How to cite this article:
Rajabi, A., & Rajabi Nezhad, S. (2025). A Criminological Analysis of Cryptocurrencies and the Challenges of Prosecuting Blockchain-Based Crimes. *Journal of Historical Research, Law and Policy, 3*(2), 1-20. https://doi.org/10.61838/jhrlp.118

Article history:
Original Research

Dates:
Submission Date: 20 February 2025
Revision Date: 13 May 2025
Acceptance Date: 20 May 2025
Publication Date: 01 June 2025

A Criminological Analysis of Cryptocurrencies and the Challenges of Prosecuting Blockchain-Based Crimes

1. Akbar. Rajabi[1*] : Department of Law, Khom.C., Islamic Azad University, Khomein, Iran
2. Sajad. Rajabi Nezhad[2]: Department of Law, Khom.C., Islamic Azad University, Khomein, Iran

*corresponding author's email: Akbar.rajabi@iau.ac.ir

ABSTRACT

The rapid rise of cryptocurrencies and blockchain technology has reshaped global financial systems while simultaneously creating unprecedented opportunities for criminal exploitation. This narrative review examines the criminological dimensions of crypto-crime by analyzing the technological characteristics of decentralized digital assets, offender motivations, behavioural patterns and the systemic challenges faced by law enforcement. The article identifies major typologies of blockchain-enabled crime—including money laundering, fraud, ransomware, darknet transactions, unauthorized mining and exchange breaches—and demonstrates how offenders leverage anonymity, transactional speed and jurisdictional ambiguity to facilitate illicit activity. Through a criminological lens, the review explores how rational decision-making, opportunity structures and transnational collaboration shape offender behaviour in digital environments. The analysis also highlights significant obstacles to detection and prosecution, such as evidentiary limitations, privacy-enhancing technologies, cross-chain obfuscation, inconsistent regulatory frameworks, smart contract complexity and the lack of harmonized global standards. In response to these challenges, the review outlines key policy frameworks and enforcement strategies, including advancements in blockchain forensics, AI-based transaction tracing, AML/CFT regulations, licensing regimes for digital asset service providers, FATF-aligned international standards, cross-border investigative mechanisms and the development of specialized cybercrime units. The review concludes that addressing crypto-crime requires a multidisciplinary, globally coordinated approach that integrates technological innovation, legal reform and enhanced institutional capacity. As blockchain ecosystems continue to evolve, the complexity and scale of digital criminality will increase, making comprehensive, forward-looking strategies essential for effective governance and crime prevention.

Keywords: *Cryptocurrency crime; blockchain forensics; cybercrime; money laundering; decentralized finance; digital evidence; regulatory frameworks; transnational crime.*

Introduction

The rapid expansion of cryptocurrencies over the past decade has transformed the global digital economy, generating profound opportunities for innovation while simultaneously creating complex challenges within the realm of criminal law. The decentralized and borderless architecture of blockchain networks has facilitated unprecedented forms of financial interaction, enabling instant, irreversible transfers that bypass the traditional controls of centralized banking institutions. As several scholars have noted, the growth of digital assets has reshaped economic behaviour in ways that directly intersect with criminogenic environments, particularly as offenders exploit anonymity, pseudonymity and the absence of conventional regulatory oversight to commit technologically sophisticated

misconduct (1). This transformation has given rise not only to new forms of digital financial activity but also to novel patterns of exploitation that expose both the vulnerabilities and the limits of existing legal frameworks. The emergence of cryptocurrencies as functional instruments in illicit markets reflects broader trends in global cybercrime, which has been expanding in complexity, transnationality and technical skill, reshaping the investigative landscape for states, corporations and legal systems worldwide (2).

The criminological study of cryptocurrency-related offences has gained increasing importance because traditional theories of crime and enforcement now encounter unique obstacles posed by the digitalization of economic life. The digital environment reduces situational barriers that historically constrained certain forms of criminal behaviour, allowing actors to operate across jurisdictions, collaborate anonymously, and conduct illicit transactions with minimal risk of immediate detection. This is evident in the way cybercriminals leverage blockchain mechanisms to facilitate fraud, identity theft and financial deception, as emphasised in analyses of digital crime ecosystems (3). In many instances, offenders utilize cryptocurrencies not simply as tools for monetary gain but as structural components of broader transnational criminal operations, including complex schemes that integrate social engineering, hacking, and corporate misconduct. The evolution of cybercrime in legal scholarship has highlighted how criminal law systems are under constant pressure to adapt to these emerging modalities of wrongdoing (4). Traditional criminological frameworks, though foundational, require reinterpretation in light of technologically mediated forms of deviance that operate beyond physical constraints and rely heavily on digital anonymity and automated interactions.

The typology of digital and financial crimes has changed significantly due to the integration of blockchain technology into contemporary illicit economies. Historically, financial crimes such as fraud, money laundering and embezzlement operated through identifiable actors and traceable channels. Today, however, crypto-assets introduce a fundamentally different terrain marked by encrypted identities, peer-to-peer transfers, decentralized finance applications and smart contract–based transactions. The digitalization of financial crime mirrors the broader evolution of economic criminal behaviours described in scholarship on digital-era financial offences, which notes how novel technologies create opportunities for both innovation and abuse (5). As online transactions have grown in scale and sophistication, so too has the capacity of criminals to exploit weaknesses in digital infrastructures, particularly when law enforcement capabilities lag behind technological advancements. This gap is compounded by the growing use of cryptocurrencies in ransomware attacks, darknet marketplaces and cross-border financial schemes, reflecting the increasingly hybrid nature of modern crime. The integration of cyber-law perspectives into this discourse highlights how offenders strategically manipulate jurisdictional ambiguities and technical loopholes to evade liability, as observed in analyses of hacker accountability and cyber-based threats (6).

The unique challenges posed by blockchain-based crimes to law enforcement and prosecutorial agencies arise from the core technological principles of blockchain itself. Unlike conventional financial systems, blockchain transactions are validated through decentralized consensus mechanisms, creating immutable records that cannot be modified or erased. This immutability, while beneficial for transparency, simultaneously complicates investigative interventions, as criminal transactions cannot be reversed and may be routed through multiple layers of obfuscation. Scholars examining cross-jurisdictional enforcement mechanisms emphasize that decentralized digital systems undermine conventional legal assumptions regarding control, traceability and state sovereignty (7). Furthermore, the use of mixing services, privacy-enhancing coins and cross-chain bridges makes it increasingly difficult for authorities to link illicit transactions to identifiable actors. The legal literature underscores that prosecutorial

challenges are exacerbated by the absence of a clear legal definition of many crypto-based offences, as regulatory frameworks remain inconsistent across jurisdictions (8). These complexities impede both the attribution of criminal responsibility and the collection of admissible digital evidence, requiring law enforcement to adopt new forensic capacities and investigative approaches.

The significance of studying crypto-related crimes extends far beyond academic interest; it bears crucial implications for legal systems, financial regulators and international law enforcement agencies. Legal analysts have warned that the rapid technological evolution of digital markets risks outpacing the development of effective regulatory responses, particularly in fields where corporate criminal liability intersects with digital transactions (9). Financial regulators face increasing difficulty in monitoring decentralized markets that do not rely on intermediaries, complicating the implementation of anti-money-laundering initiatives and know-your-customer procedures. Studies addressing the vulnerabilities of legal systems to technologically driven transformations indicate that existing regulatory models often lack the flexibility to accommodate decentralized infrastructures (10). Furthermore, international cooperation becomes indispensable as crypto-crime operations frequently cross borders, involving actors in jurisdictions with divergent enforcement standards, regulatory philosophies, and technological capacities. Scholars analyzing crimes that exploit virtual asset systems highlight how international bodies must collaborate to harmonize investigative strategies and minimize regulatory arbitrage (11). Without such coordination, gaps in enforcement create safe havens for criminal networks to flourish, undermining global financial stability and the rule of law.

