JELS Journal of Economics, Law & Society

ESREIN Economic and Social Research Institute

Decentralized Crime: Fraud, Cybercrime, and Legal Enforcement

Hazik Mohamed
Stellar Consulting Group, Singapore
ORCID ID: 0000-0001-8322-2714
Email: hazik@stellarcg.com

Abstract

The rapid rise of Decentralized Finance (DeFi) and anonymity-focused cryptocurrencies has transformed financial systems by eliminating intermediaries and enabling peer-to-peer transactions. While these innovations offer numerous benefits, they also present unprecedented challenges for crime prevention and regulatory enforcement. This paper examines how DeFi and privacy-enhanced cryptocurrencies, such as Monero and Zcash, facilitate financial crimes, including money laundering, ransomware attacks, and fraud. By applying criminological theories—Strain Theory, Routine Activity Theory, and Rational Choice Theory—this study reinterprets traditional crime models in the context of blockchain-based financial ecosystems. Law enforcement agencies face significant hurdles in investigating and prosecuting crypto-enabled financial crimes due to jurisdictional limitations, privacy-enhancing technologies, and decentralized governance. This paper explores how blockchain analytics, artificial intelligence-driven risk assessment, and cross-border regulatory collaborations, such as the Financial Action Task Force (FATF) Travel Rule and the EU's Markets in Crypto-Assets (MiCA) regulation, are being developed to counter these emerging threats. Additionally, it assesses the institutional limitations of law enforcement agencies, the role of DeFi governance communities in mitigating financial crimes, and the potential impact of central bank digital currencies (CBDCs) on reducing illicit transactions. To enhance regulatory effectiveness, this study recommends strengthening international cooperation, improving forensic capabilities for tracking illicit blockchain transactions, and implementing ethical frameworks that balance financial privacy with security. The findings contribute to criminology, financial regulation, and cybersecurity by offering insights into evolving digital crimes and proposing solutions to mitigate their risks. Future research should explore the role of artificial intelligence in DeFi crime detection and the impact of regulatory advancements on illicit financial flows in decentralized ecosystems.

Article History

Received: September 15, 2025
Accepted: November 26, 2025
Published: December 30, 2025

Keywords

blockchain forensics; criminal theory; cryptocurrency regulation; decentralized finance; financial crime.

JEL Codes

D81; G28; K42; O33;

How to Cite

Mohamed, H. (2025). Decentralized Crime: Fraud, Cybercrime, And Legal Enforcement. *Journal of Economics, Law and Society, 2(2)*, 5-22. https://doi.org/10.70009/jels.2025.2.2.1

1. Introduction

1.1. Background and Context

Decentralized Finance (DeFi) has emerged as a disruptive force in the financial industry, utilizing blockchain technology to build an open and permissionless financial ecosystem. DeFi uses smart contracts and decentralized applications (DApps) to replicate and improve traditional financial services including lending, borrowing, and trading without the need for centralized middlemen (Zreik, 2024). This paradigm shift has been paralleled by the emergence of anonymity-focused cryptocurrencies, sometimes known as privacy coins, which prioritize user secrecy by obscuring

transaction details. Cryptocurrencies like Monero and Zcash use advanced cryptographic algorithms to ensure that transaction data remains hidden, making them appealing to users wanting increased privacy (The CEO Views, 2024).

The advent of DeFi and privacy coins has caused considerable disruptions in traditional banking systems and established criminal prevention frameworks. Traditional financial institutions operate in regulated environments, using Know Your Customer (KYC) and Anti-Money Laundering (AML) standards to detect and prevent fraudulent activity. In contrast, DeFi services frequently operate without centralized oversight, allowing users to conduct financial transactions anonymously. This decentralization calls into question traditional regulatory paradigms, as the lack of middlemen makes compliance procedures more difficult to enforce (Bank of Canada, 2023).

Furthermore, the inclusion of privacy coins in DeFi platforms exacerbates these issues by giving users tools for conducting transactions that are resistant to traditional tracking and surveillance methods. The concealment of transaction details inhibits law enforcement authorities' capacity to trace funds, therefore creating a conducive environment for illicit financial activities (Europol, 2020).

The pseudonymous character of cryptocurrencies, along with the privacy features of certain digital assets, has resulted in their increased use in crimes and fraud schemes. Criminal groups use these technologies to assist money laundering, ransomware attacks, and the online sale of illegal goods and services. For example, the Financial Action Task Force (FATF) has documented an increase in cyber-enabled fraud schemes that trick victims into transferring funds using fraudulent cryptocurrency platforms (FATF, 2023).

High-profile incidents highlight the gravity of this problem. In February 2025, the cryptocurrency exchange Bybit was subjected to a sophisticated phishing attack that resulted in the theft of more than $1.4 billion in Ethereum tokens. The attackers used false interfaces to acquire illegal access to the exchange's wallet management system and then transferred the assets to unknown wallets. The Lazarus squad, a North Korean cyber squad, is suspected of orchestrating the crime and using innovative tactics to conceal the stolen assets (El País, 2025).

These changes underscore the critical need for a rethinking of old criminological theories and law enforcement techniques in the face of decentralized and privacy-enhancing financial technologies. As DeFi and anonymity-focused cryptocurrencies expand, it is critical to understand the implications for financial crime and establish robust risk mitigation procedures.

