GENERATE

Journal of Business Crime

Vol 02 (1) 2026 p. 33-45

Corresponding author:
Isyfa fuhrotun nadhifah
Email : isyfa@unisnu.ac.id

Received 6 March 2026;
Accepted 23 April 2026;
Published 27 April 2026.

Conflict of interest statement: Author(s) reported no conflict of interest

DOI: http://doi.org/10.70764/gdpu-jbc.2026.2(1)-04

DYNAMICS OF INTERNATIONAL REGULATORY AND INVESTIGATION COOPERATION IN HANDLING CRYPTO-RELATED ECONOMIC CRIMES

Isyfa fuhrotun nadhifah[1], Agwanwo Destiny Eze[2]

[1] *Universitas Islam Nahdlatul Ulama Jepara, Indonesia*
[2] *University of Port Harcourt, Nigeria*

ABSTRACT

Objective: This study aims to evaluate the effectiveness of regulatory models across selected jurisdictions such as the United States, Brazil, China, Thailand, Indonesia, and the European Union and to analyze emerging trends in crypto-related economic crime, particularly in relation to implementation gaps in FATF Recommendation 15, namely the Travel Rule, and the resulting cross-jurisdictional regulatory arbitrage dynamics.

Research Design & Methods: This study uses a comparative qualitative approach through document analysis and cross-country case studies. Secondary data comes from FATF, Interpol, UNODC, Chainalysis reports, national regulations, and academic literature, which are analyzed using thematic content analysis and comparative regulatory analysis.

Findings: Research findings indicate that regulatory fragmentation and gaps in the implementation of FATF standards create regulatory arbitrage loopholes that are exploited by crypto criminals. Crypto crime in the 2024-2025 period is becoming more professionalized, marked by the dominance of stablecoins, the involvement of state actors, and low asset recovery rates. Network-based international investigative cooperation, has proven to be more adaptive than unilateral repressive approaches.

Implications: There is a need for harmonization of cross-border AML policies, acceleration of Travel Rule implementation, and strengthening of informal investigative cooperation mechanisms and public private partnerships with VASPs to improve the effectiveness of asset tracking and recovery.

Contribution & Value Added: This study enriches the literature on digital economic crime by linking regulatory arbitrage and FATF networked governance, and provides the latest empirical evidence for the formulation of adaptive AML policies in the era of decentralized finance.

Keywords: Economic Crime, Cryptocurrency, Virtual Assets, Money Laundering, Financial Crime

JEL codes: K42, G28
Article type: research paper

INTRODUCTION

The development of global payment systems has entered a phase of fundamental transformation with the emergence of virtual assets or cryptocurrencies based on Distributed Ledger Technology (DLT) (Kreminskyi et al., 2021). Since the emergence of Bitcoin in 2009, digital currency ecosystems have evolved from mere cryptographic experiments into systemic components of the international financial architecture, with a market value exceeding trillions of dollars in 2024 (FATF, 2025). Cryptocurrency itself is defined as a decentralized virtual currency that is convertible and operates through a cryptographic mechanism based on a peer-to-peer system or blockchain (Brenig et al., 2015; Huberman et al., 2021; Vasylieva et al., 2018). The fundamental principles of cryptocurrency circulation are decentralization and relative anonymity, which fundamentally distinguish it from conventional financial systems (Dyntu and Dykyi, 2018; Khamzin et al., 2016).

However, inherent characteristics of cryptocurrency such as relative anonymity, instant cross-border transaction settlements, and quasi-autonomous nature have created significant challenges for law enforcement authorities and regulators around the world (Kreminskyi et al., 2021). Global law enforcement information systems

are developing much more slowly than technological innovations, particularly in the development of digital payment systems and cryptocurrencies, giving rise to what is known as the technological gap (Barone and Masciandaro, 2019). This gap directly complicates investigations into economic crimes and money laundering schemes that exploit cryptocurrencies, particularly given the cross-border nature of virtual currency transactions, which often transcend national legal jurisdictions (Kethineni and Cao, 2020). The use of anonymity technologies further complicates the tracking of illegal activities and undermines the effectiveness of anti-money laundering (AML) regimes that have been built over many years (Kreminskyi et al., 2021).

As the virtual currency circulation ecosystem develops dynamically, national and international legal systems are considered unable to effectively regulate and supervise these activities (Cumming et al., 2019). Interest in the potential of blockchain technology as a foundation for financial innovation continues to grow among governments, while at the same time the same technology is also attracting the attention of cybercriminals and transnational criminal organizations (Oxford Analytica, 2017). The main motives for cryptocurrency-based economic crimes include ease of use, potential financial gains for companies and individuals, and personal interests in exploiting existing regulatory loopholes (Braaten and Vaughn, 2019).

Since early 2008, the role of cryptocurrency in money laundering activities has shown a significant upward trend, mainly driven by dynamic innovations in digital payment systems that enable faster transactions and expanded criminal activities (Barone and Masciandaro, 2019; Zelisko et al., 2018). This innovation provides greater time efficiency and global reach for economic criminals (Burova and Kabakov, 2020; Kamps and Kleinberg, 2018). Data shows that Bitcoin, as the most dominant virtual currency, is estimated to facilitate up to US$76 billion in money laundering per year through illegal activities, accounting for approximately 46% of total Bitcoin transactions (Barone and Masciandaro, 2019). In addition, in 2025, the U.S. Attorney's Office for the Eastern District of New York, together with the Department of Justice's National Security Division, initiated civil forfeiture proceedings targeting approximately 127,271 Bitcoin, worth approximately USD 15 billion. The assets are suspected to be the proceeds and instruments of large-scale fraud and money laundering, which were previously stored in self-managed cryptocurrency wallets under the control of the defendants (Office of Public Affairs, 2025).

In response to the increasing complexity of cryptocurrency-based economic crimes, the international community, through organizations such as the Financial Action Task Force (FATF), is promoting the adoption of a risk-based approach to coordinate government efforts in the prevention and investigation of cross-border economic crimes (Kreminskyi et al., 2021). This approach involves establishing an international cooperation network that balances the opportunities for crypto innovation and the threat of economic crime, as well as developing global and decentralized governance mechanisms (Kreminskyi et al., 2021). The implementation of international standards such as the Travel Rule, which requires virtual asset service providers (VASPs) to collect and transmit sender and recipient information in every cross-border transaction, is a key instrument in these efforts (FATF, 2025). In this context, operational cooperation between financial intelligence agencies, international police forces such as Interpol, and the private sector is seen as a key prerequisite for responding to the increasing professionalization of cryptocurrency-based economic crime (United Nations, 2025).

This study aims to evaluate the effectiveness of different regulatory models in various jurisdictions, analyze the latest trends in crypto economic crime methodologies up to 2025, and formulate strategic recommendations for strengthening the resilience of the global financial system against the misuse of virtual assets. Through comparative analysis, this report will examine how different countries are responding to these challenges and how international synergy can mitigate the systemic risks posed by poorly regulated digital assets.

