JCPP JOURNAL OF CYBERSECURITY AND PUBLIC POLICIES

Vol. 1, Nº. 1 (Sep./Dec. 2025)
www.cybersecuritypolicies.com.br

Cryptocurrencies and Cybercrime: Political and International Challenges in the Digital Age

Rickiã Gabriel de Magalhães Rodrigues[1]

Abstract

How do different regulatory jurisdictions address the international security challenges posed by the intersection of cryptocurrencies and cybercrime? This article analyzes the policy responses of the United States, European Union, United Kingdom, and Singapore through a comparative document analysis of public policy. The findings reveal diverse regulatory approaches—ranging from restrictive models to cooperative frameworks—exposing institutional fragmentation in the face of shared threats. This research contributes to the debate on global governance and cybersecurity, offering empirical input to the field of International Relations by providing guidance for enhancing international cooperation against transnational financial cybercrime.

Keywords: cryptocurrencies; cybercrime; global governance; international security; financial regulation.

1 Master's student in Political Science at the Federal University of Pernambuco (UFPE), where also earned a Bachelor's degree in Political Science (2023). Main research focuses on international political economy, monetary and fiscal policy, interest groups, and cryptocurrencies.

Introduction

The advent of digital technologies has profoundly reshaped the contours of global politics and finance, introducing innovative opportunities alongside unprecedented challenges. Among these innovations, cryptocurrencies have emerged as a revolutionary force, promising decentralized finance, near-instant transactions, and greater financial inclusion (Nakamoto, 2008; Antonopoulos, 2017). However, this transformative potential is increasingly tied to a growing dark side: the deepening nexus between cybercrime and cryptocurrencies (Foley et al., 2019; August et al., 2025). This phenomenon is part of a broader trend where digital infrastructure, initially designed for communication and commerce, is being exploited for illicit activities and state control (Deibert, 2019).

At the same time, ransomware attacks continue to strike critical infrastructure worldwide, with criminals demanding payment exclusively in digital assets (Chainalysis, 2025). These episodes illustrate a central paradox of the digital age: the same technologies that promise to democratize financial access have also become instruments of international security threats.

In response to this landscape of growing criminal sophistication, global powers have intensified efforts to develop comprehensive regulatory frameworks. The United States, European Union, United Kingdom, and Singapore have implemented distinct policies that reflect different philosophies of digital governance and national security priorities (Galasso, 2024). This diversity of approaches highlights the lack of international consensus on optimal governance methods for decentralized digital assets (Ba; Şen, 2024).

How do different regulatory jurisdictions address the international security challenges posed by the intersection of cryptocurrencies and cybercrime? This question emerges as a central governance challenge in contemporary global politics—transcending national borders and defying traditional regulatory frameworks (Farber, 2025). The phenomenon represents a fundamental test of states' capacity to coordinate effective responses to transnational threats in a decentralized digital environment (Choucri; Anaya, 2024).

This study seeks to systematize the main jurisdictional strategies for addressing these emerging threats, providing a comparative diagnosis to guide policymakers. It serves as an empirical basis for developing best practices in digital asset governance, helping to reduce the regulatory fragmentation that benefits malicious actors (Ba; Şen, 2024).

The main objective of this research is to comparatively analyze the regulatory strategies adopted by different jurisdictions to combat the use of cryptocurrencies in cybercriminal activities. Specific objectives include: (i) identifying the main challenges perceived by each jurisdiction at the crypto-cybercrime intersection; and (ii) quantifying the international cooperation mechanisms proposed to address these transnational threats.

Methodologically, this study uses a comparative document analysis of four official public policy documents, applying a structured twelve-question questionnaire to extract data on goals, definitions, identified challenges, and proposed cooperation mechanisms (Prior, 2003; Cardno, 2018). Descriptive statistical analysis of the results will allow for the identification of patterns and divergences in jurisdictional approaches

For policymakers, this article provides a crucial comparative diagnosis for developing more effective international cooperation mechanisms. It also contributes to scholarship by offering the first systematic mapping of jurisdictional variations in responses to the crypto-cybercrime nexus, filling an important gap in the literature on international digital security.

1. Theoretical-Empirical Framework: Cryptocurrencies and Cybercrime in the Digital Age

This section is dedicated to conceptualizing and establishing the fundamental parameters for understanding the intersection of cryptocurrencies and cybercrime in the context of contemporary international relations.

The conceptual framework is structured across four analytical dimensions: (i) operational definitions of cybercrime in the digital age; (ii) technological characteristics of cryptocurrencies as a decentralized financial infrastructure; (iii) international relations theories applicable to transnational digital threats; and (iv) criminological frameworks that explain how specific features of digital assets facilitate illicit activities.

1.1 The Convergence of Digital Crime and Decentralized Finance

The intersection of cryptocurrencies and cybercrime represents a fundamental transformation in both criminal activity and international security dynamics. Cybercrime encompasses a set of illicit activities that use information technologies as a means, target, or environment for execution (Wall, 2007). Modern taxonomies distinguish between "cyber-dependent crimes"—offenses that can only be committed through computer systems—and "cyber-enabled crimes," which amplify traditional criminal activities using digital technologies (McGuire; Dowling, 2013). This distinction proves crucial for understanding how cryptocurrencies permeate both categories, serving simultaneously as targets for attacks and facilitators of criminal activity.

Cryptocurrencies are digital monetary systems based on blockchain technology that operate independently of traditional central authorities (Narayanan et al., 2016). Their defining characteristics—decentralization, pseudo-anonymity, transaction irreversibility, and global reach—create a technological environment offering both legitimate benefits and illicit opportunities.