1.2. Research Questions and Objectives

The proliferation of Decentralized Finance (DeFi) platforms and anonymity-focused cryptocurrencies has introduced complexities that challenge existing frameworks in criminology and law enforcement. This study aims to address the following research questions:

i. How do DeFi and anonymity-focused cryptocurrencies challenge traditional criminological theories?
ii. What are the implications of decentralized financial crimes for law enforcement?
iii. How can existing and emerging forensic methods counter crypto-enabled crimes?

1.3. Significance of the Study

This research holds substantial significance across multiple domains:

i. Criminology: By examining how DeFi and anonymity-focused cryptocurrencies intersect with criminal behavior, this study contributes to the evolution of criminological theories in the digital age, addressing gaps in understanding related to cyber-enabled financial crimes.
ii. Cybersecurity: Insights from this research inform the development of security measures aimed at detecting and preventing the exploitation of decentralized financial systems by malicious actors, thereby enhancing the resilience of digital financial infrastructures.
iii. Financial Regulation: The findings provide valuable perspectives for regulators seeking to craft policies that balance innovation in financial technologies with the imperative to prevent and mitigate financial crimes, ensuring that regulatory frameworks remain effective in the face of evolving technologies.
iv. Law Enforcement: By identifying the challenges and proposing ideas related to investigating crimes involving DeFi and anonymity-focused cryptocurrencies, this study aids law enforcement agencies in adapting to the complexities of the modern financial crime landscape, promoting more effective investigative and prosecutorial practices.

This research endeavours to bridge the knowledge gap at the intersection of decentralized financial technologies and criminal activity, offering foundational insights for theory and policy considerations.

2. The Role of DeFi and Anonymity-Focused Cryptocurrencies in Financial Crime

2.1. Defining DeFi and Anonymity-Centric Cryptocurrencies

Decentralized Finance (DeFi) is a paradigm change in the financial industry that uses blockchain technology to provide financial services without traditional intermediaries. DeFi relies heavily on smart contracts, which are self-executing agreements written on blockchain platforms like as Ethereum. These contracts automate transactions when certain circumstances are met, decreasing the requirement for centralized oversight (Consensys, n.d.).

Decentralized exchanges (DEXs) are another key component of the DeFi ecosystem. Unlike centralized exchanges, DEXs allow users to trade digital assets directly between themselves, improving security and privacy by eliminating the need for a central authority (Chainlink, 2023). Additionally, DeFi has lending protocols that allow users to lend and borrow cryptocurrency in a decentralized manner. Platforms like Aave let users to earn interest or receive loans by dealing directly with smart contracts, bypassing traditional financial institutions (Amazon Web Services, n.d.).

Anonymity-centric cryptocurrencies, sometimes known as privacy coins, round out the DeFi environment. These digital currencies, which include Monero, Zcash, and Dash, are intended to increase transaction anonymity. Monero, for example, uses stealth addresses and ring signatures to obscure transaction details, keeping the sender, receiver, and transaction amount private (Merkle Science, 2023). Similarly, Zcash's zk-SNARK protocol provides optional privacy features that allow users to protect transaction information. Dash includes a function called PrivateSend, which mixes funds from multiple users to increase anonymity.

2.2. Criminal Exploitation of DeFi and Privacy Coins

While the revolutionary features of DeFi and privacy coins provide legal benefits, they have also been used illicitly. One major problem is money laundering on decentralized systems. DeFi's pseudonymous nature allows criminals to conceal the source of illicit payments by cycling them via numerous procedures, making detection and tracking difficult for authorities (Department of

Homeland Security, 2022).

DeFi platforms have also been subject to targeted attacks such as flash loan exploits and rug pulls. Flash loans, which are uncollateralized loans made in a single transaction, can be used to exploit flaws in DeFi protocols, resulting in significant financial losses. Rug pulls occur when developers withdraw liquidity from a project unexpectedly, deceiving investors (University Carlos III of Madrid, 2022).

To increase anonymity, criminals use privacy-enhancing wallets and mixers. Tornado Cash and Wasabi Wallet allow users to combine their cryptocurrency transactions with others, effectively obscuring the transaction trail. This approach hinders law enforcement's efforts to trace illicit financial transfers and has been linked to a variety of criminal activity.

The expansion of DeFi has coincided with an increase in criminal operations that use its infrastructure. Notable occurrences include sophisticated phishing assaults on cryptocurrency exchanges, which cause huge financial losses. For example, in February 2025, a prominent exchange was targeted by a phishing attack, resulting in the theft of nearly US$1.4 billion in Ethereum tokens (The Hacker News, 2025). Such occurrences illustrate DeFi platform vulnerabilities and the significant financial effect of these attacks.

Privacy coins have also been implicated in ransomware attacks and fraud cases. Their enhanced anonymity features make them attractive to cybercriminals seeking to evade detection. The use of privacy coins in illicit activities underscores the challenges faced by law enforcement in tracking and prosecuting offenders in the evolving landscape of financial crime (Merkle Science, 2023).

