



THE PROSECUTOR LAW REVIEW

DITERBITKAN OLEH PUSAT STRATEGI KEBIJAKAN
PENEGAKAN HUKUM, KEJAKSAAN AGUNG

P - ISSN : 2987 - 7342 E- ISSN : 2987 - 8314

AVAILABLE ONLINE
<https://prolev.kejaksaan.go.id/>



Prosecutor's Role in Prosecuting Cryptocurrency-Related Transnational Crimes

Peran Jaksa dalam Menuntut Kejahatan Transnasional Terkait Cryptocurrency

Rita Komalasari¹, Cecep Mustafa²

¹Yarsi University, Indonesia

²Stirling University, United Kingdom

Article Info

Corresponding Author:

Fadli Alfariis

✉ rita.komalasari161@gmail.com

History:

Submitted: 12-09-2024

Revised: 24-04-2025

Accepted: 25-05-2025

Keyword:

Cryptocurrency Assets, Informal Cooperation, Transnational Cases, International Stakeholders

Kata Kunci:

Aset Cryptocurrency, Kerjasama Informal, Kasus Transnasional, Pihak-Pihak Internasional



Copyright © 2025
by The Prosecutor
Law Review.

All writings published in this journal are personal views of the authors and do not represent the views of the Attorney General Office of Indonesia.

Abstract

This study, titled Prosecutor's Role in Prosecuting Cryptocurrency-Related Transnational Crimes, aims to comprehensively analyze the crucial role of informal cooperation in addressing the challenges posed by cryptocurrency assets in transnational cases. It provides insights into how informal cooperation mechanisms among international stakeholders are vital for prosecutors in managing the complexities of cryptocurrency-related investigations. The study finds that informal cooperation is indispensable for prosecutors, offering strengths such as agility, flexibility, and effective information exchange. It also identifies weaknesses like information asymmetry and coordination issues. The analysis underscores the importance of enhancing collaborative relationships among international stakeholders and offers recommendations for improving informal cooperation mechanisms to better support prosecutorial efforts.

Abstrak

Studi ini, yang berjudul "Peran Jaksa dalam Menuntut Tindak Pidana Transnasional Terkait Cryptocurrency," bertujuan untuk menganalisis secara komprehensif peran penting dari kerja sama informal dalam mengatasi tantangan yang ditimbulkan oleh aset cryptocurrency dalam kasus transnasional. Studi ini memberikan wawasan tentang bagaimana mekanisme kerja sama informal antara pemangku kepentingan internasional sangat penting bagi jaksa dalam mengelola kompleksitas penyelidikan terkait cryptocurrency. Penelitian ini menemukan bahwa kerja sama informal sangat diperlukan bagi jaksa, menawarkan kekuatan seperti kelincahan, fleksibilitas, dan pertukaran informasi yang efektif. Studi ini juga mengidentifikasi kelemahan seperti asimetri informasi dan masalah koordinasi. Analisis ini menekankan pentingnya meningkatkan hubungan kolaboratif antara pemangku kepentingan internasional dan menawarkan rekomendasi untuk memperbaiki mekanisme kerja sama informal guna mendukung upaya penuntutan dengan lebih baik.

A. INTRODUCTION

1. Background

Prosecutor's Role in Prosecuting Cryptocurrency-Related Transnational Crimes. Cryptocurrencies, with their decentralized nature and pseudonymous transactions, have created a unique environment that transcends traditional borders, presenting significant hurdles for authorities investigating transnational cases involving digital assets.¹ As such, effective cooperation among international stakeholders is paramount to address the complexities associated with these cases. This study delves into the intricacies of informal cooperation in handling transnational cases involving cryptocurrency assets. It begins by contextualizing the significance of cryptocurrency assets in today's global financial system, elucidating their features that pose challenges to traditional investigation methods. Subsequently, the study examines the structure of informal cooperation mechanisms among international stakeholders, highlighting the roles played by various entities such as law enforcement agencies, regulatory bodies, and financial institutions.

The research on informal cooperation in handling transnational cases with cryptocurrency assets contributes novel insights and perspectives to the field of taking evidence of cryptocurrency assets in several key ways:² This research provides a thorough examination of the informal cooperation mechanisms employed by international stakeholders, shedding light on their structures, functions, and effectiveness in addressing transnational cases involving cryptocurrency assets. By offering a comprehensive analysis, the study enhances understanding of how informal cooperation complements formal legal frameworks in navigating the challenges posed by digital assets. Through a critical evaluation, this research identifies the strengths and weaknesses of informal cooperation mechanisms in handling cryptocurrency-related transnational cases. By delineating these aspects, the study offers valuable insights into the practical implications of informal cooperation and informs strategies for optimizing collaborative efforts among international stakeholders. By incorporating real-world case studies and examples, this research illustrates the practical implications of informal cooperation in addressing transnational cases involving cryptocurrency assets. By

¹Collins, John. "Crypto, crime and control." Cryptocurrencies as an enabler of organized crime, *Global Initiative Against Transnational Organized Crime* (2022).

² Laksono, Hazmi Tri, and Muhammad Fuadillah Nugraha. "Cryptocurrency Fever: Should Southeast Asian countries cooperate on facing the cryptocurrency market." *Proceedings of Airlangga Conference on International Relations (ACIR 2018) Politics, Economy, and Security in the Changing Indo-Pacific Region*. 2021. <https://doi.org/10.5220/0010276603240330>

analyzing these cases, the study provides concrete evidence of the efficacy of informal cooperation mechanisms and elucidates their impact on the outcomes of investigations and legal proceedings. Building upon the analysis of strengths and weaknesses, this research identifies potential areas for improvement in informal cooperation mechanisms. By pinpointing specific challenges and shortcomings, the study informs strategies for enhancing the effectiveness of collaborative efforts among international stakeholders in handling cryptocurrency-related transnational cases. Through its central argument, this research advocates for the importance of collaborative approaches in addressing the challenges posed by cryptocurrency assets in transnational cases. By emphasizing the necessity of fostering collaborative relationships among international stakeholders, the study underscores the value of informal cooperation alongside formal legal frameworks in combating illicit activities and upholding the integrity of the financial system. This research offers a nuanced understanding of the role of informal cooperation in taking evidence of cryptocurrency assets, providing valuable insights and perspectives that contribute to the advancement of knowledge in this rapidly evolving field.