Existing literature reveals several critical research gaps that necessitate a comprehensive criminological analysis of blockchain-based crimes. While numerous studies address technical aspects of cryptocurrency systems, fewer provide integrated criminological interpretations that connect offender motivations, opportunity structures and enforcement limitations. Research addressing cybercrime evolution has noted that legal scholarship often separates technological analysis from criminological theory, resulting in fragmented insights rather than holistic frameworks (12). Similarly, while some works examine money laundering through cryptocurrencies, they typically focus on regulatory reforms rather than behavioural dynamics, leaving a gap in understanding how digital environments shape offending patterns and criminal decision-making (13). The legal commentary on cyber-offending frequently emphasises structural or institutional vulnerabilities but seldom investigates how offenders exploit these vulnerabilities in practice, as highlighted in studies of cybercrime jurisdictional challenges (14). Furthermore, although a growing body of work addresses digital financial crimes, analyses remain limited regarding the prosecutorial difficulties surrounding blockchain evidence and decentralized platforms. This gap is particularly evident in research addressing corporate or economic crimes, where comparisons with digital financial offences reveal that traditional liability models may not align with decentralized technological systems (15).

Another underexplored area concerns the comparative analysis of digital law enforcement systems across countries. While certain studies highlight the inadequacies of national criminal codes in responding to digital crimes, such as examinations of Mongolian and Indonesian systems (16, 17), there remains insufficient exploration of how different legal cultures conceptualize and respond to blockchain-related offences. Additionally, scholarly attention has yet to fully address the sociotechnical dimensions of crypto-crime ecosystems, particularly the interplay between technological affordances, illicit market structures and the behavioural strategies of offenders. Analyses of online gambling crimes and other technology-enabled offences suggest that digital criminality evolves through adaptive feedback loops in which offenders respond dynamically to enforcement measures (18). However, the

literature does not sufficiently extend this insight to the blockchain context, where the adaptability of offenders is amplified by the rapid development of new cryptographic tools and decentralized applications.

Given these gaps and the complex, rapidly evolving nature of cryptocurrency-related crimes, the purpose of this narrative review is to synthesize existing legal, technological and criminological research to provide a comprehensive analysis of blockchain-based criminality and the challenges associated with prosecuting such offences. This review aims to integrate multidisciplinary perspectives to illuminate the core characteristics of crypto-crime, identify systemic vulnerabilities and clarify the multifaceted barriers facing modern legal enforcement. By drawing on a diverse body of scholarship, this study seeks to contribute an analytically rigorous foundation for understanding the criminological dynamics of digital asset misuse and to support the development of more responsive and effective legal strategies.

Conceptual Foundations

The conceptual foundations of cryptocurrency-related criminality require an integrated understanding of both the technological structure of digital assets and the criminological frameworks that explain how offenders interact with these systems. Cryptocurrencies function as digital representations of value that operate through cryptographic protocols rather than state-issued fiat mechanisms. Their technical and legal characteristics differ significantly from traditional currencies, as they rely on decentralized computational networks to validate transactions rather than centralized authorities. Discussions in cross-jurisdictional legal scholarship emphasize that the absence of a central supervisory institution complicates the application of conventional regulatory doctrines, particularly in cases involving transnational digital transactions (7). From a technical standpoint, cryptocurrencies are structured around public-private key encryption systems that authenticate users without revealing their real-world identities. This pseudonymity is a defining feature of digital currencies and is frequently cited in legal studies concerning cybercrime, as offenders can conceal their identities while engaging in illicit activities across multiple jurisdictions (14). The immutability of blockchain records further distinguishes cryptocurrencies from traditional assets, because once transactions are validated and added to the chain, they cannot be altered or erased, even by law enforcement. Analysts examining the digital transformation of criminal behaviour highlight this immutability as both a benefit for system integrity and a challenge for legal intervention, since irreversible transfers can facilitate the permanent movement of illicit funds (2). These core characteristics—decentralization, pseudonymity and immutability—form the foundation upon which offenders exploit digital currencies to conduct financial, cyber and transnational crimes.

The principle of decentralization lies at the heart of the cryptocurrency ecosystem. Unlike centralized banking structures, decentralized networks distribute authority across thousands of nodes, making them resistant to single-point failures and external manipulation. This architecture is celebrated in technological literature for promoting transparency and autonomy, but it also imposes significant barriers for regulatory oversight. Studies addressing the evolution of digital financial crime emphasize that decentralization reduces the effectiveness of traditional enforcement frameworks that rely on institutional intermediaries to monitor and report suspicious transactions (5). In a decentralized ecosystem, no single entity possesses full control over the ledger, which limits the capacity of states to freeze accounts or reverse unlawful transfers. Pseudonymity compounds this problem by enabling users to transact without attaching identifiable personal information to their digital addresses. While every transaction is visible on a public ledger, scholarly analyses show that blockchain pseudonymity creates opportunities for offenders to mask illicit movements by using layered transactions, mixing services and privacy-enhancing tools (1). The

immutable nature of the ledger strengthens system integrity but simultaneously solidifies the consequences of unauthorized transfers, as law enforcement cannot technically intervene once funds have been moved, a reality noted in legal commentaries on cross-border digital crime investigations (6). These intertwined features make cryptocurrencies both resilient and vulnerable, enabling legitimate innovation while facilitating criminal exploitation.

To fully understand cryptocurrency-enabled crime, it is essential to explore blockchain as the technological infrastructure that underpins digital currencies. Blockchain operates as a distributed ledger composed of sequentially linked blocks, each containing transaction information that is validated through consensus mechanisms. These mechanisms, such as Proof of Work or Proof of Stake, allow network participants to agree on the legitimacy of each transaction without centralized oversight. Legal studies discussing the adaptability of criminal law highlight how such consensus protocols complicate jurisdictional authority, as the validation of transactions occurs across nodes located in multiple countries with differing regulatory standards (4). The distributed nature of consensus undermines traditional notions of territorial enforcement, since no single state can assert control over transaction validation. Additionally, the transparent yet pseudonymous architecture of blockchain creates a paradox of traceability. Every transaction is permanently recorded and publicly visible, making blockchain one of the most transparent financial systems ever developed. Yet, as legal analyses of virtual asset misuse demonstrate, the absence of attached personal identities means that investigators often observe the movement of funds without being able to attribute those movements to specific individuals (11). This duality—complete traceability of data coupled with limited identifiability of actors—poses one of the most complex challenges for prosecutors and forensic investigators.

Smart contracts represent another critical dimension of blockchain infrastructure, offering automated, self-executing agreements encoded directly into the blockchain. Their legal and criminological implications have been the subject of extensive debate. Scholars examining smart contract enforceability emphasize their potential to reduce human error and improve transactional efficiency, while also highlighting vulnerabilities related to coding errors and malicious exploitation (19). Since smart contracts execute automatically once predefined conditions are met, they can be manipulated by offenders who exploit loopholes in the contract's logic or deploy malicious contracts for fraudulent purposes. Discussions in the field of digital transaction law show that smart contracts challenge traditional interpretations of intent, consent and enforceability, particularly when used in cross-jurisdictional contexts where legal standards differ significantly (20). This technological dimension introduces new criminogenic opportunities by enabling automated deception, unauthorized value extraction and fraudulent digital obligations that operate beyond conventional legal controls. The integration of smart contracts into decentralized finance platforms further expands the potential for criminal exploitation, as financial operations can be carried out autonomously without institutional oversight.

Criminological theories provide a vital lens through which cryptocurrency-enabled crime can be analyzed, particularly given that technological explanations alone cannot account for offender motivations or behavioural patterns. Routine Activity Theory offers a useful conceptual framework for understanding the convergence of motivated offenders, suitable targets and the absence of capable guardians in digital environments. Scholars argue that the digital transformation of everyday activities has created continuous opportunities for criminal engagement by removing physical constraints and enabling offenders to act anonymously at any time and from any location (3). Cryptocurrencies serve as highly suitable targets because they store value digitally and can be transferred instantly across borders. Meanwhile, the absence of capable guardians manifests in the limited ability of regulatory agencies

to monitor decentralized systems, as noted in discussions of cybercrime enforcement gaps (17). The theory highlights how the convergence of these conditions enables offenders to exploit blockchain ecosystems with reduced risk of detection.