3. Rethinking Traditional Criminological Theories in the Context of DeFi

3.1. Strain Theory and Economic Crime in the Digital Era

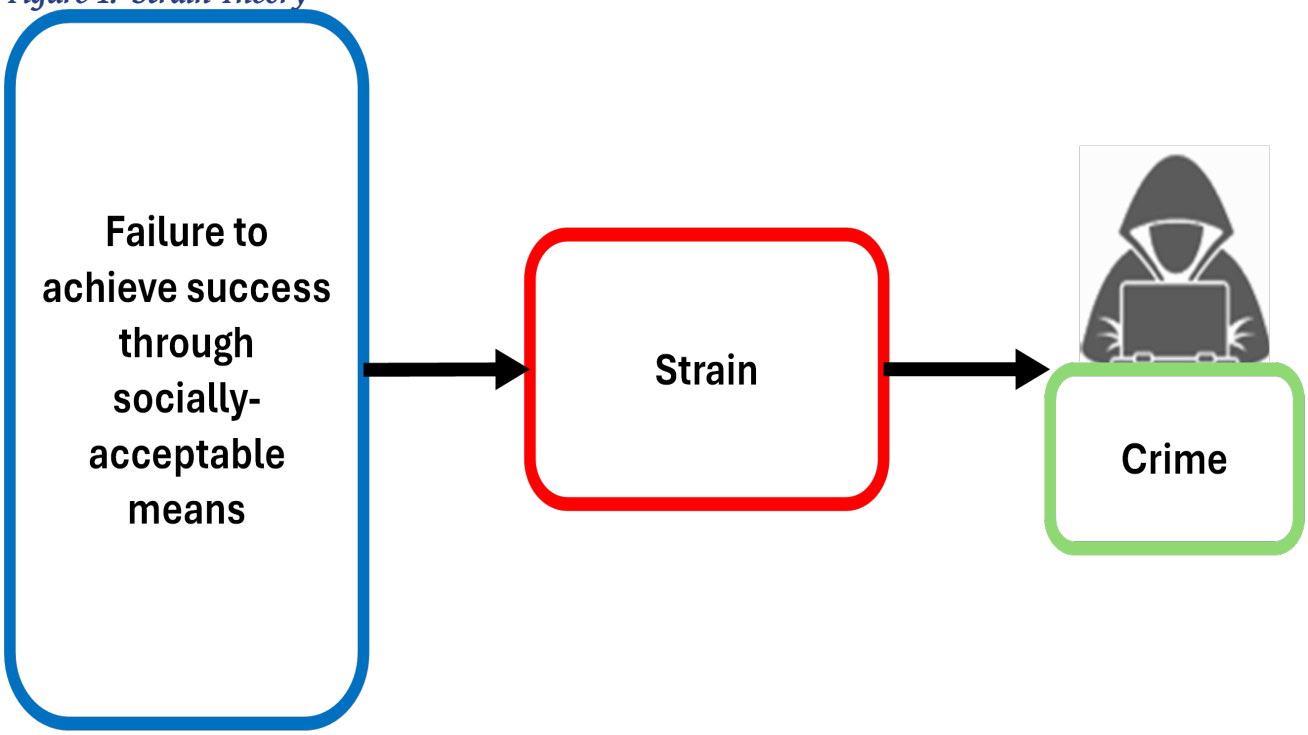
According to Strain Theory, societal pressures, such as the goal of financial success, might cause people to engage in criminal activity when lawful alternatives are unavailable. According to Merton, when people are unable to accomplish socially acceptable goals (such as financial achievement) through legitimate methods, they incur stress, which can lead to deviant behavior, including economic crimes. Strain theory's dynamics have transformed in the digital age, creating new obstacles and opportunities for economic crime. The pressure to achieve financial success has increased in the digital era due to the visibility of riches on social media and the ease with which one may compare oneself to others around the world. The digital divide—the difference between those who have access to digital technologies and those who do not—can intensify emotions of relative deprivation, which is an important component of strain theory. Individuals who feel themselves to be disadvantaged in the digital economy may experience increased stress, which increases the risk of engaging in economic crimes such as cyber fraud, identity theft, and online scams.

Decentralized Finance (DeFi) platforms have evolved as innovative financial systems that break down traditional boundaries and provide open access to financial services without the use of centralized intermediaries. While inclusion democratizes money, it also opens up new opportunities for economic criminality. The anonymous nature of DeFi transactions can attract persons looking to abuse these platforms for unlawful gain, considering them as low-risk opportunities due to the constraints they provide (Chainalysis, 2025).

These crimes are frequently helped by the anonymity and global accessibility of the internet, making them difficult to detect and punish. The digital ecosystem also opens up new chances for individuals to exploit vulnerabilities in systems and networks, complicating attempts to combat

economic crime.

Figure 1: Strain Theory



Source: Author's own.

Economic incentives are a major motivator of cybercriminal behavior in DeFi ecosystems. The considerable financial rewards associated with exploiting smart contract vulnerabilities or executing fraudulent schemes can incentivize people to commit cybercrimes. The quick appreciation of certain digital assets further enhances the possible rewards, motivating players to prioritize financial gain over ethical considerations (Chainalysis, 2025).

3.2. Routine Activity Theory and the Digital Crime Landscape

Routine Activity Theory (RAT), created by Lawrence Cohen and Marcus Felson (1979), has become a significant framework for explaining crime by emphasizing the convergence of three critical elements: a motivated criminal, an appropriate victim, and the lack of a skilled guardian. RAT, which was traditionally used to explain property crimes in physical surroundings, is now increasingly being used to explain digital crime, particularly in the context of decentralized technologies like blockchain, bitcoin, and Decentralized Finance (DeFi). As the digital world expands, criminal activities such as cyber fraud, hacking, money laundering, and ransomware have increased, aided in large part by the anonymity and decentralization provided by blockchain platforms. RAT provides vital insights into the mechanics of digital crime, as it helps explain how the interaction of these three components—motivated offenders, suitable targets, and weak or absent guardians—leads to an environment conducive to illicit behavior.

