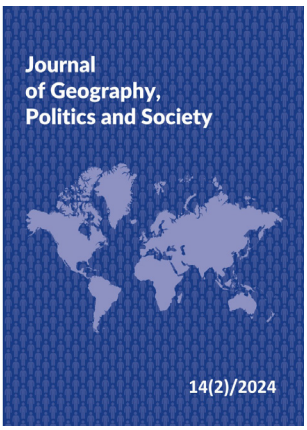

Journal of Geography, Politics and Society
2024, 14(2), 1–22
https://doi.org/10.26881/jpgs.2024.2.01

CYBERCRIMES IN THE CRYPTOCURRENCY DOMAIN: IDENTIFYING TYPES, UNDERSTANDING MOTIVES AND TECHNIQUES, AND EXPLORING FUTURE DIRECTIONS FOR TECHNOLOGY AND REGULATION

Shobhit Navani (1), Giuseppe T. Cirella (2)

(1) Faculty of Economics, University of Gdańsk, Armii Krajowej 119/121, 81-824,Sopot, Poland, ORCID: 0000-0002-3167-007X
e-mail: s.navani.958@studms.ug.edu.pl
(2) Faculty of Economics, University of Gdańsk, Armii Krajowej 119/121, 81-824, Sopot, Poland and University Center for Social and Urban Research, University of Pittsburgh, 3343 Forbes Avenue, 15260, Pittsburgh, PA, United States, ORCID: 0000-0002-0810-0589
e-mail: gt.cirella@ug.edu.pl (corresponding author)

Citation
Navani S., Cirella G.T., 2024, Cybercrimes in the Cryptocurrency Domain: Identifying Types, Understanding Motives and Techniques, and Exploring Future Directions for Technology and Regulation, *Journal of Geography, Politics and Society,* 14(2), 1–22.

Abstract
Cryptocurrency has emerged as a lucrative yet volatile landscape for cybercriminal activity, presenting novel challenges for law enforcement and policymakers alike. This review seeks to explore the diverse array of cybercrimes occurring within the cryptocurrency domain, examining their types, motives, techniques, and the regulatory responses shaping this complex ecosystem. Utilizing a scoping literature search methodology, this study analyzes 228 pertinent sources drawn from a pool of over 4,000 reviewed publications. The findings elucidate the intricate interplay between cryptocurrencies and illicit activities, revealing the multifaceted nature of cybercrimes within this realm. From the exploitation of the dark web for illicit transactions to the pervasive threat of crypto ransomware targeting entities globally, the review underscores the diverse methods and motivations driving such nefarious endeavors. By shedding light on the evolving tactics employed by cybercriminals and exploring future directions for technological and regulatory measures adopted by governments, this paper offers valuable insights to navigate this dynamic landscape effectively.

Key words
Bitcoin, illicit activities, money laundering, organized crime, regulatory measures.

Received: 22 July 2024 **Accepted**: 22 September 2024 **Published**: 31 December 2024

1. Introduction

Cryptocurrency finds its roots in cryptography, a discipline dating back to 1900 BC when hieroglyphics in an Egyptian tomb revealed early evidence of its use (Sidhpurwala, 2023). The term "cryptography" originates from the Greek words "kryptos" and "graphein," signifying "hidden secret" and "writing," respectively, encapsulating the practice of concealing information (Aggarwal, Jaiswal, 2011). The birth of the original cryptocurrency, Bitcoin, is attributed to the mysterious figure Satoshi Nakamoto in 2008. Nakamoto laid out the foundational principles in the Bitcoin Manifesto (Nakamoto, 2009), envisioning a comprehensive electronic currency operating on a peer-to-peer network model, enabling direct online payments without reliance on traditional financial intermediaries. Thus, cryptography, with

its ancient roots and modern applications, serves as the fundamental underpinning of the revolutionary concept of cryptocurrency.

Digital currencies play a pivotal role in reshaping the global economy, granting consumers broader access to goods and services since the advent of the internet. These virtual currencies facilitate direct peer-to-peer exchanges, circumventing traditional central clearinghouses. While not officially recognized as legal tender, these currencies may hold equivalent value to conventional currencies. The legal framework often lags behind technological advancements, and governments are just beginning to grapple with the challenges posed by emerging digital currencies. Simultaneously, the utilization of Bitcoin, among the most widely adopted virtual currencies, is experiencing rapid growth (Munawa, 2023; Otabek, Choi, 2024; Riahi et al., 2024). Key attributes of the Bitcoin system include its decentralized structure, free from governmental influence, and the capability for pseudonymous currency usage (Otabek, Choi, 2024).

Similar to historical technological advancements, individuals bear the responsibility to either advance societal progress or exploit innovations for concealed motives. The inherent anonymity of cryptocurrencies often entangles them in illicit activities, a focus of this literature review. The darknet, a subset of the deep web, is substantially larger than the surface web (Hatta, 2020; Raman et al., 2023; Rudesill et al., 2015), where the anonymous nature of cryptocurrency is prevalent in various illicit activities, categorizing organized crime into drug trafficking, terrorism, money laundering, and the distribution of child sexual abuse material (CSAM). The review aims to investigate the role of Bitcoin and other cryptocurrencies in criminal activities, highlighting the need for a unified regulatory framework. The coding process scrutinizes specific objectives, including identifying criminal activities, synthesizing regulatory findings, and categorizing papers based on geography, publication year, and publishing houses.

2. Materials and methods

The study systematically searched through a range of electronic journal databases and search engines, including Bing, Directory of Open Access Journals, Google, Google Scholar, Publons, ResearchGate, Scopus, Semantic Scholar, and Web of Science. In the search process, specific English language keywords, such as "bitcoin + criminality," "bitcoin + international regulations," "bitcoin + volatility," "cryptocurrency + child pornography," "cryptocurrency + organized crimes," "cryptocurrency + regulations," "cryptocurrency + scams," "cybercrime," "darknet," "drug trafficking," "illegal weapon sales," "money laundering," "crypto ransomware," "rug pull," "terrorism," and "wallet hack," were systematically employed. After compiling the literature, a systematic analysis was conducted to identify publications presenting specific findings on the darknet, cybercrime, crypto ransomware, organized crime, hacking, computer viruses, and regulatory law related to cryptocurrency. This analysis was conducted using strategic and critical reading methods (Matarese, 2013; Renear, Palmer, 2009).

In our initial literature review, we identified over 4,000 articles, reviews, and grey literature. To refine our focus, articles published before 2008 were excluded, as the concept of cryptocurrency was in its infancy prior to the launch of Bitcoin. Following this initial filtering process, we identified 845 peer-reviewed publications relevant to cryptocurrency and cybercrime. Further in-depth reviews narrowed down the selection to 228 publications, including literature in the form of books, journal articles, and technical reports. This study relies on desk research, gathering and analyzing data from diverse secondary sources and cryptocurrency-related websites. After filtering these sources, we compiled and discussed the findings, aiming to provide insights into the nature and extent of cybercrime associated with cryptocurrencies. As the study hinges on secondary data, it does not utilize a specific sample; nonetheless, rigorous attention is paid to ensuring the relevance and currency of the collected data. The anticipated findings are poised to offer valuable insights into the contemporary landscape of cybercrime within the cryptocurrency domain, significantly contributing to the formulation of more effective preventive measures against such crimes in the future.