Rational Choice Theory further enhances this understanding by emphasizing that offenders make calculated decisions based on perceived risks and rewards. Analyses of economic and corporate crime within digital contexts reveal that offenders perceive cryptocurrencies as low-risk, high-reward instruments due to their global accessibility, pseudonymity and resistance to traditional enforcement mechanisms (15). The technical affordances of blockchain reduce the perceived risk of apprehension, particularly when offenders use privacy tools or cross-chain bridges to obfuscate their activities. Rational Choice Theory thus helps explain why criminals increasingly migrate to cryptocurrency-based operations, as the architecture of digital systems shifts the cost–benefit calculus in their favour. Legal scholars emphasize that this perception persists even when governments enhance regulatory frameworks, because offenders continuously adapt to new controls by developing more sophisticated evasion methods (21).

Opportunity theory and cyber-opportunity structures offer additional insight by illustrating how digital landscapes create new spaces for criminal activity. Analyses of cyber law and digital accountability highlight that offenders often exploit vulnerabilities in technological systems, including unsecured exchanges, poorly designed smart contracts and inconsistent compliance mechanisms (22). The structure of the internet and global digital markets provides immediate access to victims and global financial networks, increasing the scale and speed at which offences can occur. Blockchain technology, in particular, expands these opportunities by enabling decentralized trading platforms, anonymous wallets and automated financial instruments that operate around the clock. Scholars examining financial crimes in emerging digital markets note that offenders use these structures to launder funds, orchestrate fraud schemes and evade jurisdictional enforcement through rapid, cross-border transactions (23). Opportunity theory thus situates cryptocurrency-related crime within the broader evolution of technological opportunity spaces that shape offender behaviour.

Situational crime prevention in crypto ecosystems requires adapting established preventive strategies to the unique properties of blockchain technology. Preventive approaches that emphasize increasing effort, increasing risk and reducing rewards must be reimagined for decentralized digital environments. Analyses of technology-driven criminal behaviour demonstrate that traditional preventive tools, such as institutional monitoring and centralized reporting systems, are significantly less effective in decentralized blockchain settings (8). The absence of intermediaries limits opportunities to impose guardianship, while automated systems reduce human oversight. Nevertheless, situational prevention can still be applied by enhancing blockchain forensic capabilities, promoting responsible exchange practices and implementing strict regulatory compliance across digital financial institutions. Research in legal reform underscores the importance of strengthening institutional capacity to detect, trace and prosecute cryptocurrency-based offences, particularly by integrating new forensic technologies and establishing coordinated international frameworks (9). Preventive approaches in crypto ecosystems must therefore rely on technological adaptation rather than traditional institutional controls.

Together, these conceptual foundations illustrate that understanding cryptocurrency-enabled crime requires a synthesis of technological knowledge and criminological theory. The distinctive technical properties of cryptocurrencies—decentralization, pseudonymity and immutability—create an environment in which offenders can exploit structural vulnerabilities with relative ease. Blockchain technology, with its consensus mechanisms and

programmable smart contracts, further expands both legitimate and illicit capabilities. Criminological theories provide essential insights into how offenders navigate these systems, why they perceive them as advantageous and how opportunity structures shape their behaviour. This integrated conceptual framework establishes the groundwork for analysing the criminal dynamics of blockchain-based systems and highlights the necessity of developing legal and preventive strategies that address both technological and behavioural dimensions of cryptocurrency-related crime.

Typology of Blockchain-Based Crimes

The typology of blockchain-based crimes reflects the growing diversification and sophistication of illicit activities that exploit the structural characteristics of cryptocurrencies and decentralized systems. Cryptocurrencies enable an ecosystem in which offenders can obscure their identities, bypass traditional financial intermediaries and conduct transnational operations with unprecedented speed. As digital asset markets expand, so too does the range of offences facilitated by blockchain technology, illustrating a convergence of economic, cyber and transnational criminal behaviours. Scholars examining the evolution of cybercrime consistently emphasize that technological shifts reshape offender strategies, leading to new forms of criminal conduct that leverage decentralization, pseudonymity and global accessibility (4). These transformations necessitate a detailed and systematic understanding of the major categories of blockchain-enabled crimes.

One of the most significant and widely studied categories is the use of cryptocurrencies for money laundering. Money laundering in the blockchain environment involves the process of concealing the origins of illicit funds by converting them into digital assets, moving them across decentralized platforms and obscuring transactional pathways. Legal analyses of virtual asset misuse emphasize that offenders exploit pseudonymity to obscure their identities during the layering and integration stages of laundering operations (1). Mixers and tumblers play a central role in this process. These services intentionally obscure transaction histories by pooling funds from multiple users and redistributing them in a way that makes it extremely difficult to trace the original source. Scholars examining cybercrime enforcement note that mixers represent a technological evolution of traditional laundering tools, designed specifically to disrupt blockchain traceability (14). Privacy coins such as Monero and Zcash further complicate enforcement efforts because their protocols intentionally hide sender and receiver information through advanced cryptographic techniques. The immutability of the blockchain amplifies these challenges, as transactions—even illicit ones—cannot be reversed, a problem highlighted in discussions of decentralized financial operations and their resistance to conventional regulatory controls (6). In jurisdictions lacking robust digital financial regulations, offenders launder funds with even greater ease, exploiting gaps in national and international enforcement frameworks (13).

Fraud and scams constitute another major category of blockchain-based crime, driven primarily by the lack of central oversight in digital asset markets and the rapid expansion of decentralized finance (DeFi). Initial Coin Offering (ICO) fraud emerged early in the cryptocurrency boom, as many issuers solicited investment for projects that did not exist or were grossly misrepresented. Legal analyses of digital financial criminality show that ICO scams often rely on deceptive white papers, fabricated technical claims and manipulated marketing narratives to attract investors before disappearing with the funds (5). Rug pulls represent a more recent variation in which project developers abandon a DeFi platform after raising capital, withdrawing liquidity pools and collapsing the token value. Scholars examining online economic crime note that rug pulls mirror traditional investment fraud but are amplified

by blockchain's anonymity, which allows perpetrators to vanish without revealing their identities (15). Ponzi-like DeFi schemes also proliferate, promising extraordinarily high returns on staking or yield-farming platforms. These schemes depend on continuous inflows of new deposits and frequently collapse once withdrawals exceed incoming investments. Analysts of transnational cyber fraud emphasize that decentralized platforms reduce regulatory oversight, enabling cross-border scam operations that involve thousands of victims before enforcement agencies can intervene (2). The inherently speculative culture of digital asset markets further increases vulnerability, as investors often engage in high-risk behaviour without fully understanding the platform's structure or legitimacy.

Ransomware and extortion operations have been fundamentally transformed by the integration of cryptocurrency payments into cybercrime ecosystems. Ransomware involves malicious software that encrypts a victim's data, followed by demands for payment in exchange for decryption keys. Crypto-payments have become the preferred method for such demands because they enable rapid, pseudonymous transfers that bypass traditional banking oversight. Scholars analyzing the evolution of digital extortion note that cryptocurrency infrastructure significantly reduces the risk for offenders by allowing funds to be transferred across multiple wallets, mixed in tumblers or converted into privacy coins immediately after receipt (3). These characteristics have led to the professionalization of ransomware operations, with organized groups developing sophisticated "ransomware-as-a-service" models that rely on cryptocurrency for revenue distribution. Legal literature examining digital criminal markets highlights that cross-jurisdictional obstacles exacerbate enforcement difficulties, as attackers commonly operate from regions with minimal legal cooperation and exploit global differences in cyber regulation (11). In some cases, extortion extends beyond simple encryption, with attackers threatening to leak sensitive data unless payments are made, creating dual-layered pressure on victims. The role of cryptocurrencies in enabling these operations underscores the need for forensic capacity-building in blockchain tracing and international coordination in cyber enforcement strategies (17).