Decentralization removes single points of failure but eliminates traditional intermediaries that perform compliance and monitoring functions (Ba; Şen, 2024). The pseudo-anonymity of cryptocurrencies creates a layer of obscurity exploitable by malicious actors, though increasingly sophisticated blockchain forensic analyses demonstrate it does not constitute absolute anonymity (World Bank, 2018).

The empirical manifestation of this convergence is most visible in ransomware attacks, which have fundamentally transformed the digital threat landscape. The near-universal preference for cryptocurrency payments stems from their ability to enable fast, cross-border transfers with lower traceability compared to traditional financial systems (Conti et al., 2018). The "Ransomware-as-a-Service" (RaaS) model has democratized access to advanced cybercriminal capabilities, enabling actors with limited technical expertise to conduct sophisticated attacks through cryptocurrency-based service platforms (Chainalysis, 2025).

Table 1. Typology of Cybercrimes Facilitated by Cryptocurrencies

Type of Cybercrime	Role of Cryptocurrency	Examples
Cyber-Dependent Crimes		
Ransomware	Preferred payment method due to pseudo-anonymity and global reach; optimizes monetization.	NotPetya, CryptoLocker, WannaCry
Hacking	Funding for tools/services; payment for stolen data.	Exchange hacking (fund theft), CryptoLocker, funding cyber operations
Malware Distribution	Payment for "malware-as-a-service" ;illicit financial gains.	Distribution of trojans, botnets
Cyber-Enabled Crimes		
Money Laundering (Crypto-washing)	Pseudo-anonymity, speed, cross-border transfer, obfuscation (mixers, layering	Hiding illicit proceeds from drug trafficking, fraud, terrorism financing
Drug Trafficking	Exclusive currency on darknet markets enabling anonymous transactions.	Drug sales on Silk Road, AlphaBay
Terrorist Financing	Financing clandestine operations; anonymous donations; sanction evasion.	Fundraising by Al-Qaeda, Hamas, ISIS; WMD funding by North Korea
Fraud/Scams	Facilitates investment scams, phishing, "romance baiting"; irreversible transactions.	nvestment scams, tech support scams, impersonation of government agents
Sanctions Evasion	Circumventing traditional financial channels; financing illicit trade and WMD programs.	Lazarus Group (North Korea) using crypto for missile development

Source: Author's elaboration (2025)

1.2 Theoretical Perspectives on Transnational Digital Threats

Analyzing the crypto-cybercrime nexus requires theoretical frameworks capturing both power dynamics among states and challenges posed by transnational non-state actors. The theory of complex interdependence by Keohane and Nye (2011) offers insight into how multiple

channels of connection—governmental, international organizational, and transnational—shape responses to threats crossing national borders. The rise of state-sponsored cybercrime further exacerbates the "cybersecurity dilemma," where one nation's defensive measures can be perceived as offensive threats by another, leading to breakdown of trust and arms races in cyberspace (Buchanan, 2017).

From a neorealist perspective, the anarchic structure of the international system creates incentives for states to exploit cryptocurrencies for strategic advantage, whether through sanctions evasion or funding covert operations (Waltz, 1979). This systemic pressure manifests empirically in cases like North Korea's systematic use of cryptocurrencies to evade international sanctions.

The Lazarus Group, linked to the North Korean regime, has generated over $1 billion through attacks on cryptocurrency exchanges since 2015, using sophisticated laundering techniques including mixing services and "chain-hopping" across different digital assets (Oladipupo, 2025). The challenge of attributing cyber attacks to specific actors complicates traditional state responses to these threats (Rid; Buchanan, 2015).

Constructivist perspectives illuminate how emerging norms around cybersecurity and digital governance are socially constructed through interactions among states, international organizations, and private actors (Wendt, 2000). The lack of consensus on appropriate governance norms for cryptocurrencies reflects broader disputes over digital sovereignty and the appropriate role of the state in regulating decentralized technologies. This normative vacuum creates opportunities for malicious actors operating between Westphalian concepts of territorial sovereignty and the borderless nature of digital spaces (Rosenau, 1997).

1.3 Criminal Ecosystems and Money Laundering Evolution

The dark web has established a sophisticated commercial ecosystem where cryptocurrencies serve as the exclusive medium for illicit transactions, creating a parallel economy operating independently of regulated financial systems. Marketplaces such as the historic Silk Road demonstrated how cryptocurrencies enable anonymous global trade in illicit goods—from drug trafficking to sale of stolen personal data (Christin, 2013). The resilience of these markets, evidenced by rapid emergence of successors after law enforcement takedowns, illustrates how crypto-decentralization allows for more efficient "crime displacement" than traditional criminal networks (Barratt; Aldridge, 2016).

The "Crypto-laundering" represents a major evolution in money laundering techniques, leveraging unique characteristics of digital assets to obscure origins of illicit funds (Albrecht et al., 2019; Houben; Snyers, 2018). The traditionally three-phase laundering process—placement, layering, and integration—has been adapted to the digital environment through crypto-to-fiat

conversions, transfers across multiple blockchains, and use of decentralized exchanges with weaker compliance measures (Fanusie; Robinson, 2018). The ability to conduct high-value operations potentially amounting to billions of dollars with low likelihood of detection makes cryptocurrency-based money laundering highly attractive (Irwin; Milad, 2016).