LITERATURE REVIEW

Theoretically, the circulation of cryptocurrency in the context of economic crime can be understood through cryptographic mechanisms that are often misused as instruments of money laundering, substitutes for national currencies, or tools for illegal investment (Kreminskyi et al., 2021). Some literature identifies mechanisms of criminal activity that include the establishment of front companies, the development of relationships with existing criminal networks, the artificial revaluation of crypto assets to encourage fraudulent investment, and the violation of fiduciary duties through the misuse of company profits (Kreminskyi et al., 2021). The four main types of crypto-related crimes identified globally are money laundering, smuggling transactions, tax evasion, and extortion (Kreminskyi et al., 2021).

Some of these criminal activities include setting up front companies, collaborating with criminal networks, manipulating crypto asset values to attract investment, breaching fiduciary duties through misuse of company profits, and conducting anonymous transactions on digital networks (Braaten and Vaughn, 2019). In addition, the financing mechanism through initial coin offerings (ICOs) has also been reported to have the potential to be used as a channel for money laundering (Barone and Masciandaro, 2019). In general, cryptocurrency-based crimes include money laundering, illegal trading, tax evasion, and extortion (Bloomberg, 2017). The absence of clear legal status and adequate regulatory basis for cryptocurrency poses significant obstacles in the investigation of criminal

acts, particularly in identifying perpetrators and proving elements of crime (Dyntu and Dykyi, 2018; Nahorniak et al., 2016).

Economic crimes in virtual asset spaces can also be explained through convenience theory, whereby cryptocurrencies provide convenience, financial gain, and relative autonomy for their owners due to the absence of strict personal information requirements (Braaten and Vaughn, 2019). From an economic perspective of "public interest theory," crypto regulation is considered a solution to market failure, particularly to address information asymmetry where many investors do not understand the technical risks of data mining and blockchain technology (Frediani, 2024). In addition, systemic risks such as those seen in the collapse of the FTX exchange reinforce the argument that government intervention is necessary to protect the country's financial stability and monetary sovereignty (Frediani, 2024).

Several studies indicate that government intervention in the cryptocurrency market is increasing, particularly through the regulation of digital asset circulation requirements and the strengthening of inter-agency cooperation to ensure the stability and security of the financial system (Haydanka, 2019; Spithoven, 2019; Stroukal, 2016). However, cryptocurrency regulation requires complex policy adjustments, covering monetary policy, trade, and national security, particularly in the cyber realm (Nath, 2020). Until now, there has been no global consensus on the definition of cryptocurrency or an integrated approach to taxation and circulation regulations (Solodan, 2019). As a result, regulations at the national level are considered insufficiently effective in preventing economic crimes related to virtual currencies (Atabekova and Radic, 2020; Dumchikov et al., 2020).

METHODS

This study uses a qualitative approach with a cross-jurisdictional analysis of documents, reports, and case studies to evaluate the effectiveness of anti-money laundering (AML) regimes in dealing with cryptocurrency-based economic crimes. Secondary data was collected from official reports of international institutions (FATF, Interpol, UNODC), blockchain intelligence reports (Chainalysis), national regulations, court decisions, and reputable academic literature. The main method used is comparative analysis to examine crypto regulation policies in various countries, which are categorized into three main groups. Countries are classified into three regulatory models, namely: (1) complete prohibition or strict restrictions; (2) no specific regulations; and (3) limited recognition as currency or financial instruments. The differences in these regulatory models indicate the absence of global policy harmonization and weak international cooperation in dealing with cryptocurrency-based economic crimes.

Table 1. Comparison of Cryptocurrency Regulatory Models and Their Impact on International Cooperation

Country Group	Policy Characteristics	Example Countries/Jurisdictions	Impact on International Cooperation
Group 1: Absolute Prohibition	Prohibiting or strictly limiting cryptocurrency transactions and exchanges.	China, Algeria, Bolivia (before 2025), Russia (certain phases).	Restricting formal data sharing; encouraging activities to move to the "shadow" area
Group 2: No Specific Policy	No specific regulations; using general tax or commodity laws.	Canada, Singapore, Indonesia, Australia, Japan.	Relying on traditional MLATs; law enforcement is ad-hoc.
Group 3: Integrated Regulation	Regulating cryptocurrencies as substitutes for official currencies or financial instruments.	Germany, Brazil, European Union (MiCA), United States, South Korea.	Facilitating structured cross-border cooperation and the "Travel Rule".

The analysis was conducted through thematic content analysis to identify regulatory patterns, gaps in the implementation of FATF Recommendations (particularly R.15 and the Travel Rule), and law enforcement practices in various countries. A comparative regulatory analysis approach was used to compare policy responses and law enforcement effectiveness in selected jurisdictions, including the United States, the European Union, South Korea, Brazil, and countries with restrictive approaches. The validity of the findings was strengthened through triangulation of sources and synthesis across policy reports, empirical data, and operational case studies.

RESULT

Differences in regulatory approaches between jurisdictions significantly create loopholes for regulatory arbitrage, where perpetrators of digital economic crimes strategically move their activities to countries with weaker anti-money laundering (AML) standards. Countries with absolute prohibition policies such as China, Thailand, and Russia tend to push crypto activities into gray areas or across borders, while countries without specific policies, including Indonesia, India, and most European Union countries, provide legal uncertainty that can be exploited by criminals (Apakhayev et al., 2018; Oxford Analytica, 2017). This finding reinforces the argument that global

regulatory fragmentation actually increases the risk of operational relocation to the shadow financial system, which has minimal AML oversight (Bulatov et al., 2019; Singh, 2015).

An evaluation of the implementation of FATF Recommendation 15 and its Interpretative Note (INR.15) shows that although a number of jurisdictions have made progress in establishing AML/CFT frameworks for virtual assets and Virtual Asset Service Providers (VASPs), there is still a significant gap between normative adoption and effective implementation at the national level. The 2024 Targeted Update Report confirms that most jurisdictions "have not fully implemented FATF standards," with 75% of countries still only partially compliant or non-compliant with R.15/INR requirements and the implementation of the travel rule, which is vital for cross-border identification data exchange, remains low despite the adoption of legislation (FATF, 2024). The lack of progress in implementing the Travel Rule and supervising VASPs contributes to AML/CFT loopholes that can be exploited in digital economic crime schemes. This delay is exacerbated by rapid innovation in crypto products and decentralized business models that go beyond the conventional legal framework (Campbell-Verduyn, 2018; Nath, 2020).