Existing literature on the role of informal cooperation in addressing the challenges posed by cryptocurrency assets in transnational cases often lacks a comprehensive analysis that encompasses the various dimensions of collaborative efforts among international stakeholders.³ Several key gaps in the literature can be identified, and this study seeks to address these gaps through its focused analysis: Much of the existing literature tends to focus on formal legal frameworks for international cooperation, with limited attention given to informal mechanisms. This study fills this gap by providing a detailed analysis of informal cooperation mechanisms, including information sharing, expertise exchange, and collaborative efforts among law enforcement agencies, regulatory bodies, and financial institutions. While some literature discusses the theoretical aspects of informal cooperation, there is often a lack of empirical evidence and real-world case studies to illustrate its practical implications.⁴ This study addresses this gap by incorporating real-world examples and case studies to demonstrate the impact of informal cooperation on the outcomes of transnational cases involving cryptocurrency assets. Existing literature may overlook the strengths and weaknesses of informal

³ Reinsberg, Bernhard. "Fully-automated liberalism? Blockchain technology and international cooperation in an anarchic world." *International Theory* 13.2 (2021): 287-313. <https://doi.org/10.1017/S1752971920000305>

⁴ Kethineni, Sessa, and Ying Cao. "The rise in popularity of cryptocurrency and associated criminal activity." *International Criminal Justice Review* 30.3 (2020): 325-344. <https://doi.org/10.1177/1057567719827051>

cooperation mechanisms in addressing the challenges posed by cryptocurrency assets. This study fills this gap by conducting a critical evaluation of informal cooperation, identifying its strengths, such as agility and flexibility, as well as its weaknesses, such as potential information asymmetry and coordination issues. The literature may lack detailed discussions on specific strategies for fostering effective collaboration among international stakeholders in handling cryptocurrency-related transnational cases. This study addresses this gap by examining various collaboration strategies, such as joint investigations, task forces, and information-sharing platforms, and assessing their effectiveness in different contexts. Many existing studies fail to provide concrete recommendations for enhancing informal cooperation mechanisms in addressing the challenges posed by cryptocurrency assets. This study fills this gap by identifying specific areas for improvement, such as enhancing trust and transparency among stakeholders, streamlining information-sharing protocols, and leveraging technological solutions for collaboration. By addressing these gaps in the literature, this study contributes to a more comprehensive understanding of the role of informal cooperation in addressing the challenges posed by cryptocurrency assets in transnational cases. Through its detailed analysis and practical insights, the study aims to inform policymakers, law enforcement agencies, and other relevant stakeholders about the importance of informal cooperation in combating illicit activities in the digital age.

2. Research Question

"How can informal cooperation mechanisms, such as joint task forces, information-sharing platforms, and technological solutions, be effectively utilized to address the challenges posed by cryptocurrency assets in transnational cases, and what factors contribute to successful collaboration among international stakeholders in combating illicit activities involving digital assets?"

3. Method

Literature study serves as a foundational method for understanding the landscape of informal cooperation in addressing challenges posed by cryptocurrency assets. By reviewing scholarly articles, reports, and case studies, insights into existing practices, challenges, and opportunities for collaboration are gleaned. Data analysis involves synthesizing findings from the literature study to identify common themes, trends, and gaps in the literature. This analysis informs the development of the study's arguments,

providing a comprehensive overview of the role of informal cooperation in combating cryptocurrency-related transnational cases.

B. DISCUSSION

1. Effective Cooperation Among International Stakeholders

In transnational cases involving cryptocurrency assets, jurisdictional boundaries often complicate investigation and prosecution efforts.⁵ Effective cooperation among international stakeholders, including law enforcement agencies, regulatory bodies, and financial institutions, is essential for overcoming these barriers. By sharing intelligence, coordinating enforcement actions, and aligning regulatory approaches, international stakeholders can enhance their collective ability to combat illicit activities and hold perpetrators accountable across borders. Cryptocurrency-related crimes require specialized knowledge and expertise in areas such as blockchain technology, digital forensics, and financial investigations. Effective cooperation allows international stakeholders to leverage their respective strengths and resources, pooling expertise from diverse fields to develop comprehensive strategies for addressing the challenges posed by cryptocurrency assets. By sharing best practices, training programs, and technical resources, stakeholders can enhance their capacity to investigate and prosecute cryptocurrency-related crimes effectively.

Information sharing is paramount in transnational cases involving cryptocurrency assets, as timely and accurate intelligence is crucial for identifying perpetrators, tracing illicit funds, and disrupting criminal networks.⁶ Effective cooperation mechanisms, such as information-sharing platforms, joint task forces, and mutual legal assistance treaties, facilitate the exchange of intelligence among international stakeholders, enabling swift and coordinated responses to emerging threats. By fostering a culture of transparency and collaboration, stakeholders can enhance their ability to detect, investigate, and prevent cryptocurrency-related crimes. Cryptocurrency assets operate in a globalized digital economy, where regulatory frameworks vary widely across jurisdictions. Effective cooperation among

⁵ Teichmann, Fabian Maximilian Johannes, and Marie-Christin Falker. "Cryptocurrencies and financial crime: solutions from Liechtenstein." *Journal of Money Laundering Control* 24.4 (2021): 775-788. <https://doi.org/10.1108/JMLC-05-2020-0060>