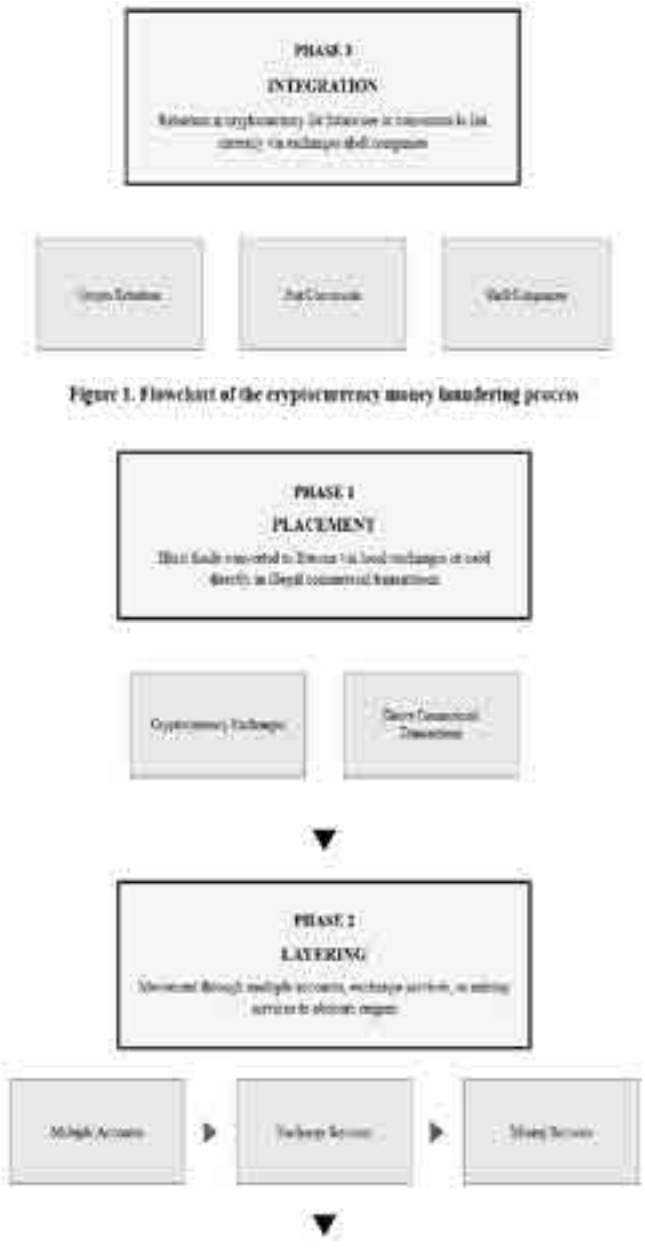


Figure 1. Flowchart of the cryptocurrency money laundering process

Source: Author's elaboration based on the three-phase money laundering model adapted for cryptocurrencies. The flowchart illustrates the operational sequence used by criminals to legitimize illicit funds through digital assets, following the classic steps of placement, stratification, and integration into the traditional financial system. (2025).

Criminological models, particularly environmental criminology, offer analytical lenses for understanding how specific features of cryptocurrencies facilitate criminal activity. Rational

Choice Theory posits that criminals are rational actors evaluating costs and benefits of their actions (Clarke; Felson, 1993).

From this perspective, cryptocurrencies significantly reduce perceived costs due to lower risks of detection and prosecution while maximizing potential benefits through access to global markets and greater operational efficiency. Routine Activity Theory suggests crimes occur when motivated offenders, suitable targets, and absence of capable guardians converge (Cohen; Felson, 1979).

2. Regulatory Responses and International Cooperation

2.1 Ransomware and the Transformation of Digital Crime

National responses to the crypto-cybercrime nexus reflect distinct regulatory traditions, foreign policy priorities, and institutional capacities. The United States maintains a fragmented approach characterized by overlapping oversight from multiple federal agencies—FinCEN, CFTC, and SEC—creating a complex regulatory landscape potentially exploitable by malicious actors (Hughe; Middlebrook, 2015).

The establishment of the FBI's Virtual Asset Unit represents centralization attempts, though coordination gaps persist. The European Union seeks harmonization through the Markets in Crypto-Assets (MiCA) regulatory framework, complemented by the NIS2 Directive on cybersecurity and the Cyber Resilience Act (Zetzsche et al., 2020).

Singapore has developed comprehensive preventive frameworks emphasizing compliance and rigorous KYC/AML requirements, while the United Kingdom balances operational enforcement with technological innovation. Brazil's evolving approach through Law No. 14,478/2022 establishes a legal framework for virtual assets while extending existing AML laws to cryptocurrency operations (Brasil, 2022). China maintains highly restrictive policies, treating cryptocurrencies as "specific virtual commodities" rather than legitimate monetary instruments, enacting sweeping bans on trading and mining activities (Hu, 2024).

Table 2. Comparative Analysis of National Cryptocurrency Regulations

Country/ Bloc	Regulatory Stance	Key Legislation/ Guidelines	Primary Regulatory Bodies	Main AML/ KYC Requirements	Policy Challenges/ Gaps
EUA	fragmented, Evolving	Bank Secrecy Act, FinCEN Guidance, CFTC/SEC Decisions	FinCEN, CFTC, SEC, FBI (VAU)	Evolving, applied to money transmitters	Regulatory fragmentation, potential for capture, DeFi vulnerabilities, data gaps

UE	Harmonized, Progressive	Markets in Crypto-Assets (MiCA), NIS2 Directive, Cyber Resilience Act	European Commission, ESMA, EBA, Europol	Strict, applied to Virtual Asset Service Providers (VASPs)	Unlicensed exchanges, privacy coins, obfuscation techniques, enforcement difficulties
Brasil	Evolving, Cautious	Law No. 14,478/2022 (BVAL), Decree No. 11,563/2023	Central Bank of Brazil (BCB), CVM	Existing AML laws extend to crypto	Lack of specific AML regime, governmental concerns, legislative proposals still under development[2]
China	Highly Restrictive, Prohibitive	"Notice on Preventing Bitcoin Risks" (2013), "Announcement on Preventing Token Issuance Financing Risks" (2017), "Notice on Further Prevention and Resolution of Virtual Currency Trading and Speculation Risks" (2021)	People's Bank of China (PBOC), Cyberspace Administration of China (CAC)	Strict, mandatory data collection	Regulatory vacuum (offshore platforms), legal ambiguity, consumer protection, global asset flow vs. single-state regulation

Source: Author's elaboration (2025)

The fragmentation in regulatory approaches creates arbitrage opportunities for criminal actors who exploit jurisdictional gaps. The problem is compounded by increasing use of cryptocurrencies by state-sponsored actors functioning as "cyber mercenaries" to achieve political and financial objectives (Maurer, 2018). This challenge is particularly acute with privacy coins and decentralized finance protocols operating beyond traditional regulatory reach.