The first component, the motivated offender, is motivated by financial gain, anonymity, or a variety of other incentives arising from the decentralized nature of platforms such as cryptocurrency exchanges and DeFi protocols. Cybercriminals are particularly drawn to decentralized finance due to its promise of pseudonymity, reduced regulation, and the lack of a centralized authority (Zohar & Dahan, 2023). With the growing popularity of digital currencies like Bitcoin and privacy-focused coins like Monero and Zcash, criminals are finding new platforms to carry out fraudulent operations such as money laundering, ransomware attacks, and phishing schemes. The digital ecosystem,

with its worldwide reach and high liquidity, provides various chances for offenders motivated by profit and the perceived low risk of detection. (Binns, 2023).

Figure 2: Routine Activities Theory

Source: Author's own.

The second component of RAT, the suitable target, is widely available in the digital environment. Individuals and organizations who use digital platforms are frequently unaware of the risks associated with decentralized financial ecosystems. Many DeFi systems and cryptocurrency exchanges lack sufficient cybersecurity protections, leaving them open to exploitation (Choo, 2020). As a result, these platforms and their users are excellent targets for cybercriminals. Similarly, the massive amount of data and dollars passing through these platforms expands the pool of possible targets. Cryptocurrencies and digital wallets frequently contain enormous quantities of value, which attracts criminals looking to exploit flaws in transaction systems. Furthermore, decentralized networks often lack direct oversight, making it more difficult for users to detect and prevent dangers (Zohar & Dahan, 2023).

The third component of RAT, the lack of a skilled guardian, is especially important in the digital arena. In traditional crime prevention schemes, guardianship may include physical security measures, law enforcement, or regulatory entities that monitor and oversee illegal activity. In the digital arena, however, the lack of such guards poses a significant difficulty. The decentralized structure of blockchain and DeFi networks reduces the influence of central authorities, allowing criminal operations to thrive with little hindrance (Choo, 2020). Furthermore, the pseudonymous nature of blockchain transactions and privacy-enhancing technology like coin mixers and privacy coins impede law enforcement's capacity to trace unlawful activity, making it difficult to prevent and prosecute cybercrimes (Binns, 2023).

According to RAT, crime happens when a motivated perpetrator, an appropriate target, and the absence of a capable guardian intersect in time and space. In the case of DeFi, decentralized networks frequently lack standard monitoring systems, thereby eliminating skilled guardians who

dissuade illicit activity. This absence creates an atmosphere in which bad actors can operate with relative impunity, exploiting system weaknesses.

The DeFi ecosystem offers multiple options for the confluence of motivated offenders and vulnerable victims. Users, frequently motivated by the prospect of huge rewards, may engage with unverified platforms or smart contracts without fully appreciating the risks involved. This habit offers a pool of ideal candidates for cybercriminals that exploit these weaknesses via strategies like as phishing, rug pulls, or exploiting software bugs in smart contracts (Chainalysis, 2025).

RAT provides a framework for understanding how digital crime emerges and why decentralized systems are particularly vulnerable to exploitation. By considering how motivated offenders, suitable targets, and weak guardians converge in the digital landscape, it becomes evident that combating digital crime requires robust technological solutions, enhanced cybersecurity protocols, and international collaboration between regulators, law enforcement agencies, and DeFi developers. Strengthening the guardianship element in digital ecosystems, through both technological and regulatory advancements, is essential to reducing the risks posed by decentralized technologies.

3.3. Rational Choice Theory and the Evolution of Financial Crime

Rational choice theory (RCT), based on classical criminology, holds that people participate in illegal action after assessing the potential rewards against the risks and costs (Cornish & Clarke, 1986). This viewpoint assumes that offenders are rational individuals who make planned judgments to maximize personal advantage. In the context of financial crime, rational choice theory offers a valuable framework for understanding how individuals and organizations capitalize on possibilities in an ever-changing financial world, particularly in the digital age. As financial systems have grown more complicated and linked, the nature of financial crime has changed, posing new obstacles for prevention and enforcement.

Figure 3: Rational Choice Theory

Source: Author's own.

The digital revolution has profoundly changed the nature of financial crime, providing new opportunities for rational actors to exploit system and network vulnerabilities. For example, the rise of internet banking, cryptocurrency, and e-commerce platforms has broadened the scope of financial crime, allowing perpetrators to perpetrate fraud, money laundering, and identity theft on a massive scale. The internet's anonymity and global reach further minimize the perceived risks of detection and prosecution, making financial crime an appealing alternative for rational individuals looking to maximize profits with least effort.

One of the major pillars of RCT is the concept of "opportunity structures," which refers to the conditions that make specific crimes more feasible and appealing (Clarke & Felson, 1993). In the digital age, technological improvements have offered new opportunities for financial crime. For example, the widespread use of mobile payment systems and peer-to-peer lending platforms has created new opportunities for fraud and embezzlement. Similarly, while blockchain technology's decentralized structure provides benefits like as transparency and security, it has also been used by criminals for activities such as ransomware attacks and illicit transactions on the dark web (Yar & Steinmetz, 2019).

The rational choice perspective emphasizes the importance of situational conditions in shaping criminal behavior. In the context of financial crime, situational factors such as weak regulatory monitoring, inadequate cybersecurity measures, and a lack of international collaboration can create a climate conducive to illegal activity (Benson & Simpson, 2018). For example, the 2008 financial crisis revealed how lax regulation and oversight enabled rational actors within financial institutions to engage in risky and unethical practices, ultimately leading to widespread economic harm.