A comparison of the effectiveness of law enforcement shows a clear contrast between countries with aggressive approaches such as the United States and countries that are still developing regulatory frameworks such as Brazil. In the United States, the use of established legal instruments such as the Bank Secrecy Act and the Money Laundering Control Act has set legal precedents for crypto exchanges and major players, including the Ripple Labs and Coin.mx cases, which demonstrate the country's capacity to integrate virtual assets into the existing AML regime (Abdulla, 2020; Balusamy et al., 2025; Piddubnyi et al., 2019). In contrast, Brazil, despite recognizing crypto as a form of electronic money, still shows institutional ambiguity reflected in court rulings and dependence on traditional banking regulations, so the effectiveness of combating crypto crime is relatively limited (Kethineni and Cao, 2020; Tu & Meredith, 2015).

Overall, the results of this study confirm that global leadership in combating digital economic crime is not only determined by the formal adoption of FATF standards, but also by law enforcement capacity, international coordination, and the ability to adapt to the decentralized nature of virtual assets. Without policy harmonization and consistent implementation across countries, the global AML regime risks continuing to lag behind the increasingly professional and cross-jurisdictional dynamics of crypto-based crime (Anggriawan and Susila, 2024; Dyntu and Dykyi, 2018; Kovalchuk et al., 2024; Zhang & Xu, 2019).

Research findings indicate that the crypto crime landscape in 2024 to 2025 will shift toward professionalization and increased scale of attacks (FATF, 2025). Despite progress in adopting FATF standards, challenges in identifying individuals or legal entities engaged in VASP activities remain high.

Table 2. Comparison of Cryptocurrency Regulatory Models and Their Impact on International Cooperation

Parameters	2024 Data	2025 Data	Strategic Implications
Total Value Stolen	$1.34 Billion	$3,4 Billion	A drastic increase in the volume and value per incident.
Share of Thefts by DPRK	~$1,34 Billion	$2.02 billion (51% increase)	The dominance of state actors in cyber security exploitation.
Illegal Stablecoin Activity	Significant	>90% of total on-chain	Stablecoins have become the primary medium for money laundering due to their stable value.
Fraud/Scam Cases	High	~$51 billion (Estimate)	The emergence of organized, industrial-scale fraud centers.
Asset Recovery Rate	Very Low	3,8%	Demonstrating urgency in strengthening asset recovery cooperation.

Source : (Chainalysis, 2025a; FATF, 2025)

One key finding is the dominance of actors from Democratic People's Republic of Korea (DPRK) who carried out attacks of very high value with lower frequency than in previous years (Chainalysis, 2025a). In February 2025, the hacking of the by bit exchange in South Korea resulted in losses of $1.5 billion, which was the largest single theft of the year. The DPRK's strategy has evolved by illegally placing IT workers in Western companies to gain privileged access to corporate financial systems, which are then used to facilitate high-value compromises.

Implementation of "Travel Rule" and Supervision of VASP

Through June 2025, 99 jurisdictions have passed or are in the process of passing legislation implementing the Travel Rule (FATF, 2025). This rule is considered crucial to ensure transparency of information in cross-border payments. In the European Union, the Markets in Crypto-Assets (MiCA) regulation will be fully effective by the end of 2024, requiring all crypto-asset service providers (CASP) to obtain authorization from national authorities (Norton Rose Fulbright, 2024). MiCA also introduces strict rules for stablecoin issuers (asset-referenced tokens and e-money tokens) to ensure liquid asset reserves. In Brazil, the Central Bank (BCB) has been designated as the primary

regulator through Law No. 14.478/2022. At the end of 2024, Brazil launched a pilot project for a central bank digital currency (Drex) and tightened reporting requirements for citizens who conduct transactions on foreign platforms exceeding 30,000 Reais per month (Sanction Scanner, 2024). These steps indicate a global trend toward integrating digital assets into strictly regulated financial systems (Chainalysis, 2025b).

Comparatively, the United States has emerged as the most aggressive jurisdiction in enforcing laws against cryptocurrency-based economic crimes. Law enforcement practices in the US demonstrate the use of existing legal instruments, such as the Money Laundering Control Act and the Bank Secrecy Act, in cracking down on crypto actors and entities that violate AML regulations (Abdulla, 2020; Piddubnyi et al., 2019). Several cases, including the prosecution of BitInstant's CEO, sanctions against Ripple Labs by FinCEN, and the Coin.mx case, show that conventional regulations can be adapted to crack down on illegal activities in the cryptocurrency ecosystem.

Outside the United States, countries' responses to cryptocurrency circulation tend to be restrictive, ranging from a total ban on altcoins to restrictions on financial institutions' activities in processing crypto transactions, as implemented in China, Vietnam, Indonesia, Iceland, and several European countries. However, this repressive approach has drawn criticism for being ineffective in preventing economic crime and instead encouraging regulatory arbitrage, whereby cryptocurrency operators move their activities to jurisdictions with weaker AML standards (Singh, 2015). These findings indicate that the decentralized nature of cryptocurrency systems structurally limits the effectiveness of policies that place too much emphasis on restrictions and prohibitions.

International Investigative Cooperation: Operation HAECHI VI

Operational cooperation has yielded significant results through initiatives such as Operation HAECHI VI, coordinated by Interpol between April and August 2025 (Chainalysis, 2025b). This operation targets seven types of cyber-enabled financial crimes, including investment fraud and money laundering related to online gambling.

Research findings indicate that the dynamics of cryptocurrency-based economic crime have prompted a global leadership race among jurisdictions to establish credible anti-money laundering (AML) regimes. Countries and territories such as the United States, Singapore, the Isle of Man, and Alderney are positioning themselves as legitimate crypto transaction hubs through know your customer (KYC) requirements, suspicious transaction reporting, and the integration of AML standards into the virtual asset ecosystem (Singh, 2015). However, challenges remain in implementing effective and consistent regulations to prevent money laundering practices around the world (Widhiyanti et al., 2023). Collaborative efforts between these countries and international institutions are essential to address challenges in cross-border money laundering surveillance and enforcement (Suwitra et al., 2024).

In this context, operational-based international investigative cooperation emerged as the most adaptive mechanism, as reflected in Operation HAECHI VI coordinated by Interpol during the period April–August 2025. This operation targets seven categories of cyber-based financial crimes, including investment fraud, pig butchering, romance scams, sextortion, and money laundering related to online gambling (International Criminal Police Organization (INTERPOL), 2024). This operation aims to strengthen collaboration between countries in tackling increasingly complex cybercrime in the region (Kharisma et al., 2025). The collaborative cross-border approach in this operation successfully overcame the limitations of national law enforcement, which is slow and bound by formal legal procedures.

Empirically, Operation HAECHI VI has yielded significant results, including the blocking of more than 68,000 bank accounts, the freezing of approximately 400 crypto wallets, and the recovery of USD 16 million in illegal assets in the form of crypto, which is part of a total global financial recovery of USD 439 million (International Criminal Police Organization (INTERPOL), 2024). The jurisdictions involved span multiple regions, including Brazil, Portugal, and Thailand, demonstrating that crypto crime is cross-regional in nature and requires intensive multilateral coordination.