Darknet market transactions constitute another major typology of blockchain-based crime, representing the intersection of drug trafficking, weapons distribution, identity theft and other illicit activities conducted via anonymous online platforms. These darknet markets operate on encrypted networks such as Tor and rely on cryptocurrencies as the primary medium of exchange due to their pseudonymous nature. Studies addressing the challenges of regulating virtual assets highlight that darknet vendors use blockchain systems because they allow the sale of illegal goods without requiring traditional payment processors that would otherwise detect suspicious activities (1). Drug markets on the darknet have expanded dramatically as cryptocurrencies lower barriers to participation, enabling buyers and sellers to transact anonymously across continents. Identity data, counterfeit documents and weapons are also commonly traded, as noted in analyses of transnational digital crime ecosystems (2). Offenders frequently combine cryptocurrency payments with operational security measures such as encrypted communications, multi-hop routing and escrow services that further obscure criminal activity. Legal scholars emphasize that enforcing laws against darknet transactions is significantly hindered by the lack of centralized points of control, making it extremely difficult to identify market operators or intercept illicit financial flows (7). Even when platforms are seized, as has occurred in several international operations, new darknet markets typically emerge quickly, illustrating the adaptability and resilience of these criminal ecosystems.

Crypto-jackings and mining-malware constitute another expanding category of blockchain-enabled crime. Crypto-jacking involves unauthorized use of another person's computing resources to mine cryptocurrencies, while mining-malware refers to malicious software installed on victims' devices for the same purpose. Scholars examining

cybercrime evolution highlight that offenders increasingly prefer crypto-jacking because it offers a continuous revenue stream with low risk of detection, especially when mining occurs in small increments across thousands of compromised devices (4). Unlike traditional data theft or extortion, crypto-jacking does not require direct interaction with victims; offenders benefit from computational theft rather than financial transfers. Analyses of technological vulnerabilities reveal that mining-malware spreads through phishing emails, malicious browser scripts and compromised websites, exploiting weak cybersecurity practices in both personal and institutional networks (22). Offenders often deploy advanced obfuscation techniques to mask mining operations, making the malware difficult to detect through standard anti-virus tools. In some cases, mining operations are embedded in large-scale botnets that generate substantial illicit revenue. Studies addressing corporate technological security emphasize that organizations face increased operational costs, reduced system performance and heightened security risks due to the proliferation of mining-malware attacks (24). These crimes highlight the expanding scope of blockchain-related exploitation, extending beyond financial fraud into forms of resource theft facilitated by digital technologies.

Theft and hacking of cryptocurrency exchanges constitute one of the most financially devastating categories of blockchain-based crime. Exchanges serve as the primary gateways between fiat currencies and digital assets, making them high-value targets for cybercriminals. Legal analysts examining digital market vulnerabilities note that exchanges often hold large reserves of user funds in centralized wallets, creating opportunities for attackers to exploit security weaknesses (8). Data breaches are among the most common incidents, with attackers infiltrating exchange servers to gain access to private keys or customer records. Phishing schemes also play a significant role, as criminals deceive users into revealing login credentials or authorizing unauthorized transactions. Studies addressing cyber responsibility highlight that even sophisticated users fall victim to social engineering schemes that exploit trust and technical unfamiliarity (11). In many cases, theft occurs through exploitation of smart contract vulnerabilities in decentralized exchanges or lending platforms, where coding errors enable attackers to drain liquidity pools or manipulate token prices. Legal scholars emphasize that the immutability of blockchain transactions makes recovery of stolen assets extremely difficult, as transfers cannot be reversed and criminal wallets can rapidly disperse funds across multiple chains using advanced obfuscation tools (7). The regulatory literature further notes that inconsistent global standards for exchange security and compliance create substantial enforcement gaps, enabling criminals to target platforms in jurisdictions with weaker oversight (9).

The typology of blockchain-based crimes demonstrates that offenders exploit a wide range of technological, regulatory and behavioural vulnerabilities in the digital asset ecosystem. Whether through laundering schemes that obscure financial origins, fraudulent investment schemes that manipulate investor trust, extortion models that capitalize on pseudonymous payments, darknet markets that rely on anonymous transactions, resource-theft malware that abuses computational infrastructure or exchange hacks that compromise massive reserves of digital assets, the criminal exploitation of blockchain technology continues to evolve. These diverse criminal modalities reflect a broader trend in which digital decentralization transforms traditional patterns of offending, enabling large-scale, transnational and technologically sophisticated crimes. Understanding these typologies provides crucial insight into the mechanisms through which offenders operate and highlights the need for strengthened legal frameworks, enhanced technological safeguards and coordinated international enforcement efforts.

Criminological Analysis of Crypto-Crimes

The criminological analysis of crypto-crimes requires an integrated understanding of offender motivations, technological opportunity structures, ecosystem actors and the behavioural patterns emerging within blockchain-enabled illicit activities. As cryptocurrencies reshape digital economies, offenders increasingly view them as ideal instruments for committing, facilitating and concealing criminal operations. The complexity of blockchain systems influences how offenders calculate risks, choose targets and coordinate activities across borders, reflecting a transformation in the nature of criminal decision-making. Criminological frameworks help explain these emerging dynamics by illustrating how technological affordances reshape offending behaviour, lower barriers to participation and amplify opportunities for transnational criminal collaboration.

The motivational structures of offenders engaging in crypto-crime are primarily rooted in economic incentives and favorable risk-reward calculations. For many offenders, the potential for significant financial gain is amplified by the volatility and speculative nature of digital asset markets. Analyses of economic crime within technologically advanced environments show that offenders are drawn to contexts where high-value transactions can be executed with minimal oversight, allowing rapid accumulation of illicit profits (15). Cryptocurrencies serve this purpose by enabling the storage and transfer of value without reliance on regulated financial institutions, making them particularly appealing to individuals seeking quick financial returns outside legal constraints. As digital financial markets evolve, offenders recognize opportunities to exploit price fluctuations, poorly regulated platforms and inexperienced investors, creating a landscape in which fraudulent schemes and market manipulation flourish. Studies examining cyber-driven criminality emphasize that offenders perceive digital markets as fertile environments for illicit gain precisely because the regulatory environment remains fragmented and inconsistent across jurisdictions (9).

The risk-reward calculations that shape offender behaviour are deeply influenced by the structural characteristics of blockchain systems. Offenders rationally assess that cryptocurrencies offer lower risks of detection compared with traditional financial crimes, due in part to pseudonymity and decentralized transaction validation. Scholars analyzing the evolution of cybercrime consistently highlight that offenders choose digital methods when the likelihood of apprehension is perceived to be low relative to potential gains (3). Blockchain technology contributes to this perception by allowing rapid movement of funds through multiple wallets, the use of privacy-enhancing coins and the ability to conduct transactions without revealing personal identity information. Additionally, offenders evaluate the limited capacity of law enforcement to trace complex cross-chain movements, particularly in jurisdictions lacking advanced forensic capabilities. Legal analyses emphasize that the immutability of blockchain records, while useful for transparency, creates an irreversible trail that offenders can exploit by quickly dispersing funds before law enforcement can intervene (17). These structural properties reduce perceived risks and reinforce offender confidence in cryptocurrency-based operations, shaping their decision to engage in a broad range of blockchain-enabled crimes.