The anonymity and decentralization inherent in DeFi platforms and privacy-centric cryptocurrencies significantly alter this rational calculation of potential risks and rewards or cost-benefit analysis of RCT. The perceived low risk of detection and prosecution in decentralized networks lowers the threshold for engaging in illicit activities, as traditional law enforcement faces challenges in tracing and attributing transactions to specific individuals (Chainalysis, 2025).

Moreover, the use of self-executing smart contracts can automate illicit transactions, reducing the need for direct human involvement and thereby minimizing the risk of exposure. These contracts can be programmed to execute fraudulent schemes or launder money without manual intervention, further complicating detection and enforcement efforts (Chainalysis, 2025).

3.4. Cybercriminal Subcultures and Online Crime Communities

The rise of the internet has given rise to a new type of criminal activity: cybercriminal subcultures and online crime communities. These digital ecosystems enable individuals with common interests in illicit activities to collaborate, share knowledge, and build sophisticated criminal enterprises. Unlike traditional criminal networks, cybercriminals frequently operate in decentralized and anonymous online spaces such as dark web forums, encrypted messaging applications, and social media platforms (Holt & Bossler, 2014). These communities provide a sense of belonging while also providing technological support, tools, and resources for members to engage in activities such as hacking, fraud, and the sale of unlawful products and services.

One of the distinguishing characteristics of cybercriminal subcultures is a focus on talent sharing and mentorship. Experienced hackers and fraudsters frequently serve as educators, providing tutorials, instructions, and even one-on-one training to new members (Yar, 2005). This knowledge transfer not only lowers the entry barrier for aspiring hackers, but it also helps to drive the growth of more powerful and sophisticated attack methods. For example, forums dedicated to ransomware development or phishing techniques provide members with access to pre-built tools, exploit kits, and even customer service, allowing individuals to carry out crimes with no technical expertise (Hutchings & Holt, 2015).

A culture of trust and reputation shapes the social dynamics in these societies as well. Members frequently rely on feedback mechanisms like ratings and reviews to establish credibility and build confidence in the community (Motoyama et al., 2011). This reputation-based mechanism ensures that only trustworthy actors prosper, resulting in a self-regulating environment resembling legitimate internet marketplaces. However, this trust is fragile, and disagreements over payments, frauds, or failed cooperation are prevalent, frequently resulting in confrontations or the dissolution of partnerships.

Despite their illicit character, cybercriminal communities frequently share the ideals and practices of legitimate online communities, such as collaboration, innovation, and a common sense of purpose. This makes them especially durable and adaptable to law enforcement operations. The advent of DeFi coincides with the emergence of cybercriminal subcultures that use these technologies for fraudulent purposes. Individuals looking to take use of DeFi platforms can collaborate through online communities and forums. These networks enable the exchange of information, tools, and methods for committing crimes such as phishing attacks, Ponzi schemes, and smart contract exploitation (Chainalysis, 2025).

Anonymity in these digital places gives cybercriminals a sense of security, which encourages the establishment of unlawful cooperation that cross geographical boundaries. The anonymous nature of blockchain transactions and the adoption of privacy-enhancing techniques make it difficult for authorities to infiltrate these networks and identify culprits, hence enabling the persistence and growth of DeFi-driven fraud communities (Chainalysis, 2025).

4. Law Enforcement Challenges in Combating Decentralized Crime

4.1. Jurisdictional and Regulatory Barriers

Law enforcement organizations attempting to enforce laws throughout the Decentralized Finance (DeFi) ecosystem face considerable hurdles due to the decentralized structure of the platforms. Traditional financial systems have defined jurisdictional boundaries, which allows for the implementation of regional rules and oversight. DeFi platforms, on the other hand, run on blockchain networks that cross national borders, allowing users from anywhere to conduct financial transactions without centralized authority. This global accessibility affects law enforcement by making it more difficult to determine the appropriate jurisdiction and hold violators accountable. The anonymous character of transactions exacerbates this issue, as identifying individuals behind illegal activity requires advanced investigative tools and international cooperation (U.S. Department of the Treasury, 2023).

Furthermore, there is a fundamental tension between protecting privacy and executing efficient financial crime prevention methods. Privacy-centric cryptocurrencies, often known as privacy coins, are intended to increase user anonymity by obscuring transaction details. While these characteristics safeguard individual privacy, they also limit law enforcement's ability to monitor transactions and uncover illicit cash flows. Balancing the right to financial privacy with the need to combat money laundering, terrorism financing, and other financial crimes provides a difficult regulatory challenge. Regulatory authorities must manage these competing objectives in order to create frameworks that protect individual privacy while also allowing for effective oversight.

4.2. Investigative Challenges and Blockchain Forensics

Tracing transactions using privacy coins and DeFi protocols presents significant hurdles for investigators. Privacy coins, such as Monero and Zcash, use powerful cryptographic techniques to mask transaction data, making it harder to associate transactions with specific individuals or

institutions. DeFi protocols, which operate over decentralized and often pseudonymous networks, complicate tracking due to the lack of centralized management and oversight. The integration of cross-chain technologies enables the frictionless transfer of assets between different blockchain networks, allowing criminal actors to shift funds across multiple platforms while concealing their origins. This intricacy necessitates investigators to deploy advanced blockchain analytics tools capable of detecting cross-chain events and identifying trends indicative of illegal behavior (Merkle Science, 2025).