The success of Operation HAECHI VI was greatly influenced by informal communication mechanisms and rapid responses between Financial Intelligence Units (FIUs), which in practice are often more effective than formal mutual legal assistance channels, which are time-consuming (Campbell-Verduyn, 2018). The speed of blockchain transactions requires a real-time, adaptive, and network-based investigative approach, as recommended in the FATF's networked governance framework (De Vido, 2014; Kutera, 2022).

The FATF's risk-based approach supports the effectiveness of international investigations. It helps regulators focus on high-risk areas, such as cryptocurrency exchanges and virtual asset service providers (VASPs), rather than imposing blanket bans, which can lead to regulatory arbitrage and the migration of illegal activities to places with weak oversight (Atiyah et al., 2023; Kutera, 2022). Operation HAECHI VI represents the practical implementation of this approach by targeting the flow of funds and intermediary infrastructure within the crypto ecosystem.

However, study results also show that there's a global regulatory lag in managing virtual assets. The complexity of technical infrastructure, fragmented jurisdictions, and delays in adopting FATF recommendations,

including implementing the travel rule, still create loopholes that economic criminals can exploit (Zhang and Xu, 2019). This situation confirms that international operations such as HAECHI VI, although effective, cannot stand alone without sustained global policy harmonization.

Overall, research findings conclude that Operation HAECHI VI provides strong empirical evidence of the effectiveness of network-based international investigative cooperation in tackling cryptocurrency-based economic crime. The integration of FATF global standards, cross-agency law enforcement coordination, and the use of blockchain technology for transaction tracking has proven to be more adaptive than unilateral repressive approaches or total bans (Cumming et al., 2019; Nath, 2020).

Table 3. Results of HAECHI VI International Operation in Handling Cryptocurrency Crimes

Operational Components	Results Achieved	Jurisdictions Involved
Bank Accounts Blocked	68,000+ accounts	Global (including Brazil, Portugal, Thailand).
Crypto Wallets Frozen	~400 wallets	Cross-border collaboration with specialized cyber units.
Recovery of Illegal Profits	$16 million (crypto only)	Part of a total $439 million financial recovery.
Primary Target	*Pig butchering, romance scams, sextortion.*	Focus on crimes that cause massive harm to individuals.

Source : (International Criminal Police Organization (INTERPOL), 2025)

Operation HAECHI VI shows that informal communication channels and rapid response mechanisms between financial intelligence units (FIUs) are often more effective than slow formal legal channels in dealing with the speed of blockchain transactions (United Nations, 2025).

DISCUSSION

Discussions on international cooperation in crypto crime investigations highlight the race among countries to become legitimate jurisdictions that comply with AML standards (Kreminskyi et al., 2021). However, these efforts are often hampered by differing national interpretations of global regulations, creating blind spots for law enforcement.

The "Sunrise" Issue and Regulatory Arbitrage

The "Sunrise Issue" phenomenon occurs when one country implements rules such as the Travel Rule while its neighbors have not, resulting in transaction data being cut off midway (Kreminskyi et al., 2021). The "sunrise" issue in crypto asset regulation arises when some countries implement FATF travel rule standards while others do not, creating inconsistencies that are exploited by crypto exchanges and virtual asset service providers (VASPs) in regions with looser oversight to avoid compliance obligations (crypto gray markets) (Atiyah et al., 2023; Saha et al., 2024). Crypto operators can engage in regulatory arbitrage by moving to more lenient jurisdictions, often referred to as dark areas in the shadow financial system. Countries such as North Korea use Mandarin-language money laundering services and mixing protocols to obscure the trail of stolen funds before returning them to the legal financial system (Chainalysis, 2025a).

During the FATF's sunrise period, compliant and non-compliant exchanges can coexist, allowing assets to be traded on unregulated offshore markets while compliant markets limit their liquidity in accordance with applicable AML/CFT requirements (Allison, 2021; Fatarib and Sali, 2021). Non-uniformity is related to regulatory arbitrage, which involves moving operations or transactions to places with more favorable rules in order to reduce costs and avoid supervision. This has become a structural issue in the global crypto market and an area of exploitation for market participants and exchange infrastructure providers (Liang et al., 2025; Stephen, 2021).

Other studies emphasize that global regulatory fragmentation, triggered by differences in legal status, asset definitions, and supervisory approaches between countries, creates legal uncertainty for market participants and investors and opens up opportunities for regulatory arbitrage that impact market stability and the effectiveness of cross-jurisdictional law enforcement (Hardana et al., 2025). Sunrise problems and regulatory arbitrage can lead to differences in compliance with AML standards. This can also hinder broader market integration and encourage crypto activity to move to jurisdictions with weaker oversight. This has the potential to increase the risk of cross-border money laundering and abuse (Al-Tawil, 2023). Crypto actors can take advantage of global regulatory misalignment to optimize their operations while avoiding strict requirements imposed in other countries (Arnold, 2025; Ramassa and Leoni, 2022). The literature emphasizes the importance of international harmonization and risk-based adaptive frameworks to reduce arbitrage gaps. It also supports cross-jurisdictional collaboration, technological innovation, and consumer protection. Global policies need to unify compliance and provide clarity and legal protection for all market participants (Hardana et al., 2025).

Rapid Response Mechanism and Cross-Sectoral Collaboration

This mechanism is important for improving the effectiveness of handling economic crimes, including money laundering involving cryptocurrency, through better international cooperation (Aksa et al., 2024; Darojat et al., 2023). This cooperation must involve various countries to create harmonious and effective regulations in dealing with economic crimes related to cryptocurrency. Effective regulations will require support from international institutions and cooperation between countries to overcome the challenges that arise in the use of cryptocurrency (Virga, 2015). This collaborative effort should also include information sharing and joint investigations to identify and follow up on illegal activities involving cryptocurrencies (Kreminskyi et al., 2021; Movchan et al., 2023). A clear legal framework is essential to facilitate this collaboration and ensure that all countries can contribute effectively to law enforcement.

One of the main obstacles to international cooperation is the borderless nature of blockchain, where the proceeds of crime can quickly cross the globe. Meanwhile, formal cooperation through Mutual Legal Assistance Treaties (MLATs) can take days or weeks. To address this, in September 2025, the FATF, together with Interpol, the Egmont Group, and the UNODC, launched the Handbook on International Cooperation against Money Laundering. This guide encourages informal cooperation through secure communication channels and rapid response mechanisms for more flexible investigations. An example of the success of this model is the coordination between US and Indian authorities that seized $150 million worth of crypto assets related to drug trafficking.