3. Results

3.1. Geographic and timeline results

In the analysis, the literature underscores the worldwide significance of cybercrime and cryptocurrency as a central focus of research. Notably, leading research endeavors from the US highlight the nation's influential role in shaping discussions and advancements in this sphere (DOJ, 2015; Dupont, Holt, 2022; ICE, 2020; Kayani, Hasan, 2024; Raman et al., 2023; Widhiyanti et al., 2023). Ukraine and Russia, interestingly for example, have emerged as prominent hubs for cybercrimes linked to cryptocurrency, revealing a thriving crypto landscape predating current geopolitical events and indicating significant interest and investment

among Ukrainians and Russians (Cong et al., 2022; Dyntu, Dykyi, 2019; Ivaniuk, Banakh, 2020; Pushkarev et al., 2020; Turchyn, Turchyn, 2021).

European research also provides substantial contributions, offering diverse perspectives and regulatory frameworks that enhance our understanding of cryptocurrency and crime. Topics such as regulatory approaches, adoption rates, and technological innovations are extensively explored, shedding light on the nuanced complexities of the cryptocurrency landscape (Godlove, 2014; Lapuh Bele, 2021; Matarese, 2013; Nazzari, Riccardi, 2024). Similarly, contributions from Asia, including regions like China, India, and Indonesia, offer invaluable insights into adoption trends, blockchain technology developments, and regulatory challenges specific to the region (Chuan, O'Leary, 2021; Mubarak, Manjunath, 2021; Piazza, 2017).

North and Central America, with their vibrant cryptocurrency ecosystems, contribute essential research on market trends, regulatory frameworks, and the impact of cryptocurrency on traditional financial systems (Bhaskar et al., 2019; Biswas, 2018; Kayani, Hasan, 2024; Kethineni et al., 2018). Contributions from other continents, such as South America (Pop, Colonescu, 2021; Pushkarev et al., 2020; Virga, 2015) , Africa (Interpol, 2020; Reddy, 2020; Reddy et al., 2020; Sanusi, Dickason-Koekemoer, 2022), and Australia (Australian Home Affairs, 2022; Dupont, Holt, 2022; Morelato et al., 2020), enrich our understanding by exploring diverse cultural, economic, and regulatory contexts (Figure 1).

This amalgamation of research from various continents underscores the global nature of cryptocurrency and highlights its profound implications over illicit activities via finance and technology. This global perspective fosters a comprehensive understanding of the evolving cryptocurrency landscape, facilitating informed decision-making and policy development in the field.

Moreover, in recognition of the pressing need to disseminate credible information amid the rapid pace of technological advancements and emerging threats, we also conducted an examination of the literature based on publishing houses and sources. This approach aimed to reinforce the reliability and credibility of our study. Among the prominent publishers, Springer emerged as the foremost contributor, exemplifying its commitment to advancing scholarly discourse in the field. Additionally, significant contributions were made

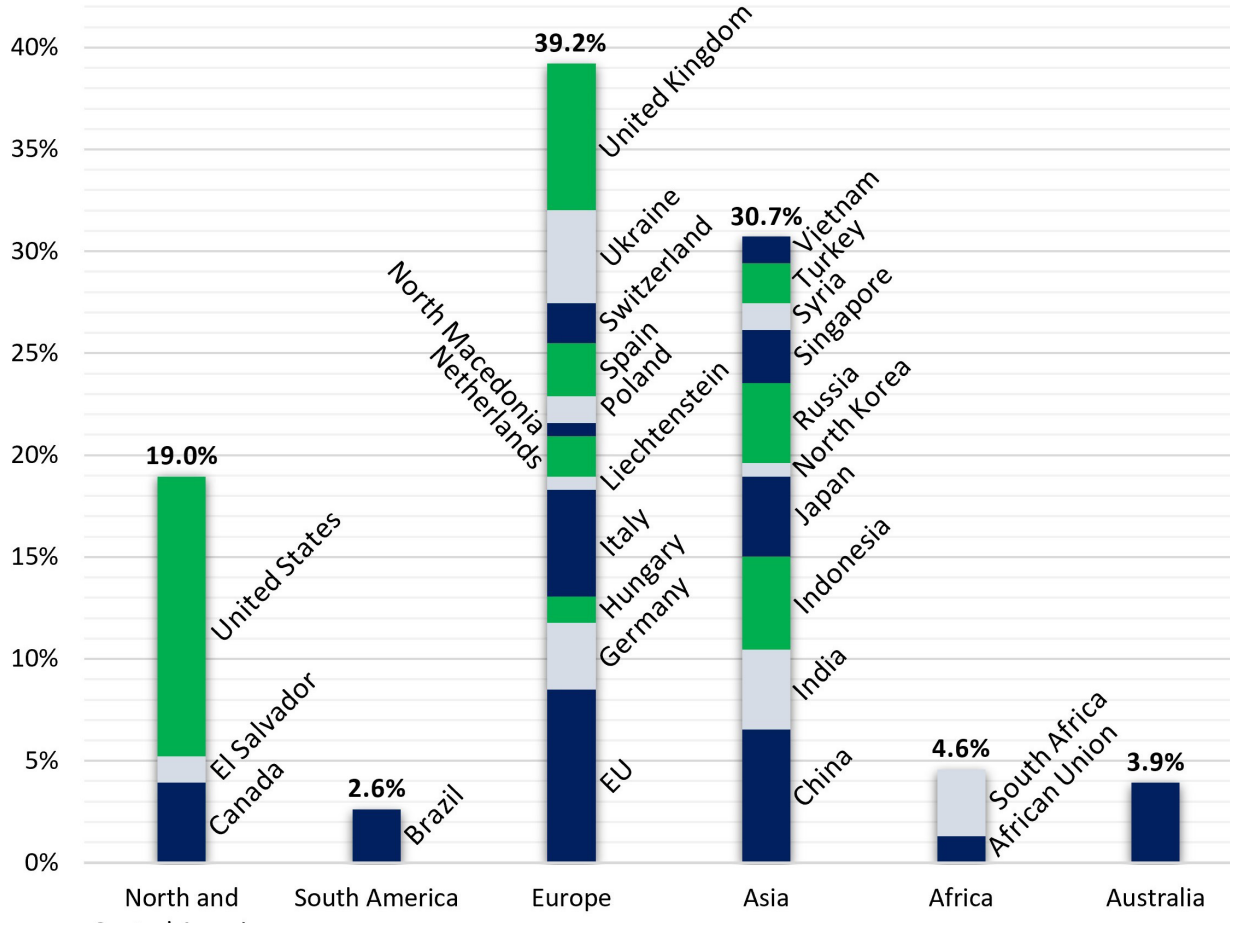

Fig. 1. Geographic distribution of the reviewed literature by continent.
Source: own study.

by Elsevier, Emerald, Frontiers, IEEE, MDPI, Oxford University Press, Routledge, SAGE, and Taylor and Francis, highlighting their pivotal role in fostering robust research dissemination. Notably, nearly half of the reviewed sources (i.e., 97) originated from diverse publishing sources such as specific university press publishers, governmental reports, and dedicated cryptocurrency websites. This diverse array of publishing houses and sources contributed to the comprehensive scope and depth of the research topic, enriching the study with a multitude of perspectives and insights from various sectors and disciplines.