Individuals who want to hide the origins and destinations of their assets frequently use obfuscation tactics such as mixers and cross-chain swaps. Mixers combine numerous transactions to disguise the trail of funds, whereas cross-chain swaps allow assets to be exchanged between blockchains without a centralized intermediary. These approaches complicate the investigation by interfering with transaction traceability and making it difficult to track the movement of illicit monies. To address these issues, law enforcement agencies must use modern forensic tools and procedures that can analyze complicated transaction patterns and de-anonymize obfuscated activity (Elliptic, 2022).

4.3. Institutional Limitations and Capacity Gaps

The rapid evolution of DeFi and privacy-focused cryptocurrencies demands ongoing, specific training for law enforcement professionals. Traditional investigative procedures are frequently insufficient to solve crimes employing decentralized and pseudonymous systems. There is a critical need for better training programs focusing on crypto-forensics, providing investigators with the skills and expertise required to navigate the complexity of blockchain technologies, analyze transaction data, and successfully apply specialized analytical tools (Simply Forensic, 2025).

Securing cooperation from DeFi developers and governance communities poses additional problems. DeFi's decentralized ethos frequently means that there is no central authority to interact with, and developers may be distributed across multiple jurisdictions with different legal systems. This decentralization can lead to reluctance or refusal to assist law enforcement, particularly if participation is deemed to violate the ideals of user privacy and autonomy. In the fragmented financial landscape, successful law enforcement requires the establishment of collaborative relationships and structures that promote responsible innovation while guaranteeing compliance with legal and regulatory norms (U.S. Department of the Treasury, 2023).

5. Innovations in Crypto-Forensics and Legal Enforcement Strategies

5.1. Advances in Blockchain Analytics and DeFi Monitoring

The rapid rise of Decentralized Finance (DeFi) has forced the creation of sophisticated blockchain analytics and monitoring systems to detect and prevent fraudulent activity. Emerging forensic techniques may now track unlawful transactions within DeFi networks by examining both on-chain and off-chain data. These tools organize and evaluate transaction facts, including as timestamps, involved addresses, and linked services, to detect trends that indicate fraudulent activity.

Artificial intelligence (AI) has become critical to improving blockchain intelligence. AI-powered platforms can process massive volumes of blockchain data in real time, detecting anomalies and suspicious activity that traditional monitoring systems may miss. For example, AI-powered risk-scoring algorithms analyze the chance of transactions being related with unlawful activity, allowing for preventative interventions against possible dangers (AnChain.AI, n.d.).

5.2. Strengthening Cross-Border Law Enforcement Cooperation

Given cryptocurrencies' global character, international cooperation is critical in addressing crypto-enabled financial crimes. The Financial Action Task Force (FATF) has established the "Travel Rule," which requires Virtual Asset Service Providers (VASPs) to collect and transmit originator and beneficiary information during transactions in order to increase transparency and deter illicit activity (Sumsub, 2024). Similarly, the European Union's Markets in Crypto-Assets Regulation (MiCA) creates a standardized legal framework for crypto-assets, including consumer protection, asset classification, and licensing requirements (European Securities and Markets Authority, n.d.).

Multilateral measures strengthen efforts to tackle cryptocurrency-related financial crimes. These joint efforts promote the sharing of intelligence, harmonization of regulatory standards, and coordination of enforcement operations across jurisdictions, thus boosting the global response to illicit activity in the crypto realm (FATF, 2024).

5.3. Regulatory and Policy Responses to Emerging Crypto Threats

As the crypto ecosystem changes, regulatory authorities tighten compliance requirements for DeFi systems and privacy-enhanced cryptocurrencies. This involves establishing strong Know Your Customer (KYC) and Anti-Money Laundering (AML) measures to guarantee that organizations involved in crypto activity follow established financial regulations (Lukka, 2025).

Balancing privacy, innovation, and security raises ethical concerns for legislators. While privacy is a vital value, it must be balanced with the importance of combating financial crimes and maintaining market integrity. Regulatory frameworks strive to strike this balance by fostering openness and accountability while not limiting technological progress and the benefits that decentralized financial systems offer (Forbes, 2025).

6. Recommendations for Policy and Practice

Addressing the complexities of decentralized financial crimes, such as those facilitated by cryptocurrencies, dark web marketplaces, and peer-to-peer networks, requires a multifaceted approach that combines regulatory innovation, technological adaptation, and international cooperation. Policymakers and practitioners must recognize the unique challenges posed by these crimes, including their borderless nature, anonymity, and rapid evolution. To effectively address the complexities of decentralized financial crimes, a multidimensional approach is essential:

1. Strengthening Global Cooperation in DeFi Regulation: Given the transnational nature of DeFi platforms, international collaboration is crucial. Regulatory bodies should work towards harmonizing policies and sharing intelligence to create a cohesive framework that transcends national boundaries. Initiatives such as the Financial Action Task Force (FATF) Travel Rule and the European Union's Markets in Crypto-Assets (MiCA) regulation exemplify steps toward unified oversight (Financial Stability Board, 2025).
2. Enhancing Forensic Capabilities in Tracking Privacy-Focused Cryptocurrencies: Investing in advanced forensic tools and training programs is imperative for law enforcement agencies. The development and deployment of artificial intelligence-driven blockchain analytics can aid in tracing illicit transactions involving privacy coins and DeFi protocols, thereby improving the detection and prevention of financial crimes (Elliptic, 2025).