2.2 International Cooperation Mechanisms and Institutional Challenges

International organizations play increasingly central roles in coordinating responses to crypto-cybercrime, though facing significant structural limitations. The Financial Action Task Force (FATF) has established standards for Virtual Asset Service Providers through its 40 Recommendations, but implementation varies substantially across member jurisdictions (FATF, 2019). The pseudo-anonymous nature of cryptocurrencies and lack of centralized ownership records hinder effective enforcement of these standards.

Interpol coordinates transnational operations through its Cybercrime Directorate, employing tools such as blockchain analytics to trace illicit flows. However, it faces challenges posed by rapid evolution of criminal tactics and limited technical capabilities of national security forces.[3] The UNODC has developed training programs on cryptographic and darknet

2 https://www.ibanet.org/Brazil-legal-framework-for-cryptoassets-and-upcoming-regulation
3 https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

investigations, acknowledging that technical knowledge gaps restrict effectiveness of national responses.[4] The emergence of Central Bank Digital Currencies (CBDCs) adds another layer of complexity to the regulatory landscape, potentially offering greater control but also new vulnerabilities (Auer; Böhme, 2020).

3. Methodology

3.1 Research Design

This research employs comparative documentary analysis to examine how different jurisdictions address the international security challenges posed by the crypto-cybercrime nexus. The methodological choice is justified by the need to capture systematic variations in official public policies, enabling structured comparison between distinct jurisdictional approaches while maintaining fidelity to the conceptual frameworks and priorities expressed by each government.

Table 3. General Methodological Information

Sections	Description
Research Question	How do different regulatory jurisdictions address the international security challenges posed by the intersection of cryptocurrencies and cybercrime?
Unit of Analysis	Official public policy documents from four jurisdictions representing different regulatory traditions
Temporal Delimitation	Contemporary documents from 2024-2025 to ensure current relevance
Sources	Government agencies and official regulatory bodies
Techniques	Comparative documentary analysis with structured questionnaire (12 questions), categorical content analysis
Software	Google Docs, Sheets and R for visual elements
Data Repository	OSF with the raw answered questions and comparative table matrixes[5]

Source: Author's elaboration (2025)

3.2 Corpus Documental and Selection Criteria

The corpus consists of four official public policy documents selected to represent different regulatory traditions and strategic approaches to the crypto-cybercrime nexus. The selection is justified by the need to capture systematic variations in institutional responses from jurisdictions with different regulatory capacities, legal traditions, and foreign policy priorities:

1. **Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service** - (Monetary Authority of Singapore)

4 https://www.unodc.org/roseap/en/2022/02/cryptocurrencies-darknet-investigations/story.html
5 https://osf.io/m654j/

2. **2024 National Strategy for Combating Terrorist and Other Illicit Financing** - (US Department of Treasury)
3. **National Strategic Assessment 2025 of Serious and Organised Crime** - United Kingdom
4. **Europol Spotlight - Cryptocurrencies - Tracing the evolution of criminal finances** (Europol)

These documents were selected based on three criteria: (i) jurisdictions with high economic relevance in the global crypto ecosystem; (ii) advanced institutional capacities for enforcement; and (iii) significant international normative influence. The preference for official primary sources ensures analysis captures policies effectively implemented by states, while temporal selection (2024-2025) guarantees contemporary relevance.

3.3 Data Collection Instrument

A structured questionnaire with 12 questions was developed to extract comparable information from the selected documents, following principles established by Bowen (2009) for reducing interpretive bias and enabling comparability. The questionnaire covers four analytical dimensions:

Framework 1: Questionnaire for Documentary Analysis

Nº	Question	Description / Application
1	What is the responsible government body for the document?	Identify whether it is a central bank, security agency, justice ministry, or another official body.
2	What are the main objectives of the document regarding cryptocurrencies and cybercrime?	E.g., money laundering prevention, ransomware crackdown, cryptoasset traceability.
3	How does the document define cybercrimes involving cryptoassets?	Check for distinctions between ransomware, fraud, tax evasion, etc.
4	Does the document define or approach the concept of "cryptoassets" or "virtual assets"?	Analyze the scope and technical depth of the definition.
5	What are the key challenges identified at the intersection of cybercrime and cryptocurrencies?	E.g., anonymity, regulatory gaps, cross-border jurisdiction issues.
6	Are specific malicious actors mentioned as threats?	Investigate whether hackers, transnational groups, terrorists, or hostile nations are cited.
7	Does the document mention international cooperation to combat cybercrime involving cryptoassets	E.g., references to Interpol, FATF/GAFI, bilateral agreements, information exchange.
8	Does the document propose partnerships with specific international organizations?	E.g., UN, FATF, OECD, Europol, World Bank.
9	What specific enforcement or law enforcement mechanisms are proposed?	Identify regulatory tools, penalties, and investigation procedures.

10	Is there mention of private sector engagement (e.g., exchanges, fintechs, banks)?	Indicate whether institutional dialogue or participatory regulation is included.
11	Does the document discuss national and international jurisdiction issues in crypto-related crimes?	Identify legal barriers and the search for cross-border legal solutions.
12	Are emerging technologies for tracking and combating crypto-related crime discussed?	E.g., blockchain analytics, artificial intelligence, tech partnerships.