⁶ Ilbiz, Ethem, and Christian Kaunert. "Sharing Economy for Tackling Crypto-Laundering: The Europol Associated 'Global Conference on Criminal Finances and Cryptocurrencies'." *Sustainability* 14.11 (2022): 6618. <https://doi.org/10.3390/su14116618>

international stakeholders is essential for promoting consistency in regulatory approaches, ensuring that regulations are harmonized and aligned to address the challenges posed by cryptocurrency assets. By sharing regulatory insights, coordinating policy development, and harmonizing enforcement actions, stakeholders can create a more cohesive regulatory environment that fosters innovation, protects investors, and mitigates risks associated with cryptocurrency assets. Effective cooperation among international stakeholders requires building trust and partnerships based on mutual respect, shared goals, and transparent communication. By establishing collaborative relationships, stakeholders can overcome barriers to cooperation, foster greater information sharing, and enhance their collective ability to address the challenges posed by cryptocurrency assets. By cultivating trust and partnerships, stakeholders can create a supportive ecosystem that facilitates collaborative efforts and strengthens the global response to cryptocurrency-related crimes. Effective cooperation among international stakeholders is essential for addressing the challenges posed by cryptocurrency assets in transnational cases. By navigating jurisdictional boundaries, leveraging specialized expertise, enhancing information sharing, promoting regulatory consistency, and building trust and partnerships, stakeholders can enhance their collective ability to combat illicit activities and uphold the integrity of the global financial system in the digital age.

2. Informal Cooperation Mechanisms

Informal cooperation mechanisms refer to collaborative efforts among international stakeholders that occur outside formal legal frameworks.⁷ These mechanisms facilitate information sharing, expertise exchange, and collaborative actions among law enforcement agencies, regulatory bodies, financial institutions, and other relevant entities involved in addressing transnational cases involving cryptocurrency assets. Informal cooperation often involves the establishment of information sharing platforms, such as networks, databases, and secure communication channels, where stakeholders can exchange intelligence and share insights on emerging threats and trends related to cryptocurrency assets. These platforms enable real-time collaboration, facilitating swift responses to evolving

⁷ Golonka, Anna. "Cooperation with third countries in combating money laundering in the face of modern challenges." *Ius Novum* 17.4 (2023): 15-39. <https://doi.org/10.2478/in-2023-0027>

challenges and enhancing stakeholders' collective ability to detect, investigate, and prevent illicit activities.

Informal cooperation may also take the form of joint task forces and working groups composed of representatives from multiple jurisdictions and sectors. These collaborative initiatives bring together experts with diverse backgrounds and skill sets to tackle specific challenges associated with cryptocurrency-related transnational cases. By pooling resources, sharing expertise, and coordinating efforts, joint task forces and working groups can enhance the effectiveness of investigations and enforcement actions. Informal cooperation mechanisms often involve mutual assistance and support among international stakeholders, where entities provide each other with technical assistance, training, and capacity-building initiatives to enhance their capabilities in addressing cryptocurrency-related crimes. By fostering a culture of collaboration and knowledge exchange, stakeholders can strengthen their collective response to emerging threats and challenges in the digital asset space.

In addition to formalized mechanisms, informal cooperation may also encompass ad hoc collaborative efforts initiated in response to specific incidents or crises involving cryptocurrency assets. These ad hoc collaborations enable stakeholders to mobilize resources, share intelligence, and coordinate actions quickly and effectively, without the bureaucratic constraints associated with formal legal frameworks. By embracing flexibility and adaptability, stakeholders can leverage ad hoc collaborations to address emerging threats and mitigate risks associated with cryptocurrency assets. Informal cooperation mechanisms play a critical role in facilitating collaboration among international stakeholders in addressing the challenges posed by cryptocurrency assets in transnational cases. By providing platforms for information sharing, fostering joint initiatives, facilitating mutual assistance, and supporting ad hoc collaborative efforts, informal cooperation mechanisms enhance stakeholders' collective ability to combat illicit activities and uphold the integrity of the global financial system.

Information sharing is paramount in addressing transnational cases involving cryptocurrency assets, as timely and accurate intelligence is crucial for identifying perpetrators, tracing illicit funds, and disrupting criminal networks.⁸ Law enforcement

⁸ Gilmour, Paul Michael. "Decentralized blockchain technology: towards a trusted and transparent beneficial ownership regime." *Financial Technology and the Law: Combating Financial Crime*. Cham: Springer International Publishing, 2022. 185-209. https://doi.org/10.1007/978-3-030-88036-1_8

agencies, regulatory bodies, and financial institutions play key roles in collecting, analyzing, and disseminating information related to cryptocurrency-related crimes, making collaboration and coordination essential for effective outcomes. Law enforcement agencies, including national police forces, investigative agencies, and Interpol, are responsible for investigating and prosecuting cryptocurrency-related crimes such as money laundering, fraud, and cybercrime. These agencies gather intelligence from various sources, including financial transactions, digital forensics, and open-source intelligence, to identify suspects and gather evidence. By sharing intelligence with international counterparts through channels such as secure communication platforms and joint task forces, law enforcement agencies can enhance their investigative capabilities and pursue transnational cases more effectively.

Regulatory bodies, such as financial intelligence units (FIUs), securities commissions, and central banks, are responsible for overseeing and regulating cryptocurrency activities within their respective jurisdictions. These bodies monitor cryptocurrency exchanges, initial coin offerings (ICOs), and other crypto-related entities to detect and prevent illicit activities, such as money laundering, terrorist financing, and securities fraud. By sharing regulatory insights, enforcement actions, and best practices with international counterparts through channels such as information-sharing platforms and regulatory forums, regulatory bodies can enhance their collective ability to combat illicit activities and safeguard the integrity of the global financial system. Financial institutions, including banks, cryptocurrency exchanges, and payment processors, play a crucial role in facilitating transactions involving cryptocurrency assets. ⁹These institutions are required to implement anti-money laundering (AML) and know your customer (KYC) procedures to mitigate the risks associated with cryptocurrency-related crimes. By sharing transaction data, suspicious activity reports (SARs), and other relevant information with law enforcement agencies and regulatory bodies, financial institutions can contribute to the detection and prevention of illicit activities involving cryptocurrency assets. Despite the importance of information sharing, challenges such as data privacy concerns, legal restrictions, and jurisdictional differences may impede collaboration among law enforcement agencies, regulatory bodies, and financial institutions.