Opportunity structures created by blockchain technology significantly expand the environments in which offenders operate. Cryptocurrencies offer anonymity and pseudonymity that are difficult to replicate in traditional financial systems. Offenders exploit these features by masking their identities through encrypted wallets, decentralized exchanges and mixing services. Scholars examining the misuse of virtual assets point to anonymity as one of the primary opportunity structures enabling money laundering, fraud and illicit market operations (1). The

speed of cryptocurrency transactions further enhances these opportunities. Funds can be transferred across borders within seconds, reducing the window for detection and intervention. Analyses of transnational cybercrime highlight that this transactional speed allows offenders to rapidly move illicit proceeds across multiple jurisdictions, significantly complicating coordination among enforcement agencies (11). Jurisdictional ambiguity also plays a critical role. Blockchain networks operate globally, without clear geographic boundaries, meaning that offenders can exploit differences in regulatory frameworks and legal systems. Legal scholars emphasize that many states lack harmonized policies for digital asset oversight, allowing offenders to take advantage of weak regulatory environments or jurisdictions with minimal cooperation agreements (21). This ambiguity creates a fragmented enforcement landscape where offenders can operate with reduced fear of prosecution.

Beyond technological affordances, the ecosystem of actors involved in crypto-crime significantly influences the structure and evolution of blockchain-enabled offences. Developers play a critical role, both intentionally and unintentionally. Some developers create malicious smart contracts, fraudulent decentralized applications or deceptive platforms designed to defraud users. Analyses of smart contract legality highlight that poorly coded or intentionally manipulated contracts can generate automatic transfers that enable rug pulls, liquidity theft and unauthorized asset extractions (19). Intermediaries also contribute to the ecosystem. These include crypto-exchange operators, OTC brokers and liquidity providers who may either knowingly facilitate illicit transactions or inadvertently enable them through insufficient compliance processes. Legal discussions of digital market vulnerabilities note that exchanges in weakly regulated jurisdictions often become hubs for money laundering and illicit transactions due to inadequate oversight (8). Online forums and communication platforms play another crucial role by connecting offenders, enabling the exchange of technical knowledge, selling illegal tools and coordinating attacks. Studies examining cybercrime communities show that online networks facilitate the dissemination of malware, ransomware kits and fraudulent investment templates, empowering less skilled individuals to participate in sophisticated crypto-crimes (2). Illicit service providers also shape the ecosystem by offering laundering services, anonymous hosting, phishing kits, hacked accounts and other resources required to execute crypto-related crimes. Their presence transforms the criminal landscape into a highly organized marketplace where offenders can acquire the tools needed to engage in illicit operations.

Trends, patterns and behavioural profiles in crypto-crime illustrate the increasing professionalization and global interconnectedness of blockchain-enabled offences. Organized cybercrime groups have become central actors in this space, developing specialized teams responsible for different aspects of criminal operations. Legal analysts examining the evolution of criminal organizations note that these groups now employ programmers, finance specialists, social engineers and laundering experts to execute coordinated attacks that exploit blockchain systems (4). Ransomware syndicates, in particular, exemplify this sophistication, as they rely on complex infrastructures for malware deployment, negotiation management and cryptocurrency laundering. Their operations are often supported by dark web forums that provide training, technical support and revenue-sharing agreements, further enhancing their operational capacity. Studies of transnational criminal networks emphasize that these groups strategically exploit jurisdictions with limited cyber enforcement capacities, enabling them to distribute responsibilities across borders and reduce the risks associated with prosecution (14).

Cross-border criminal networks represent another defining trend. Cryptocurrencies facilitate seamless international collaboration by enabling offenders in different countries to coordinate activities without relying on traditional financial institutions. Analyses of cyber-enabled crime highlight that blockchain technology dissolves

geographic barriers, allowing individuals from disparate regions to participate in shared criminal operations such as laundering schemes, global phishing campaigns and coordinated exchange hacks (11). These networks often involve loosely connected actors who contribute to criminal operations without centralized leadership structures, reflecting the decentralized nature of the technology they exploit. Legal commentators emphasize that this decentralization makes enforcement exceptionally difficult, as no single jurisdiction can address the full scope of cross-border operations, and cooperation mechanisms often lag behind technological developments (7). In some cases, offenders take advantage of geopolitical tensions, operating from regions that refuse to cooperate with international cybercrime investigations. This strategic exploitation of global legal disparities underscores the importance of international collaboration in addressing crypto-related crime.

The behavioural profiles of offenders involved in blockchain-enabled crimes reveal a continuum ranging from opportunistic individuals to highly skilled professional groups. Opportunistic offenders often engage in scams, phishing attacks or small-scale laundering operations, exploiting gaps in public knowledge and regulatory oversight. Analyses of digital financial deception demonstrate that these offenders typically rely on social engineering, deceptive marketing or fraudulent investment schemes to deceive victims in the rapidly expanding crypto-market (5). More advanced offenders demonstrate deep technical expertise, using coding skills, cryptographic knowledge and penetration techniques to exploit vulnerabilities in exchanges, smart contracts and wallet infrastructures. Legal studies emphasize that these actors are often responsible for large-scale breaches and thefts that result in multimillion-dollar losses across international markets (8). Many of these offenders operate within collaborative networks, exchanging tools, strategies and anonymization techniques through online platforms that accelerate the diffusion of criminal innovations.

Overall, the criminological dynamics of crypto-crime reveal a complex interplay between offender motivations, technological affordances, structural opportunities and evolving criminal networks. Economic incentives drive offenders to exploit blockchain systems, while reduced perceived risks and heightened rewards encourage broader participation in illicit activities. The opportunity structures embedded in blockchain's architecture create environments in which anonymity, speed and jurisdictional ambiguity facilitate cross-border crime. A diverse ecosystem of actors—including developers, intermediaries, online communities and illicit service providers—forms the backbone of digital criminal markets. Finally, the trends and behavioural patterns emerging in crypto-crime reflect the increasing sophistication, global reach and adaptability of offenders who capitalize on the decentralized and rapidly evolving nature of blockchain technology.

Challenges of Detecting and Prosecuting Blockchain-Based Crimes

The detection and prosecution of blockchain-based crimes present a complex array of legal, technical and criminological challenges that distinguish them from traditional forms of offending. Cryptocurrencies and decentralized platforms create environments in which offenders can operate with a degree of anonymity, speed and transnational reach that far exceeds the constraints of conventional financial systems. These characteristics undermine established investigative frameworks, strain legal doctrines and complicate the work of regulatory bodies across jurisdictions. As blockchain technology evolves, so too do the strategies used by criminals to evade monitoring, obscure digital traces and exploit systemic gaps in law enforcement capacity. The resulting challenges highlight the need for a nuanced understanding of the multifaceted obstacles that impede effective detection and prosecution.

One of the most persistent barriers for investigators is the anonymity and pseudonymity embedded in blockchain systems. Although blockchain transactions are publicly recorded, the identities behind digital wallet addresses are typically hidden, creating a disjunction between observable financial activity and the ability to attribute it to specific individuals. Scholars analyzing virtual asset misuse emphasize that anonymity constitutes one of the primary enablers of sophisticated laundering schemes, fraud operations and illicit marketplaces operating on the darknet (1). Privacy-enhancing coins intensify this problem. Unlike Bitcoin, which allows some degree of traceability through publicly visible addresses, privacy coins such as Monero, Dash and Zcash deploy ring signatures, stealth addresses and zero-knowledge proofs that intentionally obscure sender and receiver information. Legal studies highlight that privacy-enhancing coins are increasingly used in laundering processes precisely because their cryptographic design frustrates conventional forensic tracing (14). Obfuscation techniques further complicate attribution. Offenders routinely rely on mixers, tumblers and cross-chain bridges to break transactional linkages, spreading illicit funds across multiple blockchains and wallets. Analyses of digital crime evolution emphasize that such tools allow criminals to erase transactional patterns before investigators can detect or freeze assets, thereby reducing the evidentiary trail available for prosecution (2). As these privacy-enhancing features become more sophisticated, law enforcement agencies face growing difficulty in establishing the identity of offenders or the origins of illicit funds.

