sufficient to justify criminal punishment.

The principle of technological neutrality should guide reform. Where conduct is already criminal regardless of the medium used, legislation should clarify that crypto-assets fall within the existing offense rather than create unnecessary parallel crimes. Fraud does not become a fundamentally different offense because the victim transfers cryptocurrency rather than conventional money. Theft-like appropriation does not lose its harmful character because the property is represented by cryptographic control rather than physical possession. Money laundering remains laundering when criminal proceeds are converted into digital assets. The principal legislative task is therefore to ensure that existing offense definitions encompass contemporary forms of economic value while creating genuinely new offenses only where technological features produce conduct that existing law cannot adequately reach.

Substantive criminal law will nevertheless remain ineffective without procedural reform. Cryptocurrency investigations require the ability to identify relevant service providers, preserve account information, obtain transaction records, interpret blockchain evidence, associate wallet addresses with persons, freeze assets, secure private keys, and maintain digital assets safely during proceedings. The evidentiary status of blockchain information should therefore be clarified, including principles governing authenticity, integrity, expert interpretation, attribution, and chain of custody. Courts should recognize that a blockchain record can establish the occurrence of a transaction while not necessarily establishing the legal identity of the person behind an address. Attribution should remain an evidentiary question requiring a combination of digital and conventional proof.

Digital-asset recovery should constitute a central component of reform rather than an afterthought. Cryptocurrency can be transferred rapidly, and successful prosecution may provide little practical protection if proceeds cannot be preserved and returned to victims or confiscated from offenders. Legislation should establish clear rules for freezing assets held by regulated custodians, obtaining lawful control of digital assets, transferring seized cryptocurrency into secure government custody, managing volatility and cybersecurity risks, valuing assets, and determining their final disposition. Specialized technical protocols should accompany statutory powers so that legal authority can be implemented without accidental loss, unauthorized access, or evidentiary contamination.

Institutional coordination is equally important. Cryptocurrency-related conduct may simultaneously engage financial regulators, the central bank, financial-intelligence authorities, cybercrime police, prosecutors, courts, and other public bodies. A fragmented institutional response replicates the fragmentation already found in substantive regulation. Reform should designate a clear supervisory authority for professional cryptocurrency service providers while creating binding mechanisms for cooperation and information exchange among financial, investigative, and judicial institutions. Specialized units should possess the technical capacity to conduct blockchain analysis and digital-asset investigations, while prosecutors and judges should receive continuing training in the evidentiary and legal characteristics of cryptocurrency.

Cross-border cooperation must also be embedded in the legal framework. The technical architecture of cryptocurrency permits assets to move between users and services located in different jurisdictions with extraordinary speed. National legislation cannot eliminate this feature, but it can provide domestic authorities with clear powers to preserve evidence, request foreign information, cooperate in the freezing of assets, and participate in lawful mechanisms for confiscation and restitution. The effectiveness of such cooperation will depend both on domestic legal clarity and on the capacity of Iranian institutions to communicate with foreign counterparts and private service providers under applicable legal procedures.

The resulting model should be neither prohibitionist nor permissive. Complete prohibition would risk displacing legitimate activity into less transparent environments while failing to eliminate decentralized transactions. Unrestricted legalization without compliance duties would leave users and the financial system exposed to avoidable criminal risks. A regulated-legality model offers a more coherent alternative. Under such a model, legitimate cryptocurrency payments can occur within defined legal boundaries; professional service providers can operate under clear licensing and compliance obligations; users can understand their rights and responsibilities; investigators can access legally authorized information; courts can apply stable evidentiary standards; and criminal sanctions can be reserved for harmful and culpable conduct.

The principal legislative priority is therefore not to create the largest possible number of cryptocurrency offenses. It is to eliminate legal uncertainty and construct a coherent system in which existing criminal principles can operate effectively in a digital environment. A well-designed framework should combine legal recognition of crypto-assets, functional regulation of payment-related services, proportionate customer-identification and reporting duties, explicit application of property and financial-crime rules, targeted criminalization, digital-evidence standards, effective asset-recovery mechanisms, institutional coordination, technical capacity, and international cooperation. Such reforms would enable Iranian criminal policy to respond to the actual risks of cryptocurrency payments without suppressing their legitimate economic uses.

Ultimately, the legal challenge presented by cryptocurrency is a problem of adaptation rather than replacement. The fundamental objectives of criminal law remain familiar: protection of property, prevention of fraud, interruption of criminal finance, attribution of responsibility, preservation of evidence, recovery of unlawful proceeds, and protection of legitimate economic activity. What has changed is the technological environment in which these objectives must be achieved. Legislative reform should therefore translate established legal principles into rules capable of operating in decentralized digital payment systems. By focusing on economic function, demonstrable harm, culpability, proportionality, and technological neutrality, the Iranian legal system can close the principal gaps surrounding cryptocurrency payments while maintaining the distinction between financial innovation and criminal misuse.

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

Akartuna, E. A., Johnson, S. D., & Thornton, A. E. (2022). The Money Laundering and Terrorist Financing Risks of New and Disruptive Technologies: A Futures-Oriented Scoping Review. *Security Journal*, 1.

Alrasheed, R. A. R. (2025). Building Public Trust in Bahrain: Leveraging Artificial Intelligence to Combat Financial Fraud and Terrorist Financing Through Cryptocurrency Tracking. *Social Sciences*, *14*(5), 308.