⁹ Iarutin, Iaroslav K., and Elena E. Gulyaeva. "International and Russian Legal Regulation of the Turnover of Crypto-assets: Conceptual-Terminological Correlation." *Journal of Digital Technologies and Law* 1.3 (2023): 725-751. <https://doi.org/10.21202/jdtl.2023.32>

Overcoming these challenges requires the establishment of secure and trusted communication channels, the development of standardized protocols for information sharing, and the alignment of legal frameworks to facilitate cross-border cooperation. By addressing these challenges and fostering a culture of collaboration, stakeholders can enhance their collective ability to combat cryptocurrency-related crimes and uphold the integrity of the global financial system.

Investigating cryptocurrency-related crimes requires specialized knowledge and expertise in areas such as blockchain technology, digital forensics, financial investigations, and cybercrime. Given the complex and evolving nature of cryptocurrency assets, law enforcement agencies, regulatory bodies, and financial institutions must exchange expertise and collaborate to effectively address these challenges. Cryptocurrency investigations often involve analyzing blockchain transactions, tracing digital asset movements, and identifying patterns of illicit activity. Law enforcement agencies and regulatory bodies can exchange technical knowledge and tools for blockchain analysis, digital forensics, and data analytics to enhance their investigative capabilities. By sharing best practices, training programs, and technical resources, stakeholders can build their capacity to investigate and prosecute cryptocurrency-related crimes effectively.

Collaborative partnerships between law enforcement agencies, regulatory bodies, financial institutions, and technology experts are essential for addressing the challenges posed by cryptocurrency assets.¹⁰ These partnerships enable stakeholders to pool resources, share expertise, and coordinate efforts to combat illicit activities such as money laundering, fraud, and cybercrime. By fostering a collaborative ecosystem, stakeholders can leverage their collective strengths and capabilities to disrupt criminal networks and safeguard the integrity of the financial system. Joint investigations and task forces bring together experts from multiple jurisdictions and sectors to tackle specific cryptocurrency-related crimes. These collaborative initiatives enable stakeholders to share intelligence, coordinate enforcement actions, and pursue complex cases involving cross-border transactions and international criminal networks. By leveraging their combined expertise and resources, joint investigations and task forces can enhance their effectiveness in identifying perpetrators, gathering

¹⁰ Arifin, Ridwan, Sigit Riyanto, and Akbar Kurnia Putra. "Collaborative efforts in ASEAN for global asset recovery frameworks to combat corruption in the digital era." *Legality: Jurnal Ilmiah Hukum* 31.2 (2023): 329-343. <https://doi.org/10.22219/ljih.v31i2.29381>

evidence, and securing convictions. Capacity-building initiatives, such as training programs, workshops, and knowledge-sharing platforms, play a crucial role in enhancing stakeholders' expertise in investigating cryptocurrency-related crimes. These initiatives provide stakeholders with opportunities to learn from leading experts, acquire new skills and techniques, and stay abreast of emerging trends and developments in the digital asset space. By investing in capacity-building initiatives, stakeholders can strengthen their collective ability to address the challenges posed by cryptocurrency assets and adapt to evolving threats in the digital age. Expertise exchange and collaborative efforts are essential for investigating cryptocurrency-related crimes effectively. By sharing technical knowledge, building collaborative partnerships, conducting joint investigations, and investing in capacity-building initiatives, stakeholders can enhance their collective ability to combat illicit activities and uphold the integrity of the financial system in the digital age.

3. Case Studies Illustrating the Practical Implications of Informal Cooperation

Operation Tovar (2014): Operation Tovar, led by international law enforcement agencies including the FBI, Europol, and Interpol, targeted the Gameover Zeus botnet and the CryptoLocker ransomware scheme.¹¹ This operation exemplifies the practical implications of informal cooperation in combating cryptocurrency-related cybercrimes. Law enforcement agencies collaborated across borders to disrupt criminal infrastructure, dismantle botnets, and apprehend suspects involved in distributing malware and extorting victims for ransom payments in Bitcoin. Through real-time information sharing, joint investigations, and coordinated enforcement actions, international stakeholders successfully disrupted criminal networks and safeguarded millions of dollars in stolen funds.

AlphaBay Takedown (2017): The takedown of AlphaBay, one of the largest dark web marketplaces facilitating illegal transactions in drugs, weapons, and stolen data, highlights the importance of informal cooperation in combating illicit activities involving cryptocurrency assets.¹² Law enforcement agencies from multiple countries,

¹¹ Vardalaki, Aikaterini, and Vasileios Vlachos. "Emerging malware threats: The case of ransomware." *Cybersecurity Issues in Emerging Technologies*. CRC Press, 2021. 153-170. <https://doi.org/10.1201/9781003109952-9>

¹² Healey, Jason, Neil Jenkins, and J. D. Work. "Defenders disrupting adversaries: framework, dataset, and case studies of disruptive counter-cyber operations." *2020 12th International Conference on Cyber Conflict (CyCon)*. Vol. 1300. IEEE, 2020. <https://doi.org/10.23919/CyCon49761.2020.9131725>

including the FBI, DEA, and Europol, collaborated to dismantle the AlphaBay marketplace, seize servers, and arrest the site's administrators. Through close coordination and intelligence sharing, international stakeholders disrupted illicit markets, arrested key actors, and seized significant amounts of cryptocurrency assets, demonstrating the effectiveness of collaborative efforts in combating cryptocurrency-related crimes.

Cryptocurrency-Related Money Laundering Cases: Several real-world cases of cryptocurrency-related money laundering highlight the practical implications of informal cooperation in investigating financial crimes involving digital assets. For example, the investigation into the BTC-e cryptocurrency exchange, led by the US Department of Justice and international partners, revealed a sophisticated money laundering scheme involving the exchange of illicit funds into cryptocurrencies. By collaborating with financial institutions, regulatory bodies, and law enforcement agencies from multiple jurisdictions, investigators traced illicit funds, identified perpetrators, and dismantled the illicit operation, underscoring the importance of information exchange and coordination in combating cryptocurrency-related financial crimes.