Source: Author's elaboration (2025)

Step 1: Reading and Extraction

Each document was read in its entirety to locate answers to the 12 questionnaire questions. This "close reading" process is fundamental in documentary analysis, enabling familiarization with content before formal coding (O'Leary, 2014). Relevant information was extracted and recorded in a comparative spreadsheet, maintaining references to original pages for traceability.

Step 2: Response Coding

Extracted responses were coded into categories to enable comparison between jurisdictions, following content analysis procedures described by Schreier (2012). For example:

a) For the question about challenges (question 5), responses were categorized as: "anonymity," "jurisdiction," "transaction speed," "lack of regulation," etc.

b) For international cooperation (question 7), mentions of specific organizations were identified: "FATF," "Interpol," "bilateral agreements," etc.

Step 3: Descriptive Statistical Analysis

Coded data were analyzed quantitatively to identify frequencies, convergence patterns, divergence patterns, and gaps. This approach of transforming qualitative data into quantitative through categorical coding is widely used in comparative policy analysis (Rihoux; Ragin, 2009). Results are presented through frequency tables and comparative graphs, enabling clear visualization of similarities and differences between jurisdictional approaches.

3.4 Methodological Limitations

The main limitation is the differential availability of official documents between jurisdictions - a common challenge in comparative public policy studies (Yanow, 2007). While the United States, European Union, and United Kingdom produce detailed reports on crypto-cybercrime, many Global South jurisdictions lack equivalent documents, resulting in under-representation of these perspectives.

Additionally, documentary analysis captures only formally expressed policies, not their practical implementation or real effectiveness (Colebatch, 2009). The analysis is also limited to English-language documents, potentially missing nuanced approaches from non-English speaking jurisdictions.

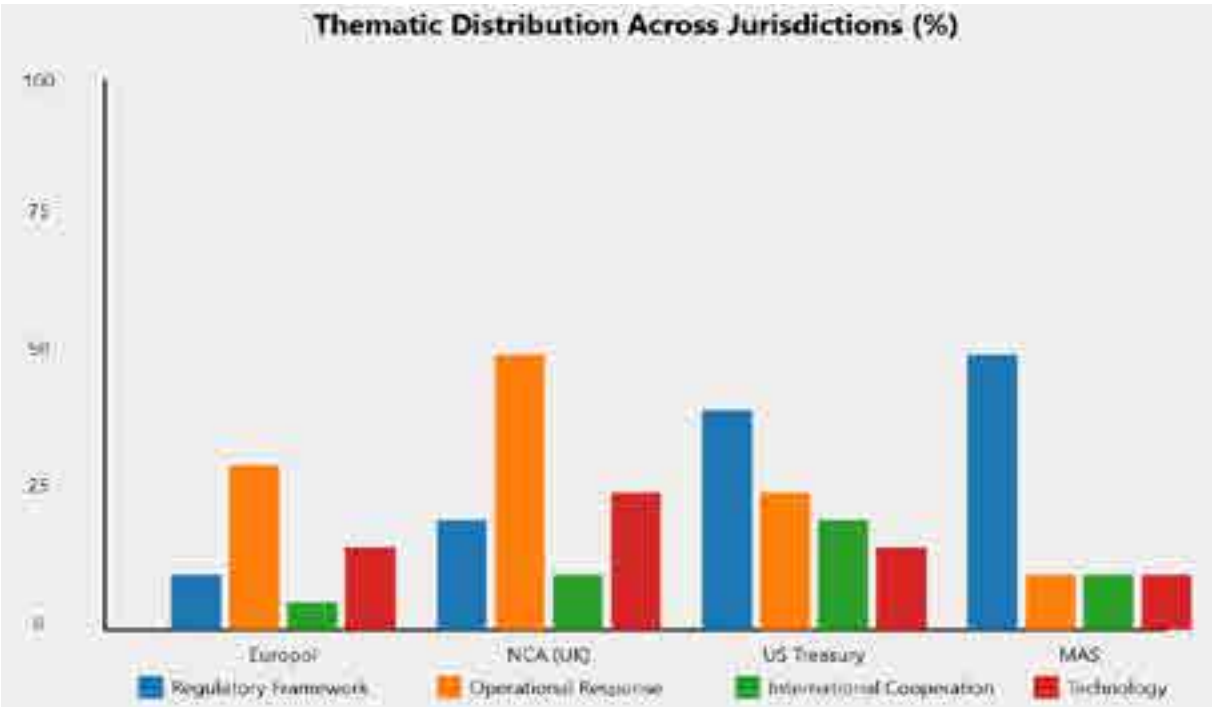
4. Results

The comparative analysis of the four official documents reveals distinct patterns in jurisdictional approaches to the crypto-cybercrime nexus, evidencing both convergences and significant divergences in regulatory and operational strategies.

4.1 Comparative Analysis of Jurisdictional Strategies

Documentary analysis identified substantial variations in regulatory approaches among the examined jurisdictions. Graph 1 presents the thematic distribution of main focuses in each analyzed document.

Graph 1. Thematic distribution across jurisdictions (%)



Source: Author's elaboration (2025)

As demonstrated in Graph 1, distinct jurisdictional profiles emerge: Singapore (MAS, 2024) concentrates 45% of its content on detailed regulatory frameworks, reflecting a preventive

compliance-based approach. In contrast, the United Kingdom (NCA, 2025) dedicates 35% to operational response, showing focus on enforcement and practical cases. The United States (US Treasury, 2024) presents a more balanced distribution, with emphasis on regulatory modernization (30%) and international cooperation (20%), while Europol (2024) prioritizes criminal trend analysis and operational cases.