In the reviewed literature, spanning from 2008 to 2024, we identified notable patterns in the publication trends concerning cryptocurrency and cybercrime. Particularly striking was the pronounced uptick in the volume of reviewed sources observed in recent years. Notably, we observed a significant spike in the number of reviewed sources in recent years, with 2020 standing out as the year with the highest publication count, totaling 43 sources. This surge was followed closely by 33 sources in 2022, 30 in 2021, 28 in 2023, and 26 in 2024 (Figure 2). This trend reflects the growing interest and recognition of the importance of studying cybercrime within the context of cryptocurrency. With the rapid advancement of technology and the increasing prevalence of cryptocurrencies in various aspects of society, researchers and scholars are increasingly drawn to investigate the intersection of these two domains. The surge in publications in recent years underscores the urgency and relevance of addressing cybercrime in the cryptocurrency sphere.

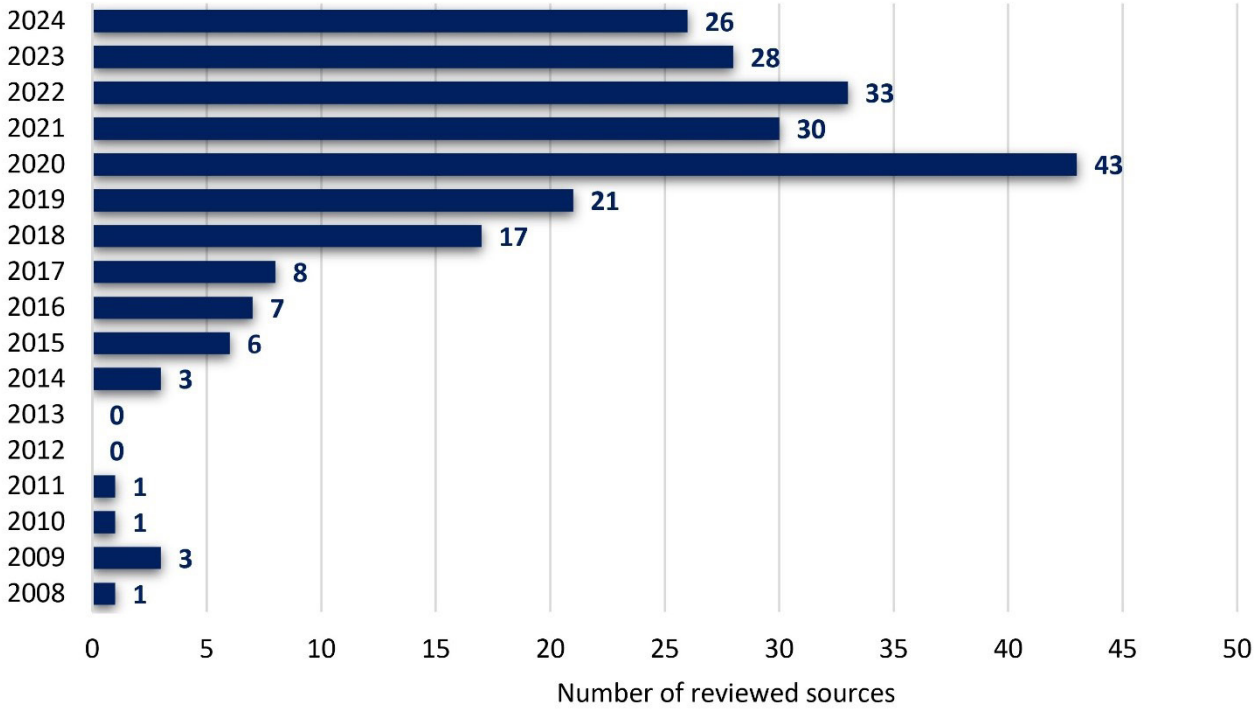

Fig. 2. Publication timeline of the reviewed literature, N = 228.
Source: own study.

Moreover, the proliferation of research in this area suggests a concerted effort to understand and combat the evolving threats posed by cybercriminal activities leveraging cryptocurrencies (Dudani et al., 2023; Patsakis et al., 2023; Volevodz, 2024). As these digital assets continue to gain traction and prominence in global economies, it becomes imperative to stay abreast of the latest developments and challenges in safeguarding against illicit activities in the digital realm (Bahamazava, Nanda, 2022; dos Reis et al., 2024; Kayani, Hasan, 2024). Overall, the upward trajectory of research publications in cybercrime and cryptocurrency reflects a proactive response to the dynamic landscape of digital finance (Auer, Tercero-Lucas, 2022; Kayani, Hasan, 2024) and underscores the collective commitment to fostering a safer and more secure digital environment.

3.2. Typological findings

After conducting an exhaustive analysis of the literature under review, we uncovered the prevalent forms of cybercrimes and their distinguishing characteristics, adhering closely to our predetermined criteria. By harnessing a vast array of scholarly sources, we thoroughly piece together key themes and emerging trends associated with crimes involving cryptocurrencies, providing deep insights into the intricate complexities of these illicit activities

and the varied regulatory responses enacted by governments worldwide. To structure our typological findings systematically, we identified key categories such as the darknet, cybercrime, crypto ransomware, and organized crime. Organized crime was further refined to encompass specific crimes, including drug trafficking, terrorism, money laundering, and CSAM. Within this categorization, various cryptocurrency coins were identified. However, in cases where a specific coin was not specified, it was categorized under Bitcoin and cryptocurrencies in general. Moreover, a detailed comparison between centralized and decentralized cryptocurrency exchanges, focusing on their key differences, advantages, and disadvantages, is provided as supplementary material (see Supplementary Data—S1). The supplementary material is organized into logical categories to facilitate understanding and comparison. This addition aims to provide readers with comprehensive insights into the distinct characteristics of each type of exchange, helping them make informed decisions based on their preferences and requirements. Additionally, we included an examination of government regulations and factors influencing cryptocurrency development and pricing. This comprehensive approach allowed us to explore how different countries and regions worldwide are grappling with the challenges and advancements in this dynamic field. Table 1 illustrates a comprehensive breakdown of the multifaceted landscape of cybercrimes involving cryptocurrencies and the regulatory landscape shaping this dynamic field.

Tab. 1. Topological breakdown of cybercrimes involving cryptocurrencies and the regulatory landscape of the reviewed literature