By adopting these recommendations, policymakers and practitioners can better address the challenges posed by decentralized financial crimes, ensuring a safer and more secure digital financial landscape.

Table 1: Summary of Challenges, Evolving Technological Innovations and Practical Policy Implementation

Section	*Focus Area*	*Key Points*
Law Enforcement Challenges in Combating Decentralized Crime	Jurisdictional & Regulatory Barriers	– DeFi operates across borders, complicating jurisdiction. – Privacy coins obscure transactions, limiting oversight. – Tension between financial privacy vs. crime prevention.
	Investigative Challenges	– Privacy coins (e.g., Monero, Zcash) mask data. – Cross-chain swaps and mixers complicate tracking. – Advanced blockchain forensics needed.
	Institutional Limitations	– Law enforcement lacks specialized training. – Limited cooperation from DeFi communities. – Decentralization reduces points of contact for investigations.
Innovations in Crypto-Forensics and Legal Enforcement Strategies	Blockchain Analytics & AI	– AI-driven tools detect anomalies and suspicious activity. – On-chain and off-chain data used for monitoring. – Risk scoring improves preventive intervention.
	Cross-Border Cooperation	– FATF Travel Rule mandates transaction data sharing. – EU's MiCA regulation creates standardized oversight. – Multilateral collaboration enhances enforcement.
	Regulatory & Policy Responses	– Stricter KYC/AML compliance for DeFi platforms. – Ethical tension: privacy vs. market integrity. – Efforts to balance innovation with security.
Recommendations for Policy and Practice	Global Cooperation	– Harmonize cross-border regulation. – Intelligence sharing and coordinated enforcement. – FATF and MiCA serve as models.
	Forensic Capabilities	– Invest in advanced blockchain forensics. – AI-based tools to trace illicit flows. – Training programs for investigators.
	Strategic Outlook	– Multi-pronged approach: regulation + tech + cooperation. – Balance innovation with oversight. – Focus on privacy coins and DeFi-related crimes.

Source: Author's ow.

7. Conclusion and Future Directions

The pseudonymous character of DeFi platforms and privacy-focused digital currencies has opened up new paths for criminal financial activity, challenging standard criminological ideas and law enforcement approaches. To properly handle the specific issues provided by digital financial crimes, established criminological frameworks must be reevaluated due to these technologies' decentralized and borderless nature.

Law enforcement organizations confront major challenges while addressing crimes in the DeFi ecosystem. The anonymity given via online platforms hinders the identification and apprehending of violators, while jurisdictional issues impede the enforcement of legislation across multiple legal systems. Despite these obstacles, advances in blockchain analytics and international regulatory activities are emerging as critical instruments in the battle against cryptocurrency-enabled financial crimes.

7.1. Areas for Further Research

The dynamic and evolving landscape of DeFi and cryptocurrencies presents several avenues for future research:

(a) ***The Impact of AI and Automation in DeFi Crime Detection:*** Exploring how artificial intelligence and machine learning algorithms can enhance the identification and mitigation of fraudulent activities within DeFi ecosystems is a promising area of study. Research should focus on developing models that can adapt to the rapidly changing tactics employed by cybercriminals (Elliptic, 2025).

(b) ***The Role of Central Bank Digital Currencies (CBDCs) in Reducing Crypto-Enabled Crime:*** Investigating whether the adoption of CBDCs can offer a regulated alternative to decentralized cryptocurrencies and potentially mitigate the prevalence of illicit activities is another critical research direction. Understanding the implications of CBDCs on financial crime dynamics will inform policymakers and law enforcement agencies in crafting effective strategies (U.S. Department of Homeland Security, 2024).

While DeFi and anonymity-centric cryptocurrencies provide new financial solutions, they also pose considerable risks in terms of criminal exploitation and regulatory supervision. A concerted effort comprising worldwide cooperation, technological innovation, and constant study is required for effectively combating and preventing decentralized financial crimes.

Declarations

The author has no relevant financial or non-financial interests to disclose. The data are available upon a reasonable request from the author.

References

Amazon Web Services. (n.d.). What is DeFi? - Decentralized Finance Explained. Retrieved from https://aws.amazon.com/web3/what-is-defi/

AnChain.AI. (n.d.). CISO: AI-powered Blockchain Analytic Tool. Retrieved from https://www.anchain.ai/ciso

Bank of Canada. (2023). Decentralized finance: Innovations and challenges. Retrieved from https://www.bankofcanada.ca/2023/10/staff-analytical-note-2023-15/

Benson, M. L., & Simpson, S. S. (2018). White-collar crime: An opportunity perspective. Routledge.

Binns, A. (2023). Decentralized finance and the rise of digital crime. *Journal of Financial Crime, 30*(1), 123-140. https://doi.org/10.1108/JFC-06-2022-0142

Bray, J. D. (2016). *Anonymity, cybercrime, and the connection to cryptocurrency.* Eastern Kentucky University. Retrieved from https://encompass.eku.edu/etd/418/

Chainalysis. (2021, December 9). Privacy Coins 101: Anonymity-Enhanced Cryptocurrencies. Retrieved from https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies/

Chainlink. (2023, August 1). Analyzing the DeFi Ecosystem. Retrieved from https://chain.link/education-hub/defi-ecosystem

Choo, K. K. R. (2020). Cybercrime and digital forensic investigations: The role of decentralization in the digital crime ecosystem. *Journal of Digital Crime and Forensics, 8*(2), 203-217. https://doi.org/10.1080/JDCF-05-2020-0064

Clarke, R. V., & Felson, M. (1993). *Routine activity and rational choice*. Transaction Publishers.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. https://doi.org/10.2307/2094589

Consensys. (n.d.). Blockchain for Decentralized Finance (DeFi). Retrieved from https://consensys.io/blockchain-use-cases/decentralized-finance

Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal: Rational choice perspectives on offending.* Springer-Verlag.