DarkSide Ransomware Attacks (2021): The DarkSide ransomware attacks, which targeted critical infrastructure and organizations worldwide, underscore the practical implications of informal cooperation in responding to cyber threats involving cryptocurrency assets.¹³ Following the Colonial Pipeline ransomware attack, law enforcement agencies, cybersecurity firms, and financial institutions collaborated to track ransom payments, disrupt ransomware infrastructure, and identify the perpetrators behind the attacks. By sharing threat intelligence, coordinating mitigation efforts, and engaging with cryptocurrency exchanges, international stakeholders mitigated the impact of ransomware attacks, recovered stolen funds, and held cybercriminals accountable for their actions.

These real-world case studies highlight the practical implications of informal cooperation among international stakeholders in addressing cryptocurrency-related transnational cases. Through collaboration, information sharing, and coordinated

¹³ Alfieri, Carolyn. "Cryptocurrency and national security." *International Journal on Criminology* 9.1 (2022): 21-48. <https://doi.org/10.18278/ijc.9.1.3>

actions, stakeholders can enhance their collective ability to combat illicit activities involving cryptocurrency assets and uphold the integrity of the global financial system.

Joint task forces and working groups are collaborative initiatives established by international stakeholders to address specific challenges posed by cryptocurrency-related transnational cases. These initiatives bring together experts from law enforcement agencies, regulatory bodies, financial institutions, and other relevant entities to pool resources, share intelligence, and coordinate efforts in combating illicit activities involving cryptocurrency assets. The primary objectives of joint task forces and working groups are to enhance information exchange, facilitate coordination of enforcement actions, and promote collaboration among international stakeholders in addressing transnational cases effectively. Joint task forces and working groups comprise representatives from multiple jurisdictions and sectors with diverse backgrounds and expertise in areas such as blockchain technology, digital forensics, financial investigations, and cybersecurity. Members may include law enforcement officials, regulatory experts, financial analysts, legal advisors, and technical specialists, each bringing unique perspectives and skills to the collaborative effort. By assembling multidisciplinary teams of experts, joint task forces and working groups can leverage their collective knowledge and resources to develop comprehensive strategies for combating cryptocurrency-related crimes. Joint task forces and working groups operate under clear mandates, objectives, and guidelines established by participating stakeholders. These mandates define the scope of the collaborative effort, delineate roles and responsibilities among members, and outline the framework for information sharing, coordination, and decision-making. Clear mandates ensure that joint task forces and working groups operate efficiently, effectively, and in accordance with legal and regulatory requirements, thereby enhancing stakeholders' collective ability to address transnational cases involving cryptocurrency assets.

Joint task forces and working groups facilitate information sharing and collaboration among international stakeholders through secure communication channels, data-sharing platforms, and regular meetings.¹⁴ Members exchange intelligence, share insights, and coordinate enforcement actions to identify perpetrators, trace illicit funds, and disrupt criminal networks involved in

¹⁴ Teichmann, Fabian Maximilian Johannes, and Marie-Christin Falker. "Cryptocurrencies and financial crime: solutions from Liechtenstein." *Journal of Money Laundering Control* 24.4 (2021): 775-788. <https://doi.org/10.1108/JMLC-05-2020-0060>

cryptocurrency-related crimes. By fostering a culture of transparency, trust, and collaboration, joint task forces and working groups enable stakeholders to leverage their collective expertise and resources to address emerging threats in the digital asset space. The establishment of joint task forces and working groups has led to significant outcomes and impact in combating cryptocurrency-related transnational cases. These collaborative initiatives have resulted in successful investigations, arrests, and prosecutions of individuals involved in illicit activities such as money laundering, fraud, and cybercrime. By leveraging synergies, sharing best practices, and coordinating efforts, joint task forces and working groups have enhanced stakeholders' collective ability to combat illicit activities involving cryptocurrency assets and uphold the integrity of the global financial system. The establishment of joint task forces and working groups is a critical component of collaborative efforts among international stakeholders in addressing cryptocurrency-related transnational cases. By bringing together experts from diverse backgrounds, establishing clear mandates, fostering information sharing and collaboration, and achieving tangible outcomes, joint task forces and working groups enhance stakeholders' collective ability to combat illicit activities involving cryptocurrency assets and promote a safer and more secure digital economy.

4. Development of Information-Sharing Platforms and Networks

Information-sharing platforms and networks are essential tools for facilitating collaboration and coordination among international stakeholders in combating cryptocurrency-related transnational cases.¹⁵ These platforms serve as centralized hubs where stakeholders can securely exchange intelligence, share insights, and coordinate enforcement actions in real-time. Information-sharing platforms enable stakeholders to access relevant information, analyze trends, and identify emerging threats in the digital asset space, thereby enhancing their collective ability to combat illicit activities involving cryptocurrency assets. Information-sharing platforms offer a range of features and capabilities designed to meet the diverse needs of international stakeholders involved in combating cryptocurrency-related crimes. These features may include secure messaging systems, data-sharing repositories, analytical tools, and

¹⁵ Barbereau, Tom, and Balázs Bodó. "Beyond financial regulation of crypto-asset wallet software: In search of secondary liability." *Computer Law & Security Review* 49 (2023): 105829. <https://doi.org/10.1016/j.clsr.2023.105829>

collaboration spaces where stakeholders can collaborate on joint investigations, share best practices, and coordinate enforcement actions. Information-sharing platforms leverage advanced technologies such as encryption, access controls, and data analytics to ensure the confidentiality, integrity, and availability of shared intelligence, thereby facilitating effective collaboration and coordination among stakeholders.

Information-sharing platforms are designed to be accessible and interoperable, allowing stakeholders from different countries and sectors to collaborate seamlessly. These platforms adhere to interoperability standards and protocols to ensure compatibility with existing systems, tools, and databases used by international stakeholders in combating cryptocurrency-related crimes. By promoting interoperability, information-sharing platforms enable stakeholders to exchange information efficiently, avoid duplication of efforts, and maximize the impact of collaborative efforts in addressing transnational cases involving cryptocurrency assets. Information-sharing platforms provide secure communication channels that enable stakeholders to exchange sensitive intelligence and collaborate on joint investigations without compromising confidentiality or integrity. These communication channels utilize encryption, authentication, and access controls to protect shared information from unauthorized access, interception, or tampering. By ensuring the security and confidentiality of communications, information-sharing platforms foster a trusted environment where stakeholders can exchange intelligence and collaborate effectively in combating illicit activities involving cryptocurrency assets.