Categorization	Coin	N	References
Darknet	Bitcoin and cryptocurrencies in general	51	Ahuja et al. (2021), Alfieri (2022), Bahamazava, Nanda (2022), Bayramova et al. (2021), Bhaskar et al. (2019), Böhme et al. (2015), Broadhead (2018), Butler (2019), Chertoff, Simon (2015), Choi et al. (2020), Collins (2022), Davies (2020), Del Monaco (2020), DOJ (2017), dos Reis et al. (2024), Dupuis, Gleason (2020), Dyntu, Dykyi (2019, 2021), ElBahrawy et al. (2020), Finklea (2017), Gupta et al. (2021), Hatta (2020), Holt et al. (2023), Jung et al. (2022), Keane (2020), Kethineni et al. (2018), Kethineni, Cao (2020), Lacson, Jones (2016), Lee et al. (2022), Lee et al. (2019), Luong (2023), Mackenzie (2022), Mataković (2022), Meland et al. (2020), Mirea et al. (2019), Morelato et al. (2020), Naqvi (2018), Nazzari (2023), Piazza (2017), Raman et al. (2023), Reddy, Minaar (2018), Rubasundram (2019), Rudesill et al. (2015), Şcheau et al. (2020), Silfversten (2020), Stroukal, Nedvědová (2016), Tan (2024), UNODC (2020, 2023), van Wegberg et al. (2018), Virga (2015)
	Monero	2	Bahamazava, Nanda (2022), Florea, Nitu (2020)
Cybercrime	Bitcoin and cryptocurrencies in general	79	Agarwal et al. (2024), Alfieri (2022), Alqahtany, Syed (2024), Andres Rodriguez-Nieto, Eremina (2023), Auer, Tercero-Lucas (2022), Badawi, Jourdan (2020), Bajra et al. (2024), Balaskas, Franqueira (2018), Bartoletti et al. (2021), Blasco, Fett (2019), Boehm, Pesch (2014), Bray (2016), Broadhead (2018), Brown (2016), Caporale et al. (2020), CERT-Bund (2022), Choi et al. (2009), Choi et al. (2020), Choi, Parti (2022), Ciphertrace (2023), Cong et al. (2022), Connolly, Wall (2019), Conventus Law (2021), Corbet et al. (2020), Courtois (2014), Critien et al. (2022), Custers et al. (2020), Del Monaco (2020), DOJ (2015), Dudani et al. (2023), Dupont, Holt (2022), Dyntu, Dykyj (2021), Dyson et al. (2018), Etto (2017), FBI (2022), Fosso Wamba et al. (2020), Gercke (2009), Gryszczyńska (2021), Gupta et al. (2021), Higbee (2018), Ivaniuk, Banakh (2020), Jung et al. (2022), Kerr et al. (2023), Kethineni et al. (2018), Kristoufek (2015), Kutera (2022), Lapuh Bele (2021), Lee (2019), Liao et al. (2016), Luong (2023), Mackenzie (2022), Mataković (2022), Mthembu et al. (2022), Pilinkiene et al. (2022), Priyambudi, Sinaga (2021), Recskó, Aranyossy (2024), Reddy, Minaar (2018), Riahi et al. (2024), Rieckmann, Stuchtey (2023), Rudesill et al. (2015), Saiedi et al. (2021), Sanusi, Dickason-Koekemoer (2022), Shinder, Cross (2008), Sigler (2018), Taylor et al. (2021), Team (2024), Thamizhisai et al. (2024), Trozze et al. (2022), UNODC (2020), van Nguyen et al. (2022), van Wegberg et al. (2018), Verduyn (2018), Virga (2015), Volevodz (2024), Watters (2023), Wronka (2022a, 2022b), Zheng (2024)
	Monero	3	Dyson et al. (2018), Gohwong (2019), Zimba et al. (2020)
	Ethereum	8	Andres Rodriguez-Nieto, Eremina (2023), Auer, Tercero-Lucas (2022), Bajra et al. (2024), Caporale et al. (2020), Dyson et al. (2018), Etto (2017), Kerr et al. (2023), Mthembu et al. (2022)
	Tether	2	Kerr et al. (2023), Mthembu et al. (2022)
	Binance	2	Kerr et al. (2023), Mthembu et al. (2022)
	USD Coin	1	Kerr et al. (2023)

Categorization		Coin	N	References
Crypto ransomware		Bitcoin and cryptocurrencies in general	22	Badawi, Jourdan (2020), Broadhead (2018), Butler (2019), CERT-Bund (2022), CISA (2023), Cong et al. (2022), Connolly, Wall (2019), Custers et al. (2020), Gercke (2009), Ghalwesh et al. (2020), Gómez-Hernández, García-Teodoro (2024), Gray et al. (2023), Hernandez-Castro et al. (2020), Kerr et al. (2023), Meland et al. (2020), Muslim et al. (2019), Naqvi (2018), Nazzari (2023), Paquet-Clouston et al. (2019), Reddy, Minaar (2018), Sherer et al. (2016), Turner et al. (2020)
		Monero	5	CERT-Bund (2022), Gómez-Hernández, García-Teodoro (2024), Gohwong (2019), Patsakis et al. (2023), Zimba et al. (2020)
Organized crime	Drug trafficking	Bitcoin and cryptocurrencies in general	16	Ali (2021), Bertola (2020), Bhaskar et al. (2019), Butler (2019), Durrant (2018), Europol (2021), Godlove (2014), Kabra, Gori (2023), Keane (2020), Luong (2023), Mirea et al. (2019), Naheem (2021), Nurhadiyanto (2020), Pieroni (2018), Saiedi et al. (2021), Zaunseder, Bancroft (2020)
	Terrorism	Bitcoin and cryptocurrencies in general	20	Alfieri (2022), Biswas (2018), Dion-Schwarz et al. (2019), DOJ (2015), Durrant (2018), Gercke (2009), Gupta et al. (2021), Ilijevski et al. (2023), Keane (2020), Kfir (2020), Luong (2023), Moore, Rid (2016), Patel, Richter (2020), Reynolds, Irwin (2017), Rubasundram (2019), Thamizhisai et al. (2024), Teichmann, Falker (2020, 2024), Wang, Zhu (2021), Zavoli (2022)
	Money laundering	Bitcoin and cryptocurrencies in general	58	Agarwal et al. (2024), Ambrus, Mezei (2022), Barone, Masciandaro (2019), Boehm, Pesch (2014), Brown (2016), Butler (2019), Ciphertrace (2023), Clements (2021), Collins (2022), Custers et al. (2020), Del Monaco (2020), Dupuis, Gleason (2020), Durrant (2018), Dyntu, Dykyi (2019, 2021), Europol (2021), Gercke (2009), Godlove (2014), Goldbarsht (2024), Goodell, Aste (2019), Helwig et al. (2022), Hendrickson, Luther (2022), Holt et al. (2023), Ilijevski et al. (2023), Irwin & Slay (2010), Johari et al. (2019), Keane (2020), Kutera (2022), Leuprecht et al. (2022), Luong (2023), Manjula et al. (2022), Masciandaro et al. (2019), Munawa (2023), Naheem (2021), Nazzari (2023), Nazzari, Riccardi (2024), Nurhadiyanto (2020), Perkins (2021), Pieroni (2018), Pilinkiene et al. (2022), Pushkarev et al. (2020), Reddy, Minaar (2018), Reynolds, Irwin (2017), Riahi et al. (2024), Rubasundram (2019), Saiedi et al. (2021), Sanz-Bas et al. (2021), Schneider (2019), Sicignano (2021), Soni (2024), Teichmann, Falker (2020a, 2020b), van Wegberg et al. (2018), Virga (2015), Widhiyanti et al. (2023), Wronka (2022a), Yunandi, Leksono (2023), Zavoli (2022)
		Monero	3	Gohwong (2019), Teichmann, Falker (2020a, 2020b)
		Zcash	5	Dyson et al. (2018), Leuprecht et al. (2022), Silfversten (2020), Teichmann, Falker (2020a, 2020b)
		Ethereum	3	Leuprecht et al. (2022), Lin et al. (2023), Munawa (2023)
	CSAM	Bitcoin and cryptocurrencies in general	13	Broadhead (2018), Celiksoy, Schwarz (2023), Davies (2020), Finklea (2017), Gercke (2009), ICE (2020), Kristoufek (2015), Maxwell (2022), Naheem (2021), Nouwen (2017), Sayid (2023), UNODC (2020), van Nguyen et al. (2022)
Government regulations and factors influencing cryptocurrency development and pricing				Adam, Dzang Alhassan (2020), Aitken (2020), Alvarez et al. (2022), Al-Zubaidie, Jebbar (2024), Ambrus, Mezei (2022), Andronova et al. (2020), Auer, Tercero-Lucas (2022), Australian Home Affairs (2022), BaFin (2018), Boehm, Pesch (2014), Böhme et al. (2015), Bokovnya et al. (2020), Botha et al. (2023), CFTC (2017), Chand et al. (2024), Chen (2023), Cherniei et al. (2021), Chimienti et al. (2019), Chuan, O'Leary (2021), Clements (2021), Davies (2020), Del Monaco (2020), DOJ (2015), Dupuis, Gleason (2020), Dyntu, Dykyi (2019, 2021), Europol (2021), FBI (2022), Gercke (2009), Godlove (2014), Grasselli, Lipton (2021), Harryarsana (2022), Ilijevski et al. (2023), Interpol (2020), Kamps, Kleinberg (2018), Kavitha and Golden (2024), Kayani, Hasan (2024), Kethineni, Cao (2020), Kien, Binh (2021), Legge (2023), Liao et al. (2016), Lipton (2021), Mazambani (2024), Moffett (2023), Mthembu et al. (2022), Mubarak, Manjunath (2021), Omeljaniuk (2020), Otabek, Choi (2024), Özer et al. (2024), Ozturk, Sulungur (2021), Perkins (2021), Pernice, Scott (2021), Phugger (2021), Piazza (2017), Pop, Colonescu (2021), Priyambudi, Sinaga (2021), Pushkarev et al. (2020), Rajagopal (2020), Reddy (2020), Reiff et al. (2023), Reynolds, Irwin (2017), Rizzo (2017), Rueckert (2019), Sanz-Bas et al. (2021), Sicignano (2021), Sidhpurwala (2023), Sovbetov (2018), Suslenko et al. (2022), Tan (2024), Teichmann, Falker (2020a, 2020b), Turchyn, Turchyn (2021), van Nguyen et al. (2022), Verduyn (2018), Wen et al. (2024), Widhiyanti et al. (2023), Xie (2019), Zheng (2024), Zavoli (2022)