Azadbakht, D. Y. F. A. F. (2024). *Money Laundering through Digital Currencies: An Analysis from the Perspective of International Law*

Bakhshi, A. (2025). Iranian Criminal Policy in Combating Cybercrimes Related to Cryptocurrencies and Unauthorized Transactions. Ninth International Conference on Jurisprudence, Law, Advocacy, and Social Sciences in the Horizon of Iran 1404, https://civilica.com/doc/2296304

Boyko, A., Dotscenko, T., & Dolia, Y. (2022). Patterns of Financial Crimes Using Cryptocurrencies. *Socio-Economic Relations in the Digital Society*, *2*(44), 23-28.
Chainalysis. (2022). *The 2022 Crypto Crime Report*.
Chohan, U. W. (2021). Cryptocurrency: A Theoretical Perspective. *SSRN Electronic Journal*.
Dyntu, V., & Dykyj, O. (2021). Cryptocurrency as an Instrument of Terrorist Financing. *Baltic Journal of Economic Studies*, *7*(5), 89-121.
Esoimeme, E. (2020). Identifying and Reducing the Money Laundering Risks Posed by Individuals Who Have Been Unknowingly Recruited as Money Mules. *Journal of Money Laundering Control*, *24*(1), 205.
Europol. (2021). *Cryptocurrencies: Tracing the Path in a Crypto World*.
Faghih, A., Barzegarzadeh, A., & Safaei, M. (2025). A Comparative Analysis of Legislative Criminal Policies in Iran and the United Kingdom in Addressing Cryptocurrency-Related Financial Crimes. *Legal Studies in Digital Age*, *4*(1), 1-10.
Financial Action Task, F. (2020). *Annual Report 2019-2020*.
Financial Action Task, F. (2022). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*.
Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering Money Laundering and Terrorist Financing: A Case for Bitcoin Regulation. *Research in International Business and Finance*, *56*, 101387.
Ghaemi Asl, M., Abolhasani, S., & Farhoud, N. (2024). Optimal Criminal Policy against the Criminal Risks of Virtual Currencies.
Ghavami, P. S. M., & Mahmoudi, A. (2024). Legal Framework and International Efforts in Combating Digital Currency Crimes: An International Instruments Approach.
Ghavampour Sarshkeh, M., & Mahmoudi, A. (2023). *The Impact of International Instruments on Controlling Business Crimes in Iran with an Approach to Digital Currencies*. Jahan-e Siasat Publications.
Giudici, G., Milne, A., & Vinogradov, D. (2020). Cryptoassets: Market Analysis and Perspectives. *Journal of Industrial and Business Economics*, *47*.
Haghi, M., Shiroud Heydari, P., Shayan Asl, S., Irani Asl, H., Mosaebi, N., & Abdollahzadeh, F. (2025). The Role of Digital Currencies in Facilitating Cybercrimes. Fifth International Conference on Advanced Research in Management and Humanities, https://civilica.com/doc/2325900
Hasan, R., Hassan, M. K., & Aliyu, S. (2020). Fintech, Blockchain and Islamic Finance: Literature Review and Research Agenda.
Houben, R., & Snyers, A. (2020). *Cryptoassets: Key Developments, Regulatory Concerns and Responses*. https://www.blockchainwg.eu/wp-content/uploads/2020/05/IPOL_STU2020648779_EN.pdf
Huang, R. H., Yang, D., & Loo, F. F. Y. (2020). The Development and Regulation of Crypto-Assets: Hong Kong Experiences and a Comparative Analysis. *European Business Organization Law Review*, *21*(2).
Ibrahim, O. (2024). Cryptocurrency: The New Unleashed Financial Instrument, Should It Be Regulated. *Humanities Journal of University of Zakho*, *12*(2), 303-317.
Jabotinsky, H. Y. (2020). The Regulation of Cryptocurrencies: Between a Currency and a Financial Product. *Fordham Intellectual Property, Media & Entertainment Law Journal*, *31*, 121.
Kapsis, I. (2023). Crypto-Assets and Criminality: A Critical Review Focusing on Money Laundering and Terrorism Financing. In *Organised Crime, Financial Crime, and Criminal Justice* (pp. 122-141).
Koshulovich, V. (2023). Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges. *Journal of Security Studies*.
Koster, H. (2020). Towards Better Implementation of the European Union's Anti-Money Laundering and Countering the Financing of Terrorism Framework. *Journal of Money Laundering Control*, *23*.
Malakoutikhah, Z. (2020). Criminalisation of Terrorism Financing in Iranian Law. *Journal of Financial Crime*, *27*(1), 231-244.
Mirmojidi, S. (2024). Examining Iran's Legislative and Judicial Criminal Policy in the Field of Cryptocurrencies with Emphasis on the Crime of Disrupting the National Economic System.
Namamian, P. (2024). The Feasibility of Addressing the Financing of Terrorist Crimes in the Realm of Cryptocurrencies: The Experiences of Iran and Other Countries. *Iranian Journal of International and Comparative Law*, *2*(1), 55.
Noronha Rodrigues, J., Bhattacharya, S., & Cabete, D. (2025). Impact of Financial Terrorism in Global Economy, Counter Feeding Currency and Other Digital Cyber Crimes. *Brazilian Journal of Law & International Relations / Relações Internacionais no Mundo*, *1*(47).
Rabbani, M. R., Khan, S., & Thalassinos, E. I. (2020). FinTech, Blockchain and Islamic Finance: An Extensive Literature Review. *International Journal of Economics and Business Administration*, *8*, 65.
Rashidi, B. G. (2024). The Challenge of Virtual Currencies in Combating Money Laundering and Terrorist Financing with Emphasis on FATF Actions and Recommendations. Ninth International Conference on Law, Psychology, Educational and Behavioral Sciences, https://civilica.com/doc/2204347
Vucinic, M. (2020). FinTech and Financial Stability: Potential Influence of FinTech on Financial Stability, Risks and Benefits. *Journal of Central Banking Theory and Practice*, *71*, 49.