4.2 Convergence and Divergence Patterns

The analysis identified common and divergent elements in jurisdictional approaches to combating crypto-cybercrime. Table 4 synthesizes the main challenges identified by each jurisdiction.

Table 4. Key Challenges Identified by Jurisdiction

Challenge Category	Europol (2024)	NCA (2025)	US Tresury (2024)	MAS (2024)
Anonymity/Privacy	High	Medium	High	High
Transaction Speed	Medium	Low	High	High
Cross-border Nature	High	High	High	High
Regulatory Gaps	Medium	High	High	Medium
Technology Evolution	Medium	High	High	Low
Volume Estimation	High	High	Medium	Not Mentioned

Legend: High = Major focus/concern | Medium = Moderate attention | Low = Limited Discussion | Not mentioned = absent from document.

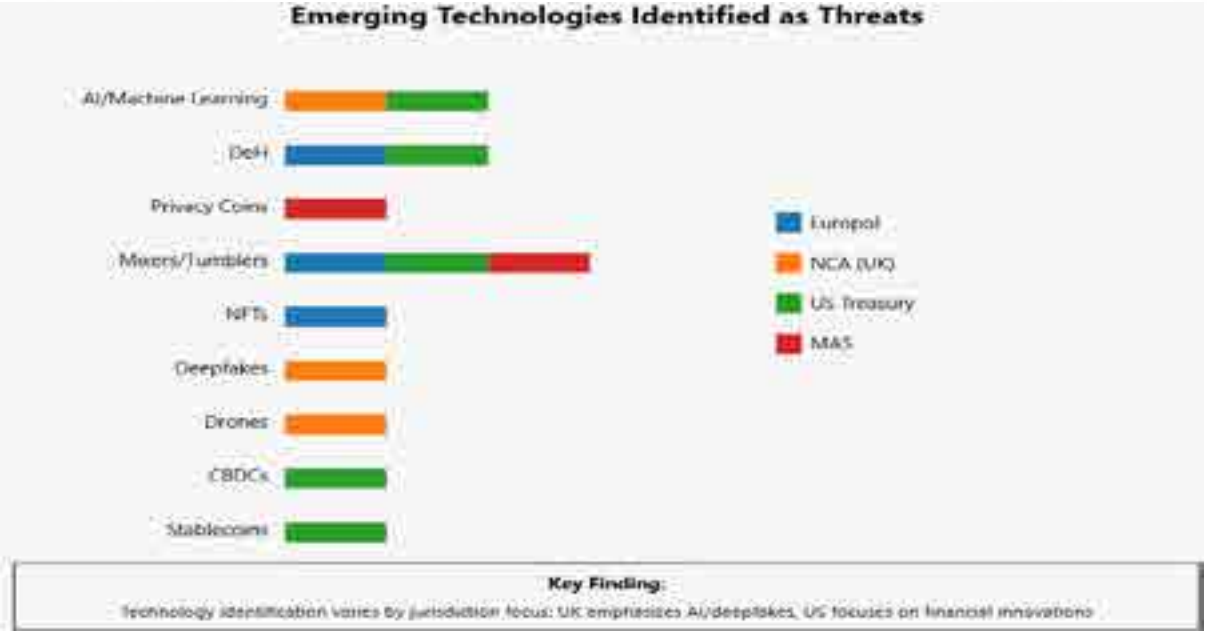
Source: Author's elaboration (2025)

The cross-border nature of transactions emerges as universal consensus, identified as the principal challenge by all jurisdictions. However, significant divergences appear in the prioritization of other challenges: while the USA (US Treasury, 2024) and Singapore (MAS, 2024) emphasize transaction speed as a critical obstacle to enforcement, the United Kingdom (NCA, 2025) dedicates greater attention to technological evolution and regulatory gaps.

4.3 Common Challenges and Differentiated Responses

The analysis reveals that although jurisdictions face similar challenges, their responses vary significantly. Figure 3 illustrates the intensity of focus on different enforcement mechanisms.

Figure 3. Emerging Technologies Identified as Threats



Source: Author's elaboration (2025)

The United States (US Treasury, 2024) demonstrates the most comprehensive approach, with strong emphasis on regulatory updates, sanctions, and asset recovery. Singapore (MAS, 2024) concentrates efforts on regulatory frameworks and rigorous KYC/AML requirements, while the United Kingdom (NCA, 2025) balances operational enforcement with technological innovation. Europol (2024), limited by its regional mandate, focuses primarily on operational coordination and intelligence analysis.

4.4 International Cooperation Mechanisms

International cooperation emerges as an area of significant divergence between jurisdictions. Table 5 maps the international organizations and cooperation mechanisms mentioned in each document.

Table 5. International Cooperation Mechanism by Jurisdiction

Organization/Mechanism	Europol (2024)	NCA (2025)	US Tresury (2024)	MAS (2024)
FATF	Not Mentioned	Not Mentioned	Extensive	Extensive
Interpol	Not Mentioned	Limited	Via FATF	Not Mentioned
Bilateral Agreements	Operational	Multiple	Extensive	RFAs Mentioned
G7 / G20	Not Mentioned	Not Mentioned	Active	Not Mentioned
UN Security Council	Not Mentioned	Not Mentioned	Referenced	Sanctions
Regional Bodies	EU framework	Post-Brexit	FSRBs	FSRBs
Task Forces	Operational	CRONOS	REPO	Not Mentioned

Legend: Extensive = Major focus with detailed discussion | Limited =Briefly Mentioned | Not mentioned = absent from document.