Note: Sources may fall into multiple categories.

Source: own study.

4. Discussion

By organizing the crimes into specific categories, we aimed to facilitate a deeper understanding of the complex dynamics at play within the realm of cybercrime and cryptocurrency. In essence, the study serves as a comprehensive resource for understanding the complex landscape of cybercrime involving cryptocurrencies, offering insights into key issues, trends, and policy considerations shaping this rapidly evolving domain. The categorization employed in the review is defined and broken down to highlight the impact of cryptocurrency on each category, offering a nuanced understanding of how these digital assets intersect with various forms of illicit activities. By dissecting the categorization utilized in the review, we delve into the multifaceted ways in which cryptocurrencies permeate and influence different realms of cybercrime. Each category is carefully examined to elucidate the mechanisms through which cryptocurrencies facilitate or exacerbate criminal activities. Through this granular exploration, we aim to unravel the complex interplay between digital currencies and illicit behaviors, shedding light on the challenges and opportunities presented by the proliferation of cryptocurrencies in the cybercrime landscape. Our analysis not only underscores the need for adaptive and agile approaches to combatting cyber threats but also underscores the importance of staying abreast of technological advancements and their implications for law enforcement and policy formulation.

4.1. The Darknet: hub of illicit transactions

Throughout the reviewed literature, a consensus has emerged regarding the pivotal role of the darknet as a hub for illicit activities, largely facilitated by transactions conducted using cryptocurrencies, which present significant challenges for tracking (Cong et al., 2022; Reynolds, Irwin, 2017). The anonymity inherent in the dark web frequently links it to illegal activities, encompassing a range of illicit actions such as drug trafficking, arms sales, hacking services, counterfeiting, distribution of CSAM, and financial fraud (Chertoff, Simon, 2015; Hatta, 2020; Raman et al., 2023). It is essential, however, to recognize that not all dark web activities are nefarious; it also provides refuge for whistleblowers, activists, and individuals seeking privacy, particularly in the face of authoritarian regimes (Böhme et al., 2015; Kfir, 2020; Patsakis et al., 2023). The combination of relatively easy access and the use of cryptocurrencies in transactions underscores the absence of a universal regulatory framework, effectively perpetuating bank secrecy within the dark web (Chertoff, Simon, 2015; Hatta, 2020; Piazza, 2017; Raman et al., 2023).

In 2011, Ross William Ulbricht launched Silk Road, a website accessible via the darknet, designed as a global online marketplace catering to illicit transactions (Figure 3). Silk Road primarily focused on facilitating the trade of narcotics, cybercrime exploit kits, stolen credit card information, and counterfeit passports. It leveraged Bitcoin as its exclusive payment method, enhancing user anonymity. Moreover, Silk Road provided money laundering services, employing tools such as mixers and tumblers to obfuscate transaction trails (Bhaskar et al., 2019; Courtois, 2014; Kethineni et al., 2018; Lacson, Jones, 2016; Reddy, Minaar, 2018).

Bitcoin plays an essential role in the dark web ecosystem due to its pseudonymous and decentralized nature (Bahamazava, Nanda, 2022; S. Choi et al., 2020; Kethineni et al., 2018). Unlike traditional currencies, Bitcoin transactions are not directly tied to individual identities, offering a level of anonymity. Instead, these transactions are recorded on a public ledger known as a blockchain, showcasing the movement of funds between Bitcoin addresses (Blasco, Fett, 2019; Phugger, 2021; Verduyn, 2018). While transaction details are visible, tracing the real-world identities behind the addresses proves challenging (Figure 4). Furthermore, Bitcoin's smart contract functionality enables the implementation of escrow services on dark web marketplaces. Escrow ensures the secure holding of buyer funds until the transaction is completed, mitigating the risk of scams or fraud. To enhance transaction privacy, Bitcoin tumblers or mixers are employed, which blend multiple transactions to obfuscate the origins of funds (Broadhead, 2018; Brown, 2016; Kethineni et al., 2018).

Moreover, privacy-focused cryptocurrencies such as Monero and Zcash present heightened anonymity features, offering both advantages and obstacles for law enforcement. Monero's transaction structure complicates the tracing process as signatures are pooled among a large group, making it challenging to link specific users to transactions (Bahamazava, Nanda, 2022; Kethineni, Cao, 2020; Zimba et al., 2020). Conversely, Zcash operates by obliterating transaction history post-execution (Silfversten et al., 2020). Unlike Bitcoin transactions, which can be monitored on public networks like blockchain.com, tracking transactions involving privacy coins like Monero or Zcash poses significant difficulties (Etto, 2017; Pilinkiene et al., 2022; Reddy et al., 2020).

Darknet activities, as demonstrated, leverage various technologies to enable and conceal illicit transactions. Cybercriminals primarily use