Department of Homeland Security. (2022, September). Combatting Illicit Activity Utilizing Financial Technologies and Cryptocurrencies. Retrieved from https://www.dhs.gov/sites/default/files/2023-09/08.%20Combatting%20Illicit%20Activity%20Phase%202_508_0.pdf

El País. (2025, February 25). Un sofisticado 'phishing' para el mayor robo de la historia cripto: 1.400 millones volaron de la cuenta de Bybit. Retrieved from https://cincodias.elpais.com/criptoactivos/2025-02-25/un-sofisticado-phishing-para-el-mayor-robo-de-la-historia-cripto-1400-millones-volaron-de-la-cuenta-de-bybit.html

Elliptic. (2022, June 9). Obfuscation on the blockchain: How to detect and mitigate the risks. Retrieved from https://www.elliptic.co/blog/obfuscation-on-the-blockchain-how-to-detect-and-mitigate-the-risks

European Securities and Markets Authority. (n.d.). Markets in Crypto-Assets Regulation (MiCA). Retrieved from https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

Europol. (2020). Cryptocurrencies: Tracing the evolution of criminal finances. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Financial Action Task Force (FATF). (2023). Illicit financial flows from cyber-enabled fraud. Retrieved from https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf

FATF. (2024). Virtual Assets: Targeted Update on Implementation of the FATF Standards. Retrieved from https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

Forbes. (2025, January 7). New EU Rules Could Threaten Your Security – What You Need To Know. Retrieved from https://www.forbes.com/sites/digital-assets/2025/01/07/new-eu-rules-threaten-your-security--what-you-need-to-know/

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40. https://doi.org/10.1080/01639625.2013.822209

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. British *Journal of Criminology, 55*(3), 596-614. https://doi.org/10.1093/bjc/azu106

Keller, P., Florian, M., & Böhme, R. (2020). Collaborative deanonymization. arXiv preprint arXiv:2005.03535. Retrieved from https://arxiv.org/abs/2005.03535

Levi, M. (2017). Fraud: Organization, motivation, and control. In M. Edelbacher, P. C. Kratcoski, & M. Theil (Eds.), *Financial crime and fraud in the digital age* (pp. 15-32). Springer.

Lukka. (2025). Explore Blockchain Analytics and Transaction Monitoring. Retrieved from https://lukka.tech/blockchain-analytics-and-transaction-monitoring/

Marko, K. (2022). Anonymity technology in virtual assets: Scope, limitations, and emerging strategies. Terrorism, Transnational Crime and Corruption Center. Retrieved from https://traccc.gmu.edu/wp-content/uploads/2022/06/Marko_Anonymity-Technology-in-Virtual-Assets-Scope-Limitations-and-Emerging-Strategies.pdf

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A

fistful of bitcoins: Characterizing payments among men with no names. Proceedings of the 2013 Conference on Internet Measurement Conference, 127-140. https://doi.org/10.1145/2504730.2504747

Merkle Science. (2024, August 5). Crypto crime: How criminals are adapting and evolving. Retrieved from https://www.merklescience.com/blog/crypto-crime-how-criminals-are-adapting-and-evolving

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, 71-80. https://doi.org/10.1145/2068816.2068824

Simply Forensic. (2025, August 1). Dark crypto: Essential forensic techniques for blockchain analysis. Retrieved from https://simplyforensic.com/dark-crypto-essential-forensic-techniques-for-blockchain-analysis/

Sumsub. (2024). Crypto Travel Rule 2024 - FATF Requirements. Retrieved from https://sumsub.com/blog/what-is-the-fatf-travel-rule/

The CEO Views. (2024, December 15). Privacy coins in decentralized finance – All you need to know. Retrieved from https://theceoviews.com/privacy-coins-in-decentralized-finance-all-you-need-to-know/

The Hacker News. (2025, February 24). THN Weekly Recap: From $1.5B Crypto Heist to AI Misuse & Apple's Data Dilemma. Retrieved from https://thehackernews.com/2025/02/thn-weekly-recap-from-15b-crypto-heist.html

University Carlos III of Madrid. (2022, August 30). On the Fragility of DeFi Lending. Retrieved from https://economics.uc3m.es/wp-content/uploads/2023/10/NewDefi_300823.pdf

U.S. Department of the Treasury. (2022, August 8). U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. Retrieved from https://home.treasury.gov/news/press-releases/jy0916

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427. https://doi.org/10.1177/147737080556056

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). Sage.

Zohar, A., & Dahan, T. (2023). Privacy coins and the role of anonymity in cryptocurrency crimes. *International Journal of Cyber Security, 25*(3), 101-118. https://doi.org/10.1007/JCS-05-2023-0032

Zreik, H. (2024, October 30). The rise of decentralised finance (DeFi): Opportunities and challenges. FinTech Futures. Retrieved from https://www.fintechfutures.com/2024/10/the-rise-of-decentralised-finance-defi-opportunities-and-challenges/