Source: Author's elaboration (2025)

The analysis reveals significant fragmentation in international cooperation mechanisms. The United States (US Treasury, 2024) and Singapore (MAS, 2024) demonstrate strong alignment with FATF frameworks, while operational documents (Europol, 2024; NCA, 2025) focus primarily on bilateral cooperation and specific task forces. This divergence suggests disconnection between strategic and operational levels of international cooperation.

4.5 Summary of Main Findings

The comparative analysis reveals three fundamental patterns in jurisdictional responses to the crypto-cybercrime nexus:

Despite universal recognition of cross-border nature as the principal challenge, jurisdictions diverge substantially in operational priorities and response mechanisms. This fragmentation is particularly evident in the identification of emerging technologies and implementation of international cooperation frameworks.

Each jurisdiction has developed distinctive competencies aligned with their institutional priorities - Singapore with preventive regulatory frameworks, United Kingdom with operational response and intelligence, United States with regulatory modernization and sanctions, and Europol with regional coordination and trend analysis.

The absence of FATF mentions in operational documents (Europol, NCA) versus their centrality in strategic documents (US Treasury, MAS) suggests disconnection between governance levels. Similarly, variation in identifying malicious actors - from specific criminal groups by nationality (NCA) to emphasis on state actors (US Treasury) - indicates lack of common taxonomy for threats.

These results evidence that although the crypto-cybercrime problem is globally recognized, responses remain fragmented and potentially inadequate to face threats that operate without jurisdictional restrictions. The next section will discuss the implications of these findings for international cooperation and public policy development.

Conclusion

The study identified three fundamental patterns: First, jurisdictions have developed distinct specializations aligned with institutional priorities - Singapore emphasizes preventive regulatory frameworks, the UK focuses on operational intelligence, the US prioritizes regulatory modernization with sanctions, and Europol concentrates on regional coordination. Second, significant fragmentation exists in international cooperation, with strategic documents (US, Singapore) aligning with FATF frameworks while operational documents (Europol, UK) focus on bilateral cooperation, suggesting disconnection between governance levels. Third, jurisdictions show varying capacity to identify emerging technological threats, indicating absence of common threat assessment frameworks.

This research faced important limitations including differential document availability across jurisdictions, under-representation of Global South perspectives, and focus on English-language sources. Documentary analysis captures only formally expressed policies rather than practical implementation or effectiveness. Future research should complement this analysis with empirical studies examining policy implementation and real-world outcomes.

Despite limitations, this research provides valuable insights for practitioners. Small and medium-sized jurisdictions can adapt proven approaches identified here, such as Singapore's compliance frameworks or the UK's intelligence-driven enforcement. Law enforcement agencies can benefit from understanding jurisdictional differences in crime categorization to improve information sharing.

The normative implications of these divergences extend beyond technical regulatory challenges. The fragmentation in responses reflects deeper disputes about digital sovereignty, state authority in decentralized systems, and balance between innovation and security. The increasing sophistication of state-sponsored cybercrime and emergence of "cyber mercenaries" challenges traditional distinctions between criminal and national security threats, requiring new frameworks for international cooperation transcending conventional law enforcement paradigms. The rapid evolution of technologies like privacy coins, decentralized finance protocols, and potential CBDCs demands adaptive regulatory approaches capable of responding to innovation while maintaining security imperatives.

Future research should focus on empirical implementation studies examining how policies translate into operational outcomes, longitudinal analysis of regulatory evolution tracking adaptation to emerging threats, and expanded geographical coverage incorporating Global South perspectives currently underrepresented in scholarly literature. Quantitative effectiveness assessments measuring actual impact of different regulatory approaches on crime reduction would provide crucial evidence for policy optimization. The crypto-cybercrime nexus represents a defining challenge for global governance in the digital age, requiring innovative coordination mechanisms transcending traditional territorial sovereignty while respecting legitimate concerns about digital autonomy and innovation.

References

ALBRECHT, Chad; DUFFIN, Kristopher; ALBRECHT, Conan; ROCHA, Victor Morales. The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*, v. 22, n. 2, p. 210-216, 2019. DOI: 10.1108/JMLC-12-2017-0074.

ANTONOPOULOS, A. M. *Mastering Bitcoin: Programming the Open Blockchain*. 2. ed. Sebastopol: O'Reilly Media, 2017.

AUGUST, T.; ZHANG, M.; CHEN, Z. The impact of cryptocurrency on cybersecurity. *Management Science*, v. 71, n. 3, p. 1282-1299, 2025. DOI: 10.1287/mnsc.2023.00969.

AUER, Raphael; BÖHME, Rainer. The technology of retail central bank digital currency. *BIS Quarterly Review*, 1 mar. 2020. Disponível em: https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

BA, H.; ŞEN, Ö. F. Explaining variation in national cryptocurrency regulation: implications for the global political economy. *Review of International Political Economy*, v. 31, n. 5, p. 1-25, 2024. DOI: 10.1080/09692290.2024.2325403

BARRATT, M. J.; ALDRIDGE, J. Everything you always wanted to know about drug cryptomarkets (*but were afraid to ask). *International Journal of Drug Policy*, v. 35, p. 1-6, 2016. DOI: 10.1016/j.drugpo.2016.07.005

BOWEN, G. A. Document analysis as a qualitative research method. *Qualitative Research Journal*, v. 9, n. 2, p. 27-40, 2009. DOI: 10.3316/QRJ0902027

BRASIL. Lei nº 14.478, de 21 dez. 2022. Dispõe sobre o marco legal dos ativos virtuais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14478.htm.

BUCHANAN, B. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. New York: Oxford University Press, 2017.

CARDNO, Carol. Policy document analysis: a practical educational leadership tool and a qualitative research method. *Educational Administration: Theory and Practice*, v. 24, n. 4, p. 623-640, 2018. Disponível em: https://files.eric.ed.gov/fulltext/EJ1305631.pdf.