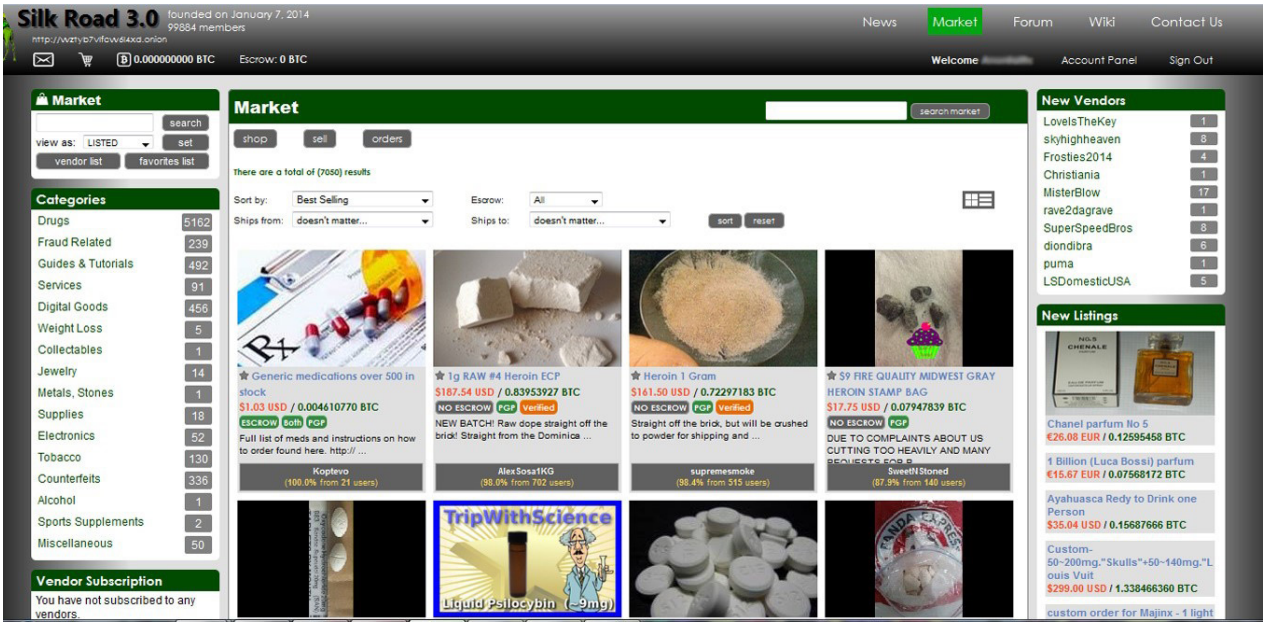

Fig. 3. Screenshot of the Silk Road 3.0 website, a darknet black market website.
Source: Screenshot taken by Nialldawson (2015) from Wikimedia Commons on April 17, 2015.

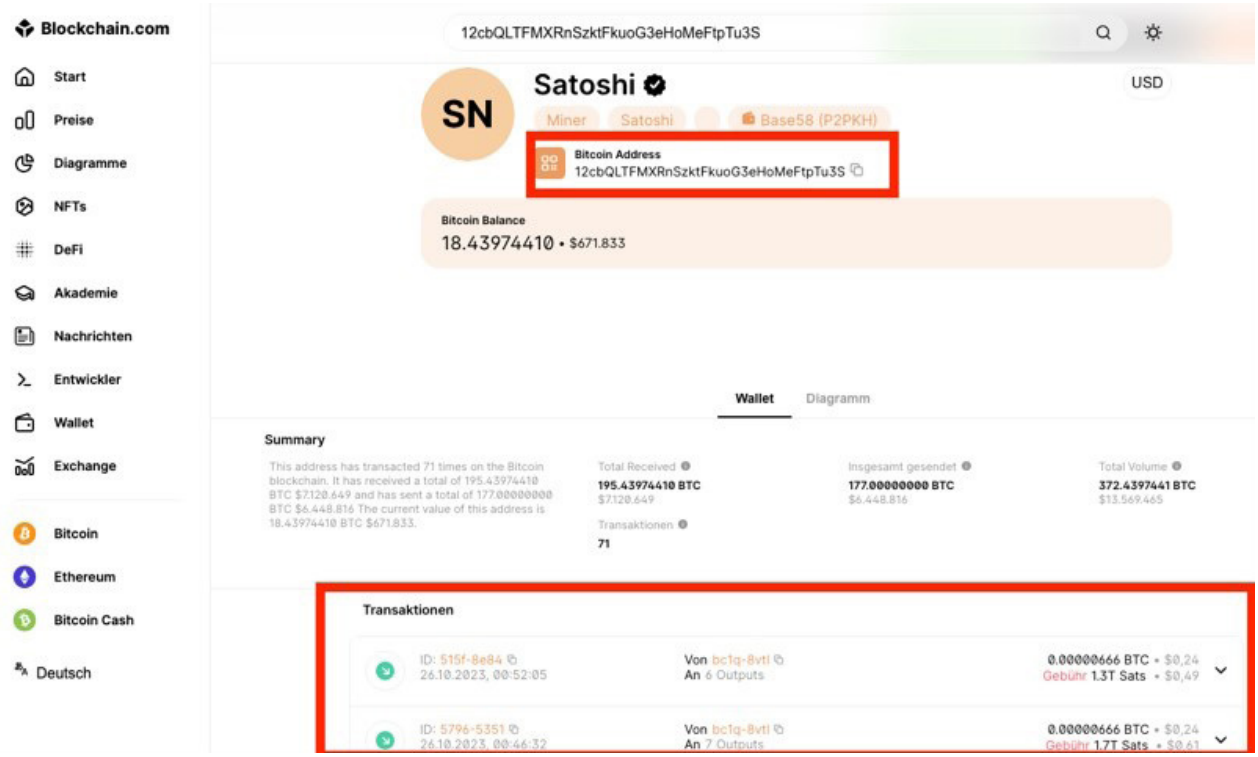

Fig. 4. Visualization of Bitcoin wallet transactions on the https://www.blockchain.com/ website, showcasing the account of Satoshi with a balance of over 18 Bitcoins. The Bitcoin address and transaction details are illustrated.
Source: Screenshot taken by Shobhit Navani on November 10, 2023.

cryptocurrencies which provide the necessary anonymity for these transactions. The Tor network is another critical technology, facilitating anonymous browsing and access to darknet markets, where illegal goods and services are bought and sold. Additionally, mixing and tumbling services are employed to obfuscate transaction trails, making it challenging for law enforcement to trace the origins and destinations of funds. To suppress these activities, enhancing blockchain analytics is crucial (Bajra et al., 2024; Raman et al., 2023). Leveraging machine learning and artificial intelligence (AI) can help detect patterns indicative of illicit transactions and trace these activities across the blockchain. Improved regulation and strict enforcement of know-your-customer (KYC) and anti-money laundering

(AML) procedures at cryptocurrency exchanges can significantly reduce the anonymity that criminals rely on. Collaborations with technology providers are also essential. By partnering with companies that provide internet infrastructure, authorities can monitor and shut down darknet sites more effectively (dos Reis et al., 2024; FinCen, 2024; Nialldawson, 2015). These combined efforts can create a more hostile environment for cybercriminals operating on the darknet.

4.2. Cybercrime in the era of digital advancement

Cybercrime encompasses a broad spectrum of illicit activities committed through the internet or digital networks, constituting a significant threat in the modern era (Dupont, Holt, 2022; Lapuh Bele, 2021; Shinder, Cross, 2008). The allure of cryptocurrencies for both cautious investors and criminal elements is undeniable (Ali, 2021; Barone, Masciandaro, 2019; Dyntu, Dykyi, 2019). Criminal entities perceive cryptocurrencies as ripe targets for exploitation, serving as not only a means of payment but also as tools for money laundering and avenues for launching cyberattacks (Ciphertrace, 2023; Custers et al., 2020; Dyntu, Dykyi, 2019). Regulators increasingly acknowledge the empowerment cryptocurrencies provide to criminal enterprises, paving the way for the emergence of novel cybercrimes.