Jurisdictional Dynamics: Cases of South Korea and Brazil

South Korea is demonstrating an increasingly preventive approach to law enforcement in virtual asset governance through strengthened regulations and oversight of Virtual Asset Service Providers (VASPs). The enactment of the Act on the Protection of Virtual Asset Users in July 2024 requires VASPs to implement customer asset segregation, stricter security standards, and insurance schemes to cover losses due to hacking, thereby enhancing consumer protection and the accountability of the crypto industry (Library of Congress, 2024). This policy was expanded in April 2025 through a revision of the Capital Markets Act, which grants the Financial Services Commission (FSC) the authority to preemptively freeze the crypto accounts of parties suspected of market manipulation, without having to wait for a court order, in order to prevent funds from being transferred to personal wallets or other jurisdictions (Sikder, 2025). Normatively, this approach is consistent with FATF recommendations that emphasize risk-based supervision of key nodes in the crypto ecosystem, although it still raises debates about the balance between effective law enforcement and protection of due process of law principles in the virtual asset regime (FATF, 2020b).

The Brazilian government officially adopted the OECD's Crypto-Asset Reporting Framework (CARF) in November 2024. This policy requires Brazilian citizens who conduct transactions through foreign service providers or P2P platforms to report transactions exceeding 30,000 Reais per month. Additionally, in November 2025, Brazil's OJK (BCB) issued a resolution requiring all foreign crypto exchanges to have a local subsidiary or partner with a licensed entity in Brazil to improve AML oversight and compliance (Chainalysis, 2025b).

Professionalization of Fraud and Exploitation AI

The development of artificial intelligence (AI) technology has changed the landscape of financial crime in the crypto ecosystem with an increasingly high level of complexity. Academic literature shows that AI, including machine learning, deep learning, and advanced algorithms, has been utilized to automate the detection of fraud patterns and, in parallel, provide new opportunities for criminal actors to scale their fraud schemes across various blockchain networks (Pérez-Cano and Jurado, 2025; Valencia et al., 2025). AI demonstrates capabilities that far exceed traditional methods, such as identifying complex transaction anomalies or hidden money laundering patterns in decentralized networks, but it also opens the door to exploitation by malicious actors due to its adaptive and unpredictable nature (Pérez-Cano and Jurado, 2025; Valencia et al., 2025). Economic crime is becoming increasingly organized with the emergence of transnational fraud centers, particularly in Southeast Asia, which use advanced technologies such as artificial intelligence (AI) to create more convincing fraudulent content (United Nation, 2025). The "Prince Group" case in Cambodia is a clear example of hundreds of workers being trafficked and forced to work in labor camps to run a pig butchering scheme that stole billions of dollars from victims around the world (Office of Public Affairs, 2025). The use of AI in generating adaptive malware code also increases the difficulty of detection for conventional digital security systems.

The integration of AI with blockchain faces unique challenges. On the one hand, this technology helps detect and prevent fraud with more accurate models. On the other hand, criminals also use the same technology to create more sophisticated crime schemes, such as hiding transaction patterns, manipulating smart contracts, or using anomaly detection to bypass conventional security systems (Pérez-Cano and Jurado, 2025; Valencia et al., 2025). Although federated learning and blockchain-based machine learning methods can improve fraud detection capabilities, challenges such as model bias, the need for high-quality labeled data, and model transparency remain significant obstacles to their practical application (Sidabutar et al., 2025; Taher et al., 2024). AI enhances fraud

operations by creating more convincing phishing messages and using smart contracts for rapid attacks. Fraud detection on networks such as Ethereum using deep learning is effective, but it also encourages the emergence of more sophisticated attack models to exploit existing loopholes (Sethy and Ray, 2025). Without adequate oversight and a clear policy framework, AI structures will provide double benefits to law enforcement and organized criminals, driving the professionalization of crypto fraud to a level far more complex than simple manual or traditional schemes.

The Evolution of Stablecoins and the Challenges of Asset Recovery

Stablecoins have become the backbone of illegal transactions because their stable value facilitates settlement compared to volatile Bitcoin (FATF, 2025). Until 2025, most illegal on-chain activities use stablecoins. The biggest challenge remains the low rate of asset recovery. The borderless nature of blockchain means that the proceeds of crime can cross From one country to another, while formal cooperation between authorities still takes days or weeks (United Nations, 2025). Therefore, accelerating inter-agency channels and closer coordination between investigators and prosecutors is vital for the prevention or the control of illegal stablecoins transactions.

The main challenge is low asset recovery rates. The borderless, fast, and decentralized nature of blockchain allows the proceeds of crime to move quickly between countries, while formal cooperation between countries, such as legal assistance and extradition, is slower (Tziakouris, 2018). This temporal imbalance creates a significant enforcement gap, where illegal assets often undergo a process of layering and obscuration before law enforcement authorities can effectively freeze or attach them (Abdramanova et al., 2019).

In this context, the risk-based and network-based governance approaches developed by the FATF become increasingly relevant. FATF emphasizes that recovering crypto assets, especially stablecoins, should not rely solely on national legal tools. It requires enhanced communication channels between institutions, real-time financial intelligence sharing, and closer coordination among investigators, financial intelligence units (FIU), and prosecutors across jurisdictions (De Vido, 2014; FATF, 2020a). This approach is also strengthened through public-private partnerships with virtual asset service providers (VASPs), which are positioned as critical nodes in the stablecoin transaction ecosystem and have the technical capacity to support rapid tracking and freezing of funds.

Thus, the evolving role of stablecoins not only increases the efficiency of global economic crime but also tests the limits of the effectiveness of international AML governance. Without cross-border coordination reforms and harmonization of FATF standards implementation, including strengthening the travel rule and asset recovery mechanisms, stablecoins have the potential to widen the gap between the speed of technological innovation and law enforcement capacity. These findings emphasize that the challenge of asset recovery is not merely a technical issue, but rather a structural one within the architecture of international cooperation in the era of decentralized finance.

Recommendations

Harmonizing global investigative standards should be a priority by developing uniform digital evidence protocols for real-time information exchange between jurisdictions. This requires a shift from slow formal legal processes to secure informal communication channels and rapid responses, as outlined in the FATF-Interpol-UNODC Handbook 2025. With harmonized standards, procedural barriers exploited by criminals to move assets can be minimized through direct coordination between investigators and prosecutors in different countries.

Improving human resource capacity and integrating artificial intelligence (AI)-based analytical technology are crucial for combating digital economic crime. Law enforcement authorities need to invest in blockchain forensics training for officers to more effectively track and seize illegal or criminal virtual assets. The use of advanced analytical tools to detect suspicious transaction patterns is also crucial to keep pace with the rapid innovation of payment systems.