Jurisdictional and territorial challenges exacerbate the difficulty of enforcing laws against blockchain-based crime. Blockchain networks operate without regard for national borders, allowing transactions to flow freely between jurisdictions with varying legal frameworks and enforcement capacities. Scholars examining the transnational dimensions of cybercrime emphasize that borderless cryptocurrency transactions undermine traditional territorial assumptions in criminal law by enabling offenders to operate from jurisdictions with weak regulatory controls or limited cooperation with foreign authorities (11). This borderless nature creates profound challenges for initiating investigations, securing evidence and asserting prosecutorial authority. Conflict-of-laws issues arise as states attempt to determine which jurisdiction has the legal authority to prosecute a given offence, particularly when a victim, offender and digital infrastructure are located in different countries. Legal analyses highlight that differing definitions of cybercrime, inconsistent regulatory standards and conflicting evidentiary requirements complicate international collaboration and lead to enforcement gaps that offenders strategically exploit (21). The absence of harmonized extradition agreements for digital offences further hinders the ability of law enforcement to apprehend suspects operating overseas. As a result, many offenders deliberately situate themselves in jurisdictions unlikely to cooperate with foreign investigations, leveraging geopolitical barriers to avoid prosecution.

Evidentiary challenges form another crucial obstacle in blockchain-based criminal cases. The digital nature of cryptocurrency transactions raises complex questions regarding the collection, preservation and admissibility of evidence. Scholars examining digital crime prosecution emphasize that maintaining a secure chain of custody for digital evidence is significantly more difficult than for physical evidence, given the ease with which digital files can be altered, deleted or corrupted (17). Blockchain data itself is immutable, but the devices, logs and external systems involved in cryptocurrency use are not. Investigators must ensure that seized wallets, servers and digital devices are preserved without tampering, a task that often requires advanced technical expertise. The volatility of cryptoassets introduces another evidentiary complication. Cryptocurrency values can fluctuate dramatically within hours, complicating efforts to determine the monetary value of assets relevant to charges, sentencing or restitution. Legal studies addressing digital financial crime note that prosecutors must often rely on historical price data to estimate asset value, a process that introduces subjectivity and legal debate (5). Limited access to private keys

represents an additional barrier. Without a suspect's private key, authorities may be unable to access or freeze digital funds, even when they have legal authority to do so. Research analyzing digital asset enforcement highlights that offenders frequently destroy or conceal private keys to prevent recovery, a tactic that effectively shields illicit assets from seizure (7).

Forensic and technical barriers present further difficulties for investigators attempting to trace blockchain transactions or analyze smart contract-based crimes. Blockchain forensics—although advancing rapidly—still faces significant limitations. Scholars studying digital asset enforcement emphasize that forensic tools are often unable to trace transactions that pass through privacy-enhancing protocols, mixers or decentralized exchanges, where user verification requirements are minimal or nonexistent (1). Even when forensic tools can map some transactional flows, they may be unable to identify the ultimate beneficial owner of a wallet, especially when actors use chains of intermediary addresses, encrypted communication channels or anonymous browsing tools. The complexity of smart contracts compounds these issues. Smart contracts are self-executing programs written in code that automatically implement transactional conditions. Legal analyses highlight that vulnerabilities in this code can lead to large-scale thefts, liquidity manipulation or unauthorized transfers, yet attributing liability in such cases is difficult because it may be unclear whether the exploit resulted from user error, coding flaws or deliberate manipulation (19). The decentralized nature of many smart contract platforms means that there is no centralized authority responsible for correcting vulnerabilities or reversing exploitative transactions. Researchers studying the evolution of digital-era criminal behaviour note that smart contract complexity allows offenders to deploy sophisticated attacks that exploit minor coding errors, often draining millions of dollars before detection (4). These technical challenges require specialized expertise that many law enforcement agencies lack, contributing to delays and failures in prosecution.

The regulatory and legal gaps surrounding blockchain-based crimes create another layer of difficulty for detection and prosecution. The global regulatory environment for cryptocurrencies remains inconsistent, fragmented and often underdeveloped. Scholars examining criminal law reform emphasize that rapid technological innovation has outpaced legal adaptation, leaving many jurisdictions without clear statutory provisions addressing digital assets, smart contracts or decentralized finance operations (8). The lack of harmonized global regulations creates opportunities for regulatory arbitrage, as offenders exploit jurisdictions with weak oversight or minimal compliance requirements. Differences in anti-money-laundering (AML) and know-your-customer (KYC) frameworks further contribute to this disparity. Legal studies highlight that some jurisdictions impose strict KYC obligations on crypto-exchanges, requiring identity verification and suspicious activity reporting, while others allow exchanges to operate without meaningful oversight (9). These inconsistencies create choke points where offenders can easily transfer funds from regulated environments into unregulated or lightly regulated zones, effectively neutralizing enforcement attempts. The absence of consistent reporting standards, registration requirements or compliance mechanisms for decentralized finance platforms further exacerbates these enforcement gaps. Analysts examining cross-jurisdictional enforcement note that even when laws exist, enforcement capacity varies widely, with many states lacking forensic expertise, digital infrastructure or adequate training for investigators (11). As a result, the global regulatory landscape remains fragmented, allowing blockchain-enabled crimes to flourish.

These regulatory gaps not only hinder detection but also create challenges during prosecution. Courts must grapple with questions regarding the legal status of digital assets, the enforceability of smart contracts and the criminal liability of actors operating within decentralized ecosystems. Scholars examining digital contract systems emphasize that traditional legal doctrines—such as mens rea, intent and causation—are difficult to apply in cases

involving automated code, decentralized platforms or anonymous actors (19). In some jurisdictions, legislation does not yet recognize digital assets as property, complicating charges related to theft or fraud. Even when digital asset statutes exist, prosecutors may struggle to demonstrate criminal intent when transactions occur automatically through code or when actors claim that exploits were merely technical manipulations rather than criminal acts. These doctrinal uncertainties weaken prosecutorial efforts and create ambiguities that defense attorneys can exploit.

Overall, the detection and prosecution of blockchain-based crimes are hindered by a convergence of anonymity features, transnational complexities, evidentiary limitations, forensic challenges and regulatory inconsistencies. Privacy-enhancing technologies and obfuscation tools obscure digital identities, while borderless networks undermine territorial jurisdiction and create conflict-of-laws dilemmas. Digital evidence requires specialized handling, and the volatility of cryptoassets complicates valuation and recovery. Forensic tools struggle to trace obfuscated transactions or interpret smart contract exploits, and legal frameworks remain fragmented and outdated. These combined challenges illustrate the profound difficulties faced by investigators, prosecutors and regulators seeking to address blockchain-based crime, underscoring the need for coordinated legal reform, enhanced forensic capacities and strengthened international cooperation.

Responses and Policy Frameworks

Responding effectively to blockchain-based criminality requires an integrated framework that combines technological innovation, regulatory adaptation, international cooperation and enhanced enforcement capabilities. As cryptocurrencies reshape the global financial landscape, policymakers and enforcement bodies must develop strategies that address both the technological complexity of decentralized systems and the criminological dynamics associated with digital offending. These responses must be multidimensional because blockchain crimes transcend geographic borders, exploit regulatory inconsistencies and leverage cryptographic tools that obscure criminal identities. A coordinated policy approach is essential to counteract the expanding sophistication of offenders and the systemic vulnerabilities within the digital asset ecosystem.

Technological approaches form the first pillar of modern strategies against blockchain-enabled crime. Blockchain forensics has become an indispensable component of investigative practice, relying on advanced analytic techniques to trace digital transactions across otherwise pseudonymous networks. Scholars examining crime in digital markets underline that blockchain forensics provides one of the few viable methods for mapping illicit financial flows, even when offenders use complex obfuscation techniques (1). These forensic systems work by analyzing transaction histories, clustering wallet addresses and identifying behavioural patterns consistent with laundering, fraud or illicit transfers. Analytics tools have evolved significantly, allowing investigators to correlate blockchain activity with off-chain indicators such as IP addresses, exchange accounts or metadata logs. Legal research emphasizing the evolution of cybercrime illustrates how these tools enable law enforcement to uncover laundering channels, map darknet payment networks and identify the infrastructure used by ransomware operators (11). Artificial intelligence–based transaction tracing represents a further advancement, with machine learning models capable of detecting anomalous patterns, predicting laundering pathways and identifying high-risk addresses with greater accuracy. Scholars discussing the adaptation of criminal law to digital contexts highlight that AI systems can dramatically reduce the human workload associated with blockchain analysis, enabling investigators to track vast volumes of transactions that would otherwise be impossible to process manually (4). As offenders increasingly

adopt advanced privacy solutions, these technological tools provide the foundation for maintaining investigative relevance in an ever-shifting digital environment.