The development of information-sharing platforms often involves collaborative partnerships and initiatives among international stakeholders, including law enforcement agencies, regulatory bodies, financial institutions, and technology providers.¹⁶ These partnerships bring together stakeholders with complementary expertise and resources to develop, implement, and maintain information-sharing platforms that meet the evolving needs of the global community in combating cryptocurrency-related crimes. By fostering collaborative partnerships and initiatives, stakeholders can leverage their collective strengths and capabilities to enhance

¹⁶ Delston, Ross S., and Stephen C. Walls. "Terrorist Exploitation Points in the International Financial System: Major Vulnerabilities in the Anti-Money Laundering and Countering the Financing of Terrorism Framework. Avenues for Transatlantic Cooperation." *Terrorism and Transatlantic Relations: Threats and Challenges* (2022): 191-222. https://doi.org/10.1007/978-3-030-83347-3_9

information sharing, coordination, and collaboration in addressing transnational cases involving cryptocurrency assets. The development of information-sharing platforms and networks is a critical component of collaborative efforts among international stakeholders in combating cryptocurrency-related transnational cases. By providing secure, accessible, and interoperable platforms for exchanging intelligence, fostering collaborative partnerships, and enabling effective communication and coordination, information-sharing platforms enhance stakeholders' collective ability to combat illicit activities involving cryptocurrency assets and uphold the integrity of the global financial system.

Trust and transparency are essential elements for effective collaboration among international stakeholders in combating cryptocurrency-related transnational cases.¹⁷ Establishing trust among stakeholders fosters confidence in information sharing, collaboration, and coordination efforts, while transparency promotes accountability, openness, and integrity in collaborative activities. Strengthening trust and transparency among stakeholders is critical for building cooperative relationships, overcoming barriers to collaboration, and enhancing stakeholders' collective ability to address challenges posed by cryptocurrency assets. Strengthening trust among stakeholders begins with fostering mutual respect and understanding of each other's roles, responsibilities, and perspectives. Law enforcement agencies, regulatory bodies, financial institutions, and other relevant entities must recognize the value of collaboration and acknowledge the expertise, resources, and contributions of their counterparts in combating cryptocurrency-related crimes. By demonstrating mutual respect and understanding, stakeholders can build trust and establish a foundation for effective collaboration and coordination in addressing transnational cases involving cryptocurrency assets.

Transparency is facilitated through open communication and information sharing among stakeholders, where relevant information, insights, and updates are shared openly and transparently. Stakeholders must prioritize transparency in their collaborative activities, ensuring that decisions, actions, and outcomes are communicated clearly and comprehensively to all parties involved. Open communication and information sharing promote accountability, build confidence, and foster a culture of trust among stakeholders, enabling them to work together more

¹⁷ Lupianto, Ezzah Nariswari. "Asset Recovery for Victims of "Binary Option" Case in Review of International Criminal Law." *Corruptio* 3.1 (2022): 47-60. <https://doi.org/10.25041/corruptio.v3i1.2640>

effectively in combating illicit activities involving cryptocurrency assets. Strengthening trust and transparency among stakeholders involves establishing clear guidelines and protocols for collaboration, outlining expectations, responsibilities, and processes for information sharing, coordination, and decision-making. These guidelines ensure that stakeholders operate within a framework of transparency and accountability, adhering to ethical standards, legal requirements, and best practices in their collaborative activities. Clear guidelines and protocols promote consistency, fairness, and integrity in collaborative efforts, enhancing stakeholders' confidence in each other's actions and decisions.

Strengthening trust and transparency among stakeholders requires building collaborative partnerships based on shared values, goals, and interests.¹⁸ Law enforcement agencies, regulatory bodies, financial institutions, and other relevant entities must work together to identify common challenges, develop shared objectives, and align their efforts in combating cryptocurrency-related crimes. By building collaborative partnerships, stakeholders can leverage their collective strengths and resources to address complex challenges, foster innovation, and achieve meaningful impact in addressing transnational cases involving cryptocurrency assets. Strengthening trust and transparency among stakeholders is essential for effective collaboration in combating cryptocurrency-related transnational cases. By fostering mutual respect and understanding, promoting open communication and information sharing, establishing clear guidelines and protocols, and building collaborative partnerships, stakeholders can enhance trust, promote transparency, and work together more effectively to combat illicit activities involving cryptocurrency assets and uphold the integrity of the global financial system.

Standardizing information-sharing protocols and procedures is crucial for promoting consistency, interoperability, and effectiveness in collaborative efforts among international stakeholders in combating cryptocurrency-related transnational cases. The diverse nature of stakeholders, varying legal frameworks, and jurisdictional complexities highlight the importance of establishing common standards and practices to streamline information exchange, coordination, and decision-making processes. Standardization ensures that stakeholders operate within a framework of

¹⁸ Kshetri, Nir. "The nature and sources of international variation in formal institutions related to initial coin offerings: preliminary findings and a research agenda." *Financial Innovation* 9.1 (2023): 9. <https://doi.org/10.1186/s40854-022-00405-x>

transparency, accountability, and trust, enhancing their collective ability to address challenges posed by cryptocurrency assets. Standardizing information-sharing protocols and procedures involves developing common frameworks, guidelines, and protocols that define the principles, processes, and requirements for collaboration among stakeholders. These frameworks outline standardized procedures for data collection, analysis, sharing, and dissemination, ensuring consistency and uniformity in information-sharing practices across jurisdictions and sectors. Common frameworks provide stakeholders with clear guidelines and expectations for collaborative activities, enabling them to operate more efficiently and effectively in addressing transnational cases involving cryptocurrency assets.