Strengthening public-private partnerships and regulatory integration through a rigorous licensing model Should be accelerated to address the global regulatory arbitrage gap. Countries are encouraged to adopt collaborative oversight mechanisms, such as the MoU between the Financial Services Authority (Otoritas Jasa Keuangan (OJK)) and Dubai's Virtual Assets Regulatory Authority (VARA), and to require foreign crypto asset service providers to have a local entity or licensed partner to comply with Anti-Money Laundering (AML) standards. In addition, the development of an operational alert system involving financial intelligence and the private sector will be very helpful in strengthening early mitigation of the risk of misuse of crypto assets at the national and regional levels (Alonzo, 2024).

CONCLUSION

International regulatory and investigative cooperation is a prerequisite for safeguarding the integrity of the global financial system from the threat of crypto-related economic crime. While legal instruments like the European Union's MiCA and new regulations in Brazil and South Korea have provided a stronger framework, the

borderless nature of crypto still leaves room for exploitation by professional criminals, posing a serious threat to the state. Success in combating these crimes depends not only on the sophistication of tracking technology but also on the global political will to close regulatory arbitrage loopholes and expedite cross-border legal processes. With asset recovery rates still very low (3.8% in 2025), the future focus must be on prevention through the full implementation of the "Travel Rule" and enhancing real-time asset recovery capabilities through more agile cross-sectoral collaboration. Only through solid synergy between governments, international institutions, and the private sector can digital financial innovation thrive safely without becoming a tool for criminal activity that harms global society.

The implications of these findings call for a fundamental transformation of the global financial oversight architecture, with countries no longer able to stand alone in the face of organized cyber threats. Regulators face significant pressure to rapidly shift to an integrated regulatory model to prevent their jurisdictions from becoming blind spots in the global financial system. For law enforcement agencies, the limited asset recovery rate of only 3.8% implies the need for significant investment in AI-based blockchain forensics technology and increased human resource capacity to keep pace with the pace of criminal innovation. At a macro level, failure to close this regulatory gap threatens not only economic stability but also monetary sovereignty and national security, given the growing use of crypto as a means of financing organized crime and evading international sanctions.

REFERENCES

Abdramanova, N. K., Bekenova, A. B., Abayev, M. B., & Sstkey, T. B. (2019). Latent Crime Research Methodology in Europe, Commonwealth of Independent States (CIS) and Kazakhstan. *Journal of Advanced Research in Law and Economics, 10*(5 (43)), 1358–1369.

Abdulla, Z. K. (2020). The principles of territorial integrity of the states and self-determination of the people and their role in ensuring the international security and the international law and order. *Science and Life of Kazakhstan, 7*(2), 20–24.

Aksa, A., Hadiyanto, A., & Ciptono, C. (2024). Upaya Pemberantasan Tindak Pidana Pencucian Uang oleh Pusat Pelaporan Dan Analisis Transaksi Keuangan Melalui Kerjasama Internasional. *Jurnal USM Law Review, 7*(2), 586–602. https://doi.org/10.26623/julr.v7i2.8896

Al-Tawil, T. N. (2023). Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal of Money Laundering Control, 26*(6), 1150–1164. https://doi.org/10.1108/JMLC-07-2022-0109

Allison, I. (2021). Crypto 'Gray' Markets Could Be Unintended Consequence of FATF Travel Rule. *Coindesk*. https://www.coindesk.com/policy/2020/05/21/crypto-gray-markets-could-be-unintended-consequence-of-fatf-travel-rule?

Alonzo, B. (2024). Crypto Regulation (and De-Regulation) in the U.S. and E.U. and the Effects of Each on Consumer Protection and Illicit Transactions. *ILRA : International Law Review Association*. https://www.smu.edu/-/media/site/law/students/law-journals/alonzo_final.pdf

Anggriawan, R., & Susila, M. E. (2024). Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations. *Novum Jus, 18*(2), 249–277. https://doi.org/10.14718/NovumJus.2024.18.2.10

Apakhayev, N., Omarova, A. B., Kussainov, S., Nurahmetova, G. G., Buribayev, Y. A., Khamzina, Z. A., Kuandykov, B., Tlepina, S. V, & Kala, N. S. (2018). Review on the Outer Space Legislation: Problems and Prospects. *Statute Law Review, 39*(3), 258–265. https://doi.org/10.1093/slr/hmx010

Arnold, M. (2025). Gaps in crypto rules can be exploited, warns Financial Stability Board. *Financial Times*. https://www.ft.com/content/86593f5c-b524-4050-951b-d19ddcfb6158?

Atabekova, A., & Radic, N. (2020). EU legislative discourse on unaccompanied minors: Exploring conceptual-linguistic architecture. *Journal of Legal, Ethical and Regulatory, 23*(1).

Atiyah, G. A., Manap, N. A., & Aziz, S. N. A. (2023). Legal Status of Cryptocurrency Circulation in Iraq: Lessons from the United Arab Emirates and the United States. *Hasanuddin Law Review, 9*(1), 1. https://doi.org/10.20956/halrev.v9i1.3867

Balusamy, S., Rengasamy, R., & Aravind J. (2025). Protecting Financial Transactions and Cryptocurrency Networks from Fraud Using AI-Powered Blockchain Technology. *2025 Global Conference in Emerging Technology (GINOTECH)*, 1–6. https://doi.org/10.1109/GINOTECH63460.2025.11076940

Barone, R., & Masciandaro, D. (2019). Cryptocurrency or usury? Crime and alternative money laundering techniques. *European Journal of Law and Economics, 47*(2), 233–254. https://doi.org/10.1007/s10657-019-09609-6

Bloomberg, J. (2017). Using Bitcoin Or Other Cryptocurrency To Commit Crimes? Law Enforcement Is Onto You. *Forbes*. https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/?sh=6b8d0e3d3bdc

Braaten, C. N., & Vaughn, M. S. (2019). Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions. *Deviant Behavior, 42*(8), 958–978. https://doi.org/10.1080/01639625.2019.1706706

Brenig, C., Accorsi, R., & Möller, G. (2015). Economic analysis of cryptocurrency backed money laundering. *23rd European Conference on Information Systems, ECIS 2015, 2015*(May), 1–18.