Cryptocurrencies, notably Bitcoin, reign supreme as the preferred mode of financial exchange on the dark web, facilitating the trade of illicit goods, services, and data integral to cybercriminal operations (Brown, 2016; Caporale et al., 2020; S. Choi et al., 2020). Criminal syndicates extensively leverage Crime-as-a-Service, a form of cloud computing, to perpetrate cybercrimes with alarming efficiency, further fueling the expansion of cybercrime year after year (Gryszczyńska, 2021; Higbee, 2018; Lapuh Bele, 2021). Bitcoin, often associated with cybercrime, remains a focal point due to its intrinsic security vulnerabilities and widespread usage in underground economies. While its pseudo-anonymous nature and global accessibility appeal to money launderers and criminals, it is imperative to discern that Bitcoin's fundamental technology is not inherently nefarious (Kristoufek, 2015; Nakamoto, 2009; Rueckert, 2019). Individuals seeking privacy amid pervasive surveillance systems also utilize cryptocurrencies, highlighting the nuanced landscape in which these technologies operate.

However, combatting organized cybercrime poses formidable challenges, particularly in navigating the intricate technicalities of cryptocurrencies. Digital forensics teams encounter not only sophisticated cybercriminal syndicates but also the complex cryptographic underpinnings of digital currencies, often tipping the scales in favor of cybercriminals (Balaskas, Franqueira, 2018; Cong et al., 2022; Naqvi, 2018; Patsakis et al., 2023). For instance, the US saw a concerning rise in cyber threats in 2022, as revealed by the internet crime report from the Federal Bureau of Investigation (FBI). Over 800,000 complaints related to cybercrime were filed, resulting in total losses surpassing USD 10 billion, significantly surpassing the previous year's total of USD 6.9 billion. This underscores the urgent need to enhance cybersecurity measures and proactive law enforcement efforts to address the escalating cyber threat landscape (FBI, 2022).

Regarding the wide range of technologies used to facilitate this illicit activity. Crime-as-a-Service (CaaS) platforms have emerged as a significant threat, offering illicit services for hire, ranging from hacking services to the distribution of malware. Cryptocurrencies serve as a preferred medium for CaaS transactions due to their inherent anonymity, allowing cybercriminals to conduct financial exchanges without easily traceable identities (Ciphertrace, 2023; Hendrickson, Luther, 2022; Mazambani, 2024). Furthermore, cybercriminals leverage sophisticated hacking tools and exploit kits to infiltrate systems and pilfer sensitive data, exacerbating cybersecurity vulnerabilities (Gohwong, 2019; Interpol, 2020; Patsakis et al., 2023). To effectively combat this cybercrime, the deployment of advanced threat detection systems is imperative. AI-powered cybersecurity solutions are pivotal in this regard, capable of detecting and mitigating threats in real-time. These technologies bolster defenses against sophisticated cyber attacks, providing organizations with proactive security measures (Kutera, 2022; Mazambani, 2024; Volevodz, 2024). Additionally, fostering public-private partnerships is crucial. Collaboration between law enforcement agencies and cybersecurity firms enables the sharing of intelligence and resources, enhancing the collective ability to respond swiftly to cyber threats and criminal activities.

Moreover, comprehensive education initiatives are essential to raise awareness among users and organizations about prevalent cyber threats such as phishing attacks (Cong et al., 2022; Gray et al., 2023; Nazzari, Riccardi, 2024). By educating the public about cybersecurity best practices and emerging threats, individuals and entities can better safeguard themselves against cybercriminal tactics. This multifaceted approach integrates technological advancements with collaborative efforts and educational outreach to fortify defenses against the evolving landscape of cybercrime.

4.3. Crypto Ransomware: emerging threats and economic considerations

The Cybersecurity and Infrastructure Security Agency (CISA) of the US defines malware as any software crafted to illicitly breach IT systems, with the intent to pilfer data, disrupt services, or cause harm to networks (CISA, 2023). Ransomware, a specific type of malware, operates by encrypting targeted data or systems and withholding access until a ransom is paid. Notably, the evolution of ransomware has given rise to a particularly pernicious variant known as crypto ransomware, wherein perpetrators demand payment in cryptocurrency for the release of encrypted data or system access (Brown, 2016; CERT-Bund, 2022; Custers et al., 2020; Gray et al., 2023). This shift to cryptocurrency payments enhances anonymity for cybercriminals and complicates traditional law enforcement efforts to track and apprehend perpetrators.

The rise of crypto ransomware represents a significant cybersecurity challenge, exacerbated by the intricate interplay of social and technical factors within its ecosystem. As noted in a study by L. Connolly and D.S. Wall (2019), the impact of crypto ransomware has become increasingly pronounced in recent years, reflecting the adaptability and sophistication of cybercriminal tactics. The proliferation of cryptocurrency-based extortion schemes underscores the need for robust cybersecurity measures and proactive defense strategies to mitigate the risks posed by ransomware attacks (CISA, 2023; Meland et al., 2020; Muslim et al., 2019).

Examples of crypto ransomware demonstrate the evolving landscape of cyber threats. For instance, Crypto Locker emerged on September 5, 2013, heralding a new era of ransomware. This malicious software encrypted files on victims' systems, withholding decryption keys until a ransom was paid, typically within a strict 72-hour window. Payment methods often included Bitcoin or MoneyPak, adding layers of anonymity for cybercriminals (Liao et al., 2016). A significant blow to the distribution of Crypto Locker came in June 2014 with Operation Tovar. This international effort, spearheaded by the US Department of Justice (DOJ), CISA, the FBI, Europol, and other law enforcement agencies, targeted the Game Over Zeus botnet, a primary distributor of Crypto Locker. The operation's success dealt a severe blow to the prevalence of Crypto Locker and disrupted its criminal infrastructure (Hernandez-Castro et al., 2020).

Moreover, an economic model proposed by Hernandez-Castro et al. (Hernandez-Castro et al., 2020) sheds light on the nuanced dynamics of crypto ransomware payments. This model considers the victim's willingness to pay, with cybercriminals adjusting ransom demands based on the perceived value and characteristics of targeted victims. This price discrimination strategy aims to maximize profits by tailoring ransom amounts to victims' financial capabilities. Given the escalating threat posed by crypto ransomware, organizations and individuals must prioritize prevention and preparedness efforts (Brown, 2016; Gohwong, 2019; Meland et al., 2020; Muslim et al., 2019). This includes implementing comprehensive cybersecurity protocols, such as regular data backups, network segmentation, and user training to recognize and respond to phishing attempts. Additionally, maintaining up-to-date software patches and employing advanced threat detection technologies can help mitigate the risk of ransomware infections (Fosso Wamba et al., 2020; Gray et al., 2023; Meland et al., 2020; Paquet-Clouston et al., 2019). By adopting a proactive approach to cybersecurity, stakeholders can bolster their resilience against ransomware threats and safeguard critical data and systems from exploitation. As such, understanding the intricacies of crypto ransomware payments is crucial in developing effective strategies for prevention and response in the face of evolving cyber threats.

Crypto ransomware represents a significant cybersecurity challenge, where attackers use malware to encrypt data and demand ransom payments in cryptocurrency. Ransomware attacks typically involve anonymous communication channels like Telegram for negotiating ransoms. To mitigate the risk of crypto ransomware, regular data backups are essential (Gómez-Hernández & García-Teodoro, 2024; Patsakis et al., 2023; Sherer et al., 2016; Team, 2024). Network segmentation is another critical measure, as it helps to isolate critical systems and prevent the spread of ransomware within an organization. Developing and regularly updating incident response plans is also crucial, enabling organizations to respond quickly and effectively to ransomware attacks, minimizing the impact on operations. The best prevention is not to have crypto ransomware installed persons and organization devices. To prevent this, it involves a multi-faceted approach: regular software updates and patching, firewalls and endpoint protection, encryption of sensitive data both at rest and in transit, multi-factor authentication, regular audits and assessments, regularly updating access control, utilization of AI and machine learning to detect anomalies, and zero trust architecture. By integrating these measures, one can create a robust defense against hacking attempts via crypto ransomware (CERT-Bund, 2022; Gómez-Hernández, García-Teodoro, 2024; Gray et al., 2023; Nazzari, 2023; Patsakis et al., 2023; Team, 2024).