Legal and regulatory responses constitute the second essential component of an effective policy framework. Anti-money-laundering and counter-financing of terrorism (AML/CFT) regulations are critical for addressing the misuse of cryptocurrencies in laundering operations and terror financing schemes. Analysts examining financial crime enforcement emphasize that applying AML/CFT controls to crypto-exchanges, wallet providers and decentralized platforms is necessary to ensure transparency, accountability and reporting of suspicious transactions (9). These measures commonly require identity verification, transaction monitoring and record-keeping obligations that align digital asset service providers with traditional financial institutions. Licensing and registration of crypto-exchanges represent an important extension of AML frameworks. Scholars analyzing regulatory gaps highlight that jurisdictions with robust licensing systems reduce opportunities for criminals to exploit poorly regulated exchanges, forcing service providers to comply with strict operational and cybersecurity standards (8). Licensing regimes often require exchanges to implement stringent KYC protocols, maintain audit-ready transaction logs and enforce continuous compliance checks to prevent misuse.

The role of the Financial Action Task Force (FATF) is central to these regulatory efforts. FATF recommendations provide global standards for assessing and mitigating risks associated with virtual assets, urging member states to implement risk-based approaches to supervision, monitoring and enforcement. Legal analyses discussing cross-border financial crime emphasize that FATF's "travel rule"—requiring the exchange of identifying information between virtual asset service providers—plays a critical role in reducing pseudonymity and disrupting laundering channels (21). By promoting harmonized international frameworks, FATF guidelines help reduce regulatory disparities between jurisdictions, limiting regulatory arbitrage and making it more difficult for offenders to exploit weak legal environments. Scholars examining digital asset enforcement underscore that widespread adoption of FATF standards enhances global resilience against crypto-crime and strengthens the coherence of international regulatory regimes (7).

International cooperation is the third critical dimension of effective response frameworks, given the inherently transnational nature of blockchain-based crime. Crypto-crimes frequently involve offenders, victims, servers and financial flows distributed across multiple jurisdictions, making inter-agency coordination essential for meaningful enforcement. Studies on transnational digital crime emphasize that coordinated investigative mechanisms—such as joint task forces, shared intelligence databases and cross-border rapid response protocols—are necessary to address crimes that cannot be prosecuted effectively within isolated national systems (11). Inter-agency cooperation enables the pooling of technical resources, the sharing of investigative expertise and the harmonization of procedural standards for handling digital evidence. These collaborative structures also play a role in identifying and dismantling global ransomware networks, darknet marketplaces and transnational laundering operations. Effective cross-border investigation mechanisms require strong diplomatic frameworks, cooperative legal instruments and international agreements that facilitate the exchange of information, extradition of suspects and coordinated asset seizure efforts. Legal studies highlight that inconsistencies in national cyber laws hinder cross-border investigations, making international harmonization a necessary precondition for effective digital crime enforcement (21). Mutual legal assistance treaties (MLATs), regional cybercrime conventions and real-time information sharing platforms provide essential infrastructure for bridging the investigative gap between jurisdictions.

Law enforcement capacity building forms the final, and arguably most critical, layer of blockchain crime responses. As digital assets become mainstream, enforcement agencies must acquire advanced training, technological literacy and specialized operational units capable of addressing the complexities of blockchain investigations. Scholars examining criminal justice adaptation emphasize that digital literacy is no longer optional; investigators must understand blockchain mechanics, wallet technologies, smart contracts and the behavioural strategies used by offenders in decentralized systems (2). Capacity building involves training officers to use blockchain forensic tools, interpret analytic dashboards and manage digital evidence in a legally defensible manner. Specialized crypto-crime units are increasingly necessary to handle sophisticated investigations such as smart contract exploits, exchange breaches or multi-chain laundering schemes. Legal research underscores that these units benefit from multidisciplinary structures that integrate programmers, forensic analysts, legal experts and financial investigators to address the full spectrum of crypto-crime dynamics (4). Enhanced training also supports the development of competent prosecutors who understand the technological context of digital asset cases and can present complex evidence persuasively in court. Studies on digital enforcement reform emphasize that law enforcement agencies lacking dedicated training and specialized units are unable to respond effectively to rapidly evolving blockchain-based threats (17).

Capacity building also requires investment in institutional infrastructure. Agencies must acquire advanced forensic software, secure data storage facilities for seized digital evidence and high-performance computing systems capable of analyzing blockchain networks at scale. Legal and criminological research highlights that resource disparities between countries result in uneven enforcement capacities, creating safe havens where offenders can operate with limited risk of prosecution (14). To bridge this gap, international support programs, technical assistance initiatives and cross-border research collaborations are increasingly important. These initiatives enhance the ability of under-resourced jurisdictions to participate in global enforcement efforts, reducing the systemic weaknesses that criminals often exploit.

Together, these technological, regulatory, cooperative and capacity-building approaches illustrate a comprehensive framework for responding to blockchain-based crime. Advanced forensic tools and AI systems provide the technological backbone for tracing illicit transactions. Regulatory reforms ensure stronger oversight through licensing, AML/CFT compliance and FATF-aligned standards. International cooperation offers a mechanism for addressing borderless crime through shared intelligence and coordinated investigations. Capacity building empowers law enforcement agencies with the specialized skills and infrastructures required to prosecute technologically sophisticated offences. Although significant challenges remain, these integrated responses represent the most promising path toward establishing an effective global framework for addressing the rapidly evolving landscape of crypto-crime.

Conclusion

The expansion of blockchain technology and cryptocurrencies has introduced a new era of digital transformation in which financial innovation and criminal exploitation evolve in parallel. The conclusion of this narrative review highlights the fundamental realities shaping the contemporary landscape of crypto-crime and underscores the necessity of adopting multidimensional approaches to address its complexities. Cryptocurrencies have redefined the boundaries of financial systems by enabling decentralized, pseudonymous, borderless transactions that operate independently of traditional regulatory and institutional frameworks. These features, while beneficial in many

legitimate contexts, also create fertile conditions for criminal misuse. As a result, blockchain ecosystems have become host to a wide range of illicit activities, including money laundering, fraud, ransomware, darknet market transactions, illicit mining operations and large-scale exchange thefts. Each category of crime demonstrates how offenders strategically exploit the technological characteristics and systemic weaknesses inherent to decentralized networks.

Understanding these developments requires a criminological lens capable of explaining offender motivations, decision-making processes and behavioural adaptations. Offenders are drawn to cryptocurrencies not only for their financial potential but also for the reduced risks associated with anonymity, transaction speed and jurisdictional ambiguity. The decentralized nature of blockchain systems offers structural opportunities for evasion that traditional financial systems do not provide. As offenders become more technologically sophisticated, they incorporate advanced obfuscation techniques, privacy-enhancing tools and cross-border operational strategies that challenge conventional models of investigation and prosecution. Criminal networks increasingly organize themselves in flexible, transnational formations that leverage online platforms, encrypted communication channels and decentralized infrastructures. These behavioural and structural shifts illustrate the profound transformation taking place within the broader field of digital criminality.

The challenges facing law enforcement and regulatory bodies stem directly from the core characteristics of blockchain technology. Investigators must contend with pseudonymous transactions, the proliferation of privacy coins, the irreversible nature of blockchain records and the widespread use of mixers and tumblers that obscure transactional pathways. Jurisdictional uncertainty poses additional obstacles, as the global, non-territorial operation of blockchain networks disrupts traditional assumptions about territorial legal authority. Prosecutors frequently encounter evidentiary difficulties, including problems with establishing digital chains of custody, valuing volatile assets and accessing private keys required for asset seizure. Forensic limitations further complicate these efforts, especially when smart contract complexity or cross-chain operations restrict the ability to trace or interpret activity. Regulatory frameworks have also lagged behind technological developments, resulting in fragmented global policies that create inconsistent enforcement environments and opportunities for regulatory arbitrage.