Bulatov, N. K., Sarzhanov, D. K., Elubaev, S. Z., Suleymenov, T. B., Kasymzhanova, K. S., & Balabayev, O. T. (2019). Model of effective system of processing of organic wastes in biogas and environmental fuel production plant. *Food and Bioproducts Processing, 115*(May), 194–207. https://doi.org/10.1016/j.fbp.2019.03.005

Burova, A. Y., & Kabakov, V. V. (2020). "Unerroric" of multistage discrete Fourier transform of digital signal without arithmetic operations of multiplication. *Amazonia Investiga, 9*(25), 429–437. https://www.amazoniainvestiga.info/index.php/amazonia/article/view/1092

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change, 69*(2), 283–305. https://doi.org/10.1007/s10611-017-9756-5

Chainalysis. (2025a, December 18). North Korea Drives Record $2 Billion Crypto Theft Year, Pushing All-Time Total to $6.75 Billion. *Chainalysis*. https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/

Chainalysis. (2025b, December 23). 2025 Crypto Regulatory Round-Up: What Changed and What's Ahead. *www.chainalysis.com*. https://www.chainalysis.com/blog/2025-crypto-regulatory-round-up/

Cumming, D. J., Johan, S., & Pant, A. (2019). Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty. *Journal of Risk and Financial Management, 12*(3), 126. https://doi.org/10.3390/jrfm12030126

Darojat, M. I., Yahya, A., Wahyudi, D., & Firdaus, G. R. Y. (2023). Pencucian Uang Lintas Negara dengan Menggunakan Cryptocurrency: Perspektif Bentuk Kerjasama Penanganan Antar Negara. *Jurnal Anti Korupsi, 12*(2), 60. https://doi.org/10.19184/jak.v12i2.38823

De Vido, S. (2014). Network regulation of cross-border economic crime. *Kobe University Law Review, 48*, 83–97.

Dumchikov, M., Kononenko, N., Batsenko, L., Halenin, R., & Hlushchenko, N. (2020). Issues of regulating cryptocurrency and control over its turnover: international experience. *Revista Amazonia Investiga, 9*(31), 10–20. https://doi.org/10.34069/AI/2020.31.07.1

Dyntu, V., & Dykyi, O. (2018). Cryptocurrency in the system of money laundering. *Baltic Journal of Economic Studies, 4*(5), 75–81.

Fatarib, H., & Sali, M. A. (2021). Cryptocurrency And Digital Money in Islamic Law: Is it Legal? *Jurisdictie, 11*(2), 237–261. https://doi.org/10.18860/j.v11i2.8687

FATF. (2020a). 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs. *Financial Action Task Force*. https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html

FATF. (2020b). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. *Financial Action Task Force*.

FATF. (2024). Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs. *Financial Action Task Force*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html?

FATF. (2025, June). FATF urges stronger global action to address Illicit Finance Risks in Virtual Assets. *www.fatf-gafi.org*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

Frediani, M. E. A. (2024). Crafting the Future of Finance: A Comparative Analysis of Cryptocurrency Regulation in the Global Economy. *Journal of Financial Risk Management, 13*(01), 193–206. https://doi.org/10.4236/jfrm.2024.131010

Hardana, A., Siregar, S. E., & Utami, T. W. (2025). Tantangan Hukum dalam Regulasi Cryptocurrency di Era Ekonomi Digital Global. *Jurnal Hukum Bisnis, 14*(4), 1–12. https://doi.org/10.47709/jhb.v14i04.6775

Haydanka, Y. L. (2019). The Public and political scope of decentralisation in the Trnava region of Slovakia. *Tomsk State University Journal, 444*, 101–109.

Huberman, G., Leshno, J. D., & Moallemi, C. (2021). Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *The Review of Economic Studies, 88*(6), 3011–3040. https://doi.org/10.1093/restud/rdab014

International Criminal Police Organization (INTERPOL). (2024). Global Financial Fraud Assessment (Issue May). *www.interpol.int.*

International Criminal Police Organization (INTERPOL). (2025, September 24). USD 439 million recovered in global financial crime operation. *www.interpol.int*. https://www.interpol.int/News-and-Events/News/2025/USD-439-million-recovered-in-global-financial-crime-operation

Kamps, J., & Kleinberg, B. (2018). To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science, 7*(1), 18. https://doi.org/10.1186/s40163-018-0093-5

Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review, 30*(3), 325–344. https://doi.org/10.1177/1057567719827051

Khamzin, A. S., Aldashev, S., Tileubergenov, Y. M., Kussainova, A. K., Khamzina, Z. A., & Buribayev, Y. A. (2016). Legal regulation of employment in Kazakhstan. *International Journal of Environmental and Science Education, 11*(18), 11907–11916.

Kharisma, D., Swandiani, N. L. P. E., & Paliwang, A. N. A. A. (2025). The Role of Interpol in Addressing Transnational Cybercrime: A Review of Global Law Enforcement Collaboration in Southeast Asia. *Perkara : Jurnal Ilmu Hukum Dan Politik, 3*(2), 860–875. https://doi.org/10.51903/nrcgp489

Kovalchuk, O., Shevchuk, R., & Banakh, S. (2024). Cryptocurrency Crime Risks Modeling: Environment, E-Commerce, and Cybersecurity Issue. *IEEE Access, 12*, 50673–50688. https://doi.org/10.1109/ACCESS.2024.3386428

Kreminskyi, O., Kuzmenko, O., Antoniuk, A., & Smahlo, O. (2021). International cooperation in the investigation of economic crimes related to cryptocurrency circulation. *Estudios de Economia Aplicada, 39*(6). https://doi.org/10.25115/eea.v39i6.5247

Kutera, M. (2022). Cryptocurrencies as a subject of financial fraud. *Journal of Entrepreneurship, Management and Innovation, 18*(4), 45–77. https://doi.org/10.7341/20221842

Liang, W., Peterson, B., Owen, J., & Taofeek, A. (2025). Regulatory Arbitrage in Global Cryptocurrency Exchanges: Gaps in AML/CFT Enforcement. https://www.researchgate.net/publication/395384821_Regulatory_Arbitrage_in_Global_Cryptocurrency_Exchanges_Gaps_in_AMLCFT_Enforcement

Library of Congress. (2024). South Korea: Act to Regulate Cryptocurrency Markets Goes into Effect. *www.loc.gov*. https://www.loc.gov/item/global-legal-monitor/2024-07-18/south-korea-act-to-regulate-cryptocurrency-markets-goes-into-effect/?

Movchan, A., Shliakhovskyi, O., Kozii, V., & Fedchak, I. (2023). Investigating cryptocurrency financing crimes terrorism and armed aggression. *Social Legal Studios, 6*(4), 123–131. https://doi.org/10.32518/sals4.2023.123

Nahorniak, I., Leonova, K., & Skorokhod, V. (2016). Cryptocurrency in the context of development of digital single market in European Union. *InterEULawEast: Journal for the International and European Law, Economics and Market Integrations, 3*(1), 107–124. https://hrcak.srce.hr/160591

Nath, G. V. M. (2020). Cryptocurrency Crimes – Need for a Comprehensive Global Crypto Regulation. *SSRN Electronic Journal, August 31*, 2020. https://doi.org/10.2139/ssrn.3683669

Norton Rose Fulbright. (2024, October). Regulating crypto-assets in Europe: Practical guide to MiCA. *Nortonrosefulbright*. https://www.nortonrosefulbright.com/en/knowledge/publications/2cec201e/regulating-crypto-assets-in-europe-practical-guide-to-mica

Office of Public Affairs. (2025, October 14). Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes. *www.justice.gov*. https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged

Oxford Analytica. (2017). Law will lag international cryptocurrency crime (Emerald Expert Briefings). https://doi.org/10.1108/OXAN-DB222104

Pérez-Cano, V., & Jurado, F. (2025). Fraud Detection in Cryptocurrency Networks—An Exploration Using Anomaly Detection and Heterogeneous Graph Transformers. *Future Internet, 17*(1), 44. https://doi.org/10.3390/fi17010044

Piddubnyi, O. Y., Piddubna, D., Horislavska, I. V., Koval, A. M., & Lebid, I. . (2019). Interaction of psychology and ecological-legal personality on the way of formation of normative-legal regulation in the 21st century. *Asia Life Sciences, 1*(1), 287–302.