Standardization of information-sharing protocols and procedures requires the adoption of interoperable technologies and platforms that facilitate seamless communication and collaboration among stakeholders.¹⁹ Interoperable technologies ensure compatibility and integration between systems, tools, and databases used by international stakeholders in combating cryptocurrency-related crimes. By adopting interoperable technologies, stakeholders can exchange information securely, avoid duplication of efforts, and maximize the impact of collaborative efforts in addressing transnational cases involving cryptocurrency assets. Standardizing information-sharing protocols and procedures involves aligning with existing legal and regulatory frameworks governing information sharing, privacy, and data protection. Stakeholders must ensure that standardized protocols and procedures comply with applicable laws, regulations, and international agreements to safeguard individual rights, protect sensitive information, and mitigate legal risks. Alignment with legal and regulatory frameworks promotes transparency, accountability, and trust among stakeholders, enabling them to collaborate more effectively while adhering to ethical and legal standards.

Standardization of information-sharing protocols and procedures requires ongoing review, evaluation, and improvement to adapt to evolving threats, technologies, and best practices. Stakeholders must regularly assess the effectiveness of standardized protocols and procedures, solicit feedback from stakeholders, and incorporate lessons learned into future iterations. Continuous review and

¹⁹ Sukumar, Arun, Dennis Broeders, and Monica Kello. "The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy." *Contemporary Security Policy* 45.1 (2024): 7-44. <https://doi.org/10.1080/13523260.2023.2296739>

improvement ensure that standardized protocols and procedures remain relevant, responsive, and adaptable to the changing landscape of cryptocurrency-related transnational cases, enhancing stakeholders' collective ability to address emerging challenges and uphold the integrity of the global financial system. Standardizing information-sharing protocols and procedures is essential for promoting consistency, interoperability, and effectiveness in collaborative efforts among international stakeholders in combating cryptocurrency-related transnational cases. By developing common frameworks, adopting interoperable technologies, aligning with legal and regulatory frameworks, and embracing continuous review and improvement, stakeholders can enhance trust, transparency, and collaboration in addressing challenges posed by cryptocurrency assets and safeguarding the integrity of the global financial system.

5. Leveraging Technological Solutions for Secure and Efficient Collaboration

Technology plays a crucial role in facilitating secure and efficient collaboration among international stakeholders in combating cryptocurrency-related transnational cases.²⁰ By leveraging technological solutions, stakeholders can streamline information exchange, enhance communication, and improve coordination of enforcement actions across borders. Technological solutions enable stakeholders to overcome barriers such as distance, time zones, and language differences, fostering a culture of collaboration, innovation, and responsiveness in addressing challenges posed by cryptocurrency assets. Secure communication platforms are essential for facilitating confidential and encrypted communication among international stakeholders involved in collaborative efforts. These platforms provide secure messaging, file sharing, and collaboration tools that ensure the confidentiality, integrity, and authenticity of shared information. Secure communication platforms enable stakeholders to exchange sensitive intelligence, coordinate enforcement actions, and collaborate on joint investigations without compromising security or privacy. Blockchain analysis tools are instrumental in tracing cryptocurrency transactions, identifying patterns of illicit activity, and attributing transactions to specific actors or entities. These tools leverage blockchain data to provide insights into the flow of funds, the movement of assets, and the behavior of users on cryptocurrency networks. By utilizing blockchain analysis tools,

²⁰ Murtazashvili, Iliia, et al. "Blockchain networks as knowledge commons." *International Journal of the Commons* 16.1 (2022): 108-119. <https://doi.org/10.5334/ijc.1146>

stakeholders can uncover hidden connections, detect suspicious activities, and gather evidence to support investigative efforts in combating cryptocurrency-related crimes. Data analytics and machine learning technologies enable stakeholders to analyze vast amounts of data, detect anomalies, and identify emerging trends in the digital asset space. These technologies empower stakeholders to make informed decisions, prioritize investigative leads, and allocate resources more effectively in addressing transnational cases involving cryptocurrency assets. By harnessing the power of data analytics and machine learning, stakeholders can enhance their capacity for predictive analysis, risk assessment, and proactive intervention in combating illicit activities.

Interoperable information-sharing platforms facilitate seamless communication and collaboration among international stakeholders by integrating with existing systems, tools, and databases used in combating cryptocurrency-related crimes.²¹ These platforms enable stakeholders to access relevant information, share intelligence, and coordinate enforcement actions in real-time, regardless of geographical location or organizational affiliation. Interoperable information-sharing platforms promote transparency, interoperability, and efficiency in collaborative efforts, enhancing stakeholders' collective ability to address challenges posed by cryptocurrency assets. Encryption and data protection measures are essential for safeguarding sensitive information and ensuring the security of collaborative activities among international stakeholders. These measures include encryption protocols, access controls, and data anonymization techniques that protect shared information from unauthorized access, interception, or tampering. By implementing encryption and data protection measures, stakeholders can enhance the confidentiality, integrity, and availability of shared intelligence, thereby fostering trust, transparency, and collaboration in combating cryptocurrency-related transnational cases. Leveraging technological solutions is essential for facilitating secure and efficient collaboration among international stakeholders in combating cryptocurrency-related transnational cases. By utilizing secure communication platforms, blockchain analysis tools, data analytics, interoperable information-sharing platforms, and encryption and data protection measures, stakeholders can enhance their collective ability to address challenges

²¹ Katsios, Stavros, and Ioannis Blatsos. "Cryptocurrencies' Asset Recovery: A Multi-Dimensional Approach." *Cyber Laundering: International Policies and Practices*. 2023. 281-310. https://doi.org/10.1142/9781800612839_0011

posed by cryptocurrency assets and uphold the integrity of the global financial system in the digital age.

C. CONCLUSION

In conclusion, this study has highlighted the pivotal role of informal cooperation in enhancing the prosecutor's effectiveness in tackling cryptocurrency-related transnational crimes. By examining mechanisms such as joint task forces, information-sharing platforms, and technological solutions, it is clear that effective collaboration among international stakeholders is crucial for prosecutors to address the challenges posed by digital assets.