Despite these challenges, the review also demonstrates that effective responses are emerging across multiple domains. Technological advancements in blockchain forensics, data analytics and AI-driven transaction tracing offer powerful tools for mapping illicit flows, identifying suspicious patterns and supporting investigative work that would otherwise be impossible at scale. Regulatory strategies, such as enhanced AML/CFT requirements, licensing of digital asset service providers and the implementation of global standards, represent critical steps toward mitigating systemic risks. International cooperation has become essential, fostering shared investigative strategies, intelligence exchange and coordinated enforcement operations across borders. Capacity building within law enforcement agencies—including specialized units, improved digital literacy and increased institutional resources—further strengthens the ability of states to address the growing sophistication of crypto-crime.

Ultimately, the criminological analysis presented throughout this review demonstrates that no single approach is sufficient to address the multifaceted nature of blockchain-enabled crime. Instead, an integrated strategy that combines technological innovation, legal reform, international coordination and enhanced enforcement capacity is necessary. The complexity of crypto-crime lies not only in its technical dimensions but also in the behavioural, structural and transnational dynamics that shape how offenders operate. As blockchain technology continues to

develop and expand into new sectors, these criminal modalities will evolve in parallel, creating ongoing challenges for policymakers, regulators and investigators.

The conclusion reinforces the need for proactive, forward-looking strategies that anticipate future developments in both technology and criminal adaptation. Continued research, cross-disciplinary collaboration and global regulatory harmonization are essential to building resilient frameworks capable of protecting digital economies while preserving the legitimate benefits of blockchain innovation. This narrative review highlights that the fight against crypto-crime is not simply a matter of policing a new form of financial transaction; it is a comprehensive effort to understand and respond to a rapidly transforming digital ecosystem that influences economic practices, criminal behaviour and societal risk at a global scale.

Acknowledgments

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

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

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

Transparency of Data

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

Funding

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

References

1. Koutsoupia V. Challenges of the Use of Virtual Assets in Money Laundering. Nordic Journal of European Law. 2023;6(4):53-78. doi: 10.36969/njel.v6i4.25919.
2. Mulyana Y. Cybercrime and Transnational Criminal Law: Tackling Online Fraud and Identity Theft. Jurnal Nawala. 2025;2(8):75-85. doi: 10.62872/zep90829.
3. Singh S, Pandey S. The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws. International Journal for Multidisciplinary Research. 2025;7(2). doi: 10.36948/ijfmr.2025.v07i02.41627.
4. Krasko MI, Tsevukh A. Evolution of Cybercrime: How Criminal Law Adapting to the Digital Era? Analytical and Comparative Jurisprudence. 2025;2(3):387-93. doi: 10.24144/2788-6018.2025.03.2.63.
5. Mina-Bone SG. Evolución Del Derecho Penal Económico Frente a Los Delitos Financieros Digitales. Revista Científica C&M. 2024;2(3):52-66. doi: 10.55813/gaea/rcym/v2/n3/50.

6. Rusmana IPE, Novelin T. Legal Analysis of Criminal Responsibility for Hackers From the Perspective of Cyber Law in Indonesia. Jihad Jurnal Ilmu Hukum Dan Administrasi. 2024;6(4). doi: 10.58258/jihad.v6i4.7676.
7. Atiyah GA, Ibrahim AI, Jasim AA. Enforcement of Smart Contracts in Cross-Jurisdictional Transactions. International Journal of Law and Management. 2024. doi: 10.1108/ijlma-06-2024-0220.
8. Lubis J. The Urgency of Criminal Law Reform to Adapt to the Development of Information Technology. International Journal of Advanced Research. 2025;1(6):287-95. doi: 10.61730/6wxx1c52.
9. Saxena A, Dhaka N. Corporate Criminal Liability: An Indian Perspective. Ijgrit. 2025;03(03):27-40. doi: 10.62823/ijgrit/03.03.7886.
10. Lubis MA, Syaputra MYA. Design of Election Criminal Enforcement Through a Restorative Justice Approach in Nort Sumatra. Jurnal Mercatoria. 2024;17(1):95-107. doi: 10.31289/mercatoria.v17i1.11989.
11. Movchan A, Shliakhovskyi O, Kozii V, Fedchak I. Investigating Cryptocurrency Financing Crimes Terrorism and Armed Aggression. Соціально-Правові Студії. 2023;6(4):123-31. doi: 10.32518/sals4.2023.123.
12. Stepashin VM. The Criminal Code of Mongolia. The General Part. Crime. Law Enforcement Review. 2024;8(3):142-51. doi: 10.52468/2542-1514.2024.8(3).142-151.
13. Tarigan EH, Saragih YM. Legal Analysis of Corporate Criminal Liability in Oil and Gas Sector Crimes in Indonesia. Jurnal Riset Rumpun Ilmu Sosial Politik Dan Humaniora. 2024;3(3):36-45. doi: 10.55606/jurrish.v3i3.6405.
14. Harefa JE, Rahmayanti R, Siswanto E, Rozy F, Sihite INP. Jurisdictional Enforcement of Cyber Crime Against Lottery Scam. Ijls. 2025;2(3):165-9. doi: 10.62951/ijls.v2i3.675.
15. Prabowo D, Saragih YM, Hadi MFA, Emri SI, Sianipar KRD. Implementation of Corporate Criminal Accountability in Indonesian National Economic Crime. Jurnal Riset Rumpun Ilmu Sosial Politik Dan Humaniora. 2025;4(3):743-8. doi: 10.55606/jurrish.v4i3.5998.
16. Romas IO. Subject of Escape From Places of Detention: Characteristics and Ways to Improve Normative Regulation. Теория И Практика Общественного Развития. 2024(11):264-9. doi: 10.24158/tipor.2024.11.32.
17. Rusman R, Fakrulloh ZA. Reform of Law Enforcement to Strengthen the Legal System in Eradicating Money Laundering Through Cryptocurrency Investments. Journal of Social Research. 2024;4(1):1-15. doi: 10.55324/josr.v4i1.2332.
18. Bentara B, Iskandar I, Setianingrat E, Permana DY, Dikrurahman D. Legal Responsibility for Perpetrators of Online Gambling Crimes. Journal of World Science. 2025;4(5):512-21. doi: 10.58344/jws.v4i5.1408.
19. Baso F, Yusuf DU, Djaoe ANM, Iswandi I, Ramadhany A. Overview of Smart Contract: Legality and Enforceability. Dialogia Iuridica. 2024;16(1):096-111. doi: 10.28932/di.v16i1.10024.
20. Dave E. Smart Contracts and AI: The Legal Landscape of Autonomous Transactions. 2025. doi: 10.31219/osf.io/m2pt4_v1.
21. Tarigan EH, Saragih YM. Corporate Criminal Liability in Oil and Gas Sector Crimes in Indonesia. Jurnal Riset Rumpun Ilmu Sosial Politik Dan Humaniora. 2024;3(3):53-62. doi: 10.55606/jurrish.v3i3.6475.
22. Handaruan FDY. Illegal Fishing: Analysis of MV Nika Case in International Criminal Law Perspective. International Law Discourse in Southeast Asia. 2024;3(2). doi: 10.15294/ildisea.v3i2.35124.
23. Minggu SH, Dm MY, Pardede R. Law Enforcement Against Palm Oil Theft. Jilpr Journal Indonesia Law and Policy Review. 2025;6(3):617-30. doi: 10.56371/jirpl.v6i3.460.
24. M AY, Hardianto S. The Role of Criminal Law in Combating Corporate Crime That Harms the Public Interest. Global. 2024;2(11):2616-25. doi: 10.59613/global.v2i11.364.