CHAINALYSIS. *2025 Crypto Crime Report*. New York: Chainalysis Inc., 2025.

CHOUCRI, N.; ANAYA, J. CyberIR@MIT: Exploration and Innovation in International Relations 2.0. *MIT Political Science Department Research Paper* 2024-4, 2024. DOI: 10.2139/ssrn.3936863

CHRISTIN, N. Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In: *Proceedings of the 22nd International Conference on World Wide Web*. Rio de Janeiro: ACM, 2013. p. 213-224.

CLARKE, R. V.; FELSON, M. (Ed.). *Routine Activity and Rational Choice*. New Brunswick: Transaction Publishers, 1993.

COHEN, L. E.; FELSON, M. Social change and crime rate trends: A routine activity approach. *American Sociological Review*, v. 44, n. 4, p. 588-608, 1979. DOI:10.2307/2094589

COLEBATCH, H. K. *Policy*. 3. ed. Maidenhead: Open University Press, 2009 [1. ed. 1997].

CONTI, M.; GANGWAL, A.; RUJ, S. On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers & Security*, v. 79, p. 162-189, 2018. DOI: 10.1016/j.cose.2018.08.008.

DEIBERT, R. Three painful truths about social media. *Journal of Democracy*, v. 30, n. 4, p. 77-90, 2019 Disponível em: https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/

FANUSIE, Y.; ROBINSON, T. *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*. Washington: Center on Sanctions and Illicit Finance, 2018.

FARBER, S. The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *SSRN Electronic Journal*, 2025. Disponível em: http://dx.doi.org/10.2139/ssrn.5228798

FATF – Financial Action Task Force. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris: FATF/OECD, 2019.

FOLEY, S.; KARLSEN, J. R.; PUTNIŅŠ, T. J. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies*, v. 32, n. 5, p. 1798-1853, 2019. Disponível em: http://dx.doi.org/10.2139/ssrn.3102645

GALASSO, J. The crypto revolution: A comparative analysis of crypto regulation in the United States and the European Union. *Touro Law Review*, v. 39, n. 4, p. 1-45, 2024. Disponível em: https://digitalcommons.tourolaw.edu/lawreview/vol39/iss4/12

HOUBEN, R.; SNYERS, A. *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. Bruxelas: European Parliament, 2018. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)619024.

HU, J. The regulation of cryptocurrency in China. *International Journal of Digital Law and Governance*, v. 1, 2024.

HUGHES, S. J.; MIDDLEBROOK, S. T. Advancing a framework for regulating cryptocurrency payments intermediaries. *Yale Journal on Regulation*, v. 32, n. 2, p. 495-559, 2015. Disponível em: https://www.cs.yale.edu/homes/jf/Hughes.pdf

IRWIN, A. S. M.; MILAD, G. The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control*, v. 19, n. 4, p. 407-425, 2016. DOI: 10.1108/JMLC-01-2016-0003

KEOHANE, R. O.; NYE, J. S. *Power and Interdependence*. 4. ed. Boston: Longman, 2011.

MAURER, T. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2018.

MCGUIRE, M.; DOWLING, S. *Cyber crime: A review of the evidence*. Londres: Home Office, 2013. (Research Report 75).

NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press, 2016.

O'LEARY, Z. *The essential guide to doing your research project*. 2. ed. Londres: SAGE Publications, 2014.

OLADIPUPO, O. Sanctions evasion 2.0: unpacking the role of cryptocurrency in North Korea and Iran's external trade relations. *Lead City Journal of the Social Sciences*, v. 10, n. 1, 2025. Disponível em: https://www.researchgate.net/publication/392312032_Sanctions_Evasion_20_Unpacking_the_Role_of_Cryptocurrency_in_North_Korea_and_Iran's_External_Trade_Relations.

PRIOR, Lindsay. *Using documents in social research*. Londres: SAGE Publications, 2003.

RID, T.; BUCHANAN, B. Attributing cyber attacks. *Journal of Strategic Studies*, v. 38, n. 1-2, p. 4-37, 2015.DOI: 10.1080/01402390.2014.977382.

RIHOUX, B.; RAGIN, C. C. (Ed.). *Configurational comparative methods: Qualitative comparative analysis (QCA) and related techniques*. Thousand Oaks: SAGE Publications, 2009. DOI: 10.4135/9781452226569.

ROSENAU, James N. *Along the domestic-foreign frontier: exploring governance in a turbulent world*. Cambridge: Cambridge University Press, 1997. DOI: 10.2307/2585471.

SCHREIER, M. *Qualitative content analysis in practice*. Londres: SAGE Publications, 2012.

WALL, D. S. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press, 2007.

WALTZ, Kenneth N. *Theory of international politics*. Reading, MA: Addison-Wesley, 1979.

WENDT, A. (2000). *A Social Theory of International Politics*. Social Theory of International Politics. 26. DOI 10.1017/CBO9780511612183

WORLD BANK. *Cryptocurrencies and Blockchain: Policy Objectives and Regulatory Approaches*. Washington: World Bank Group, 2018.

YANOW, Dvora. Qualitative-interpretive methods in policy research. In: FISCHER, Frank; MILLER, Gerald J.; SIDNEY, Mara S. (Ed.). *Handbook of public policy analysis: theory, politics, and methods*. Boca Raton: CRC Press, 2007. p. 405-415.

ZETZSCHE, D. A.; ARNER, D. W.; BUCKLEY, R. P.; WEBER, R. H. The Markets in Crypto-Assets regulation (MICA) and the EU digital finance strategy. *Capital Markets Law Journal*, v. 15, n. 2, p. 203-225, 2020. Disponível em: http://dx.doi.org/10.2139/ssrn.3725395