Ramassa, P., & Leoni, G. (2022). Standard setting in times of technological change: accounting for cryptocurrency holdings. *Accounting, Auditing & Accountability Journal, 35*(7), 1598–1624. https://doi.org/10.1108/AAAJ-10-2020-4968

Saha, S., Hasan, A. R., Mahmud, A., Ahmed, N., Parvin, N., & Karmakar, H. (2024). Cryptocurrency and financial crimes: A bibliometric analysis and future research agenda. *Multidisciplinary Reviews, 7*(8), 2024168. https://doi.org/10.31893/multirev.2024168

Sanction Scanner. (2024, July 4). Cryptocurrency Regulations in Brazil. *www.sanctionscanner.com*. https://www.sanctionscanner.com/blog/cryptocurrency-regulations-in-brazil-1153

Sethy, A., & Ray, A. (2025). Detection of fraudulent transactions in Ethereum blockchain smart contracts using deep learning. *International Journal of Information Technology*. https://doi.org/10.1007/s41870-025-02900-7

Sidabutar, N. R., Kesuma, S. A., Nasution, F. N., & Erwin, K. (2025). Artificial Intelligence, Big Data, and Blockchain Technologies in Financial Fraud Detection: A Systematic Literature Review. *COSTING : Journal of Economic, Bussines and Accounting, 8*(6).

Sikder, T. (2025, November 28). South Korea to Tighten Crypto Travel Rule Below $680, Block "High Risk" Offshore Exchanges. *Finance Magnates*. https://www.financemagnates.com/cryptocurrency/south-korea-to-tighten-crypto-travel-rule-below-680-block-high-risk-offshore-exchanges/

Singh, K. (2015). The New Wild West: Preventing Money Laundering in the Bitcoin Network. *Northwestern Journal of Technology and Intellectual Property, 13*(1), 37–64.

Solodan, K. (2019). Legal Regulation Of Cryptocurrency Taxation in European Countries. *European Journal of Law and Public Administration, 6*(1), 64–74. https://www.ceeol.com/search/article-detail?id=795370

Spithoven, A. (2019). Theory and Reality of Cryptocurrency Governance. *Journal of Economic Issues, 53*(2), 385–393. https://doi.org/10.1080/00213624.2019.1594518

Stephen, R. (2021). Regulatory Arbitrage in Cryptocurrency Markets: Global Perspectives. https://doi.org/https://www.researchgate.net/profile/Joenn-Asher/publication/395726554_Regulatory_Arbitrage_in_Cryptocurrency_Markets_Global_Perspectives/links/68d2205f220a341aa14e750a/Regulatory-Arbitrage-in-Cryptocurrency-Markets-Global-Perspectives.pdf

Stroukal, D. (2016). Bitcoin and other cryptocurrency as an instrument of crime in cyberspace. *International Institute of Social and Economic Sciences 4407036*. https://ideas.repec.org/p/sek/ibmpro/4407036.html

Suwitra, I. K., Hadiyanto, A., & Ciptono, C. (2024). Pencegahan Tindak Pidana Pencucian Uang Melalui Lintas Internasional Dalam Perspektif Undang-Undang Tindak Pidana Pencucian Uang. *Jurnal USM Law Review, 7*(2), 960–973. https://doi.org/10.26623/julr.v7i2.9434

Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach. *Engineering, Technology & Applied Science Research, 14*(1), 12822–12830. https://doi.org/10.48084/etasr.6641

Tu, K. V., & Meredith, M. W. (2015). Rethinking Virtual Currency Regulation in the Bitcoin Age. *The Banking and Finance Law Commons, Washington Law Review, 90*(1), 271.

Tziakouris, G. (2018). Cryptocurrencies A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective. *IEEE Security & Privacy, 16*(4), 92–94. https://doi.org/10.1109/MSP.2018.3111243

United Nation. (2025). Leveraging crypto: Southeast Asian experts strengthen regional cooperation in Brunei. www.unodc.org.

United Nations. (2025, October 28). Global experts advance the joint fight against crypto-enabled crime. *www.unodc.org*. https://www.unodc.org/corruption/en/news/2025-10-28_global-experts-advance-the-joint-fight-against-crypto-enabled-crime.html

Valencia, L. R., Arellano, M. J. O., Figueroa, S. A. G., Nuño, C. M., Piqueras, B. M., Paredes, A. del V. C., Rosende, S. B., López, J. M., Sanz, E. P., & Alfaroviz, A. L. (2025). A Systematic Review of Artificial Intelligence Applied to Compliance: Fraud Detection in Cryptocurrency Transactions. *Journal of Risk and Financial Management, 18*(11), 612. https://doi.org/10.3390/jrfm18110612

Vasylieva, M., Zelisko, A. V., & Zozuliak, O. I. (2018). Cooperatives in Ukraine: Applicative Peculiarities of Legal

Integration up to the EU Standards. *Journal of Advanced Research in Law and Economics, 5*(35), 1789–1797.

Virga, J. M. (2015). International criminals and their virtual currencies: the need for an international effort in regulating virtual currencies and combating cyber crime. *Revista de Direito Internacional, 12*(2). https://doi.org/10.5102/rdi.v12i2.3557

Widhiyanti, H. N., Hussein, S. M., & Ganindha, R. (2023). Indonesian Cryptocurrencies Legislative Readiness: Lessons from the United States. *Sriwijaya Law Review, 7*(1), 150–172. https://doi.org/10.28946/slrev.vol7.iss1.2138

Zelisko, A. V., Zozuliak, O. I., & Sishchuk, L. V. (2018). Legal Regulation of the Non-Entrepreneurial Legal Entities' Status: Foreign Experience. *Journal of Advanced Research in Law and Economics, 9*(5(35)), 1806–1818.

Zhang, N., & Xu, Y. (2019). Environmental Study on Cooperation System of Crossborder Tracking Economic Crimes based on Block Chain-Take telecommunication fraud as an example. *Ekoloji Dergisi, 107*.