The paper emphasizes the importance of trust, transparency, and standardized protocols in facilitating cooperation, which are essential for prosecutors to successfully manage complex cases involving cryptocurrency. It underscores the need for clear guidelines, secure communication channels, and interoperable technologies to streamline collaborative efforts. Real-world case studies illustrate how informal cooperation has proven effective in disrupting criminal networks, tracing illicit funds, and holding perpetrators accountable, thereby enhancing the prosecutor's role in achieving justice.

As a policy recommendation, it is imperative for governments, law enforcement agencies, regulatory bodies, and financial institutions to prioritize the establishment of formalized frameworks and protocols for informal cooperation in combating cryptocurrency-related transnational cases. This includes investing in training, capacity-building, and technology infrastructure to enhance stakeholders' capabilities for collaboration, information sharing, and coordinated enforcement actions. Additionally, policymakers should consider harmonizing legal and regulatory frameworks to facilitate cross-border cooperation and streamline investigative processes in combating cryptocurrency-related crimes.

By embracing a collaborative approach and implementing proactive measures, stakeholders can enhance their collective ability to address the challenges posed by cryptocurrency assets and safeguard the integrity of the global financial system in the digital age. Together, through informal cooperation and coordinated efforts, stakeholders can effectively combat illicit activities involving cryptocurrency assets and uphold the rule of law in the evolving landscape of the digital economy.

REFERENCES

- Arifin, Ridwan, Sigit Riyanto, and Akbar Kurnia Putra. "Collaborative efforts in ASEAN for global asset recovery frameworks to combat corruption in the digital era." *Legality: Jurnal Ilmiah Hukum* 31.2 (2023): 329-343. <https://doi.org/10.22219/ljih.v31i2.29381>
- Barbureau, Tom, and Balázs Bodó. "Beyond financial regulation of crypto-asset wallet software: In search of secondary liability." *Computer Law & Security Review* 49 (2023): 105829. <https://doi.org/10.1016/j.clsr.2023.105829>
- Collins, John. "Crypto, crime and control." *Cryptocurrencies as an enabler of organized crime, Global Initiative Against Transnational Organized Crime* (2022).
- Delston, Ross S., and Stephen C. Walls. "Terrorist Exploitation Points in the International Financial System: Major Vulnerabilities in the Anti-Money Laundering and Countering the Financing of Terrorism Framework. Avenues for Transatlantic Cooperation." *Terrorism and Transatlantic Relations: Threats and Challenges* (2022): 191-222. https://doi.org/10.1007/978-3-030-83347-3_9
- Gilmour, Paul Michael. "Decentralized blockchain technology: towards a trusted and transparent beneficial ownership regime." *Financial Technology and the Law: Combating Financial Crime*. Cham: Springer International Publishing, 2022. 185-209. https://doi.org/10.1007/978-3-030-88036-1_8
- Golonka, Anna. "Cooperation with third countries in combating money laundering in the face of modern challenges." *Ius Novum* 17.4 (2023): 15-39. <https://doi.org/10.2478/in-2023-0027>
- Healey, Jason, Neil Jenkins, and J. D. Work. "Defenders disrupting adversaries: framework, dataset, and case studies of disruptive counter-cyber operations." 2020 12th *International Conference on Cyber Conflict (CyCon)*. Vol. 1300. IEEE, 2020. <https://doi.org/10.23919/CyCon49761.2020.9131725>
- Ilbiz, Ethem, and Christian Kaunert. "Sharing Economy for Tackling Crypto-Laundering: The Europol Associated 'Global Conference on Criminal Finances and Cryptocurrencies'." *Sustainability* 14.11 (2022): 6618. <https://doi.org/10.3390/su14116618>
- Laksono, Hazmi Tri, and Muhammad Fuadillah Nugraha. "Cryptocurrency Fever: Should Southeast Asian countries cooperate on facing the cryptocurrency market." *Proceedings of Airlangga Conference on International Relations (ACIR 2018) Politics, Economy, and Security in the Changing Indo-Pacific Region*. 2021. <https://doi.org/10.5220/0010276603240330>
- Lupianto, Ezzah Nariswari. "Asset Recovery for Victims of "Binary Option" Case in Review of International Criminal Law." *Corruptio* 3.1 (2022): 47-60. <https://doi.org/10.25041/corruptio.v3i1.2640>
- Kshetri, Nir. "The nature and sources of international variation in formal institutions related to initial coin offerings: preliminary findings and a research agenda." *Financial Innovation* 9.1 (2023): 9. <https://doi.org/10.1186/s40854-022-00405-x>

- Katsios, Stavros, and Ioannis Blatsos. "Cryptocurrencies' Asset Recovery: A Multi-Dimensional Approach." *Cyber Laundering: International Policies and Practices*. 2023. 281-310. https://doi.org/10.1142/9781800612839_0011
- Kethineni, Sessa, and Ying Cao. "The rise in popularity of cryptocurrency and associated criminal activity." *International Criminal Justice Review* 30.3 (2020): 325-344. <https://doi.org/10.1177/1057567719827051>
- Teichmann, Fabian Maximilian Johannes, and Marie-Christin Falker. "Cryptocurrencies and financial crime: solutions from Liechtenstein." *Journal of Money Laundering Control* 24.4 (2021): 775-788. <https://doi.org/10.1108/JMLC-05-2020-0060>
- Reinsberg, Bernhard. "Fully-automated liberalism? Blockchain technology and international cooperation in an anarchic world." *International Theory* 13.2 (2021): 287-313. <https://doi.org/10.1017/S1752971920000305>
- Sukumar, Arun, Dennis Broeders, and Monica Kello. "The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy." *Contemporary Security Policy* 45.1 (2024): 7-44. <https://doi.org/10.1080/13523260.2023.2296739>
- Teichmann, Fabian Maximilian Johannes, and Marie-Christin Falker. "Cryptocurrencies and financial crime: solutions from Liechtenstein." *Journal of Money Laundering Control* 24.4 (2021): 775-788. <https://doi.org/10.1108/JMLC-05-2020-0060>
- Vardalaki, Aikaterini, and Vasileios Vlachos. "Emerging malware threats: The case of ransomware." *Cybersecurity Issues in Emerging Technologies*. CRC Press, 2021. 153-170. <https://doi.org/10.1201/9781003109952-9>