4.4. Organized crime: utilization of cryptocurrency

Following a comprehensive review of the literature, organized crimes were classified into four prevalent categories characterized by the widespread utilization of cryptocurrency. These categories encompass drug trafficking, terrorism, money laundering, and the distribution of CSAM.

4.4.1. Drug trafficking

Drug trafficking involves the illicit production, transportation, and distribution of controlled substances, encompassing narcotics, hallucinogens, stimulants, and other banned drugs (Bahamazava, Nanda, 2022; Bertola, 2020; Holt et al., 2023). The World Drug Report 2020 by the United Nations Office on Drugs and Crime (UNODC) emphasizes that drug transactions, including new psychoactive substances, occur across both the open internet and the darknet. Notably, purchases made on various darknet marketplaces are frequently settled using cryptocurrencies, particularly Bitcoin, which are also prevalent in legitimate transactions on the open web. As previously highlighted, Silk Road, a notorious platform operating on the dark web, gained infamy for its vast array of illicit products, prominently featuring illegal drugs (Figure 3). In 2022, marijuana emerged as the top-selling drug on Silk Road, with transactions exceeding USD 46 million. Cocaine closely followed with 82,582 transactions totaling USD 17.4 million, while heroin sales reached an estimated USD 8.9 million. Additional sales of popular drugs such as methamphetamine, lysergic acid diethylamide, ecstasy, and various narcotics, including oxycodone and fentanyl, collectively generated around USD 19.2 million (Alfieri, 2022)..

In a significant development, the DOJ announced the seizure of AlphaBay, the largest criminal marketplace on the internet, after operating for over two years on the dark web. AlphaBay facilitated the sale of a wide array of illegal goods, including deadly drugs, fraudulent identification documents, malware, firearms, and toxic chemicals worldwide. The coordinated international effort to dismantle AlphaBay involved law enforcement agencies from Thailand, the Netherlands, Lithuania, Canada, the UK, and France, along with the European law enforcement agency Europol. Alexandre Cazes, also known as Alpha02 and Admin, a Canadian citizen residing in Thailand and the alleged creator and administrator of AlphaBay, was apprehended by Thai authorities on behalf of the US. Tragically, Cazes reportedly took his own life while in custody in Thailand on July 12, 2017, following his arrest on July 5, 2017 (DOJ, 2017).

To suppress drug trafficking facilitated by cryptocurrencies, enhanced surveillance of darknet markets is necessary. Using advanced analytics and AI, authorities can monitor and infiltrate these markets more effectively (Bertola, 2020; Kabra, Gori, 2023; Raman et al., 2023). Blockchain monitoring tools can track cryptocurrency transactions related to drug trafficking, providing valuable leads for law enforcement. Additionally, strengthening international cooperation is crucial. By collaborating with global law enforcement agencies, coordinated efforts can be made to dismantle drug trafficking networks and bring perpetrators to justice.

4.4.2. Terrorism

Interconnections between terrorism financing, money laundering, cybercrime, and traditional criminal activities have been well-documented (Irwin & Slay, 2010). In 2015, a DOJ press release highlighted the case of Ali Shujri Amin, a 17-year-old who pleaded guilty to aiding the Islamic State of Iraq and Syria (ISIS), a militant terrorist group, through social media platforms like X. Amin, under the aliases of "Amreeki" and "American Witness," advocated for Bitcoin as an anonymous, decentralized, and encrypted means of transferring funds to ISIS, making tracking transactions challenging (DOJ, 2015).

Similarly, in 2017, Indonesia's financial intelligence unit, Pusat Pelaporan dan Analisis Transaksi Keuangan, reported that ISIS was utilizing online payment services like PayPal and Bitcoin to finance domestic operations, with Bahrun Naim, the orchestrator of the 2016 Jakarta attacks, allegedly utilizing these services (Rizzo, 2017). Additionally, in January 2018, the al-Qaeda-linked webzine al-Haqiqa published an article instructing readers on using cryptocurrencies for terrorism financing (Kfir, 2020).

To combat terrorism financing via the dark web and cryptocurrencies, advanced technological and intelligence tools are imperative. The inherent anonymity of transactions and users presents a significant challenge, necessitating the development of pattern recognition algorithms, behavioral maps, rule bases, and predictive models (Andronova et al., 2020; Dyntu, Dykyj, 2021; Ilijevski et al., 2023). It is essential to establish systems capable of autonomously identifying potential instances of money laundering and terrorist financing, enhancing proactive detection and intervention (Dyntu, Dykyj, 2021; Kfir, 2020; Rubasundram, 2019; Wang, Zhu, 2021). Moreover, terrorist organizations have increasingly turned to cryptocurrencies to finance their activities, taking advantage of the anonymity provided by these digital assets. Encrypted

communication tools like Telegram and Signal are also used to coordinate activities and transfer funds anonymously. This combination of technologies presents significant challenges for counter-terrorism efforts.

To combat terrorism financing via cryptocurrencies, establishing dedicated financial intelligence units is imperative. These units can monitor and analyze suspicious cryptocurrency transactions, identifying potential terrorist financing activities. Investing in decryption technologies can also help law enforcement agencies intercept and decode encrypted communications, revealing the networks and plans of terrorist organizations. Implementing global standards for cryptocurrency regulation is another critical step. By ensuring consistent enforcement against terrorist financing, the international community can prevent the misuse of digital currencies for terrorist activities. As such, banning crypto mixers, such as Sindbad.io, removes a critical tool used by terrorists to anonymize and move funds, enhancing the traceability of transactions and disrupting financial networks that support terrorism (Dion-Schwarz et al., 2019; Kfir, 2020; Rubasundram, 2019; Teichmann, Falker, 2024). By increasing transparency, deterring illicit use of cryptocurrencies, enhancing law enforcement capabilities, and fostering international cooperation, such bans play a crucial role in curtailing terrorism. This combined approach makes it more difficult for terrorist organizations to finance their operations, thereby contributing to global security efforts.

4.4.3. Money laundering

Money laundering through cryptocurrencies, particularly Bitcoin, involves several distinct stages. Bitcoin is often used for such purposes, and details about these methods are provided in supplementary material (see Supplementary Data—S2). One common method is to engage with a Bitcoin trader (Custers et al., 2020; Otabek, Choi, 2024). In this approach, the trader facilitates face-to-face exchanges, where Bitcoins are traded for fiat currency. During these transactions, both parties bring their devices, and the trader immediately exchanges Bitcoins for the agreed-upon fiat currency, either in cash or via online banking. This method typically involves either a cybercriminal or an intermediary as the client, and due to the risks and complexities involved, transaction fees are generally high. Another method involves using online money laundering services, which offer an additional channel for converting illicit proceeds.

These clandestine online entities, often accessible through the dark web, offer to launder funds received in Bitcoin. After transferring the Bitcoins to such a service, clients can choose to receive the funds through legitimate online financial payment services like PayPal, Western Union, MoneyGram, or prepaid cards (Brown, 2016; Nazzari, 2023; Sicignano, 2021; Teichmann, Falker, 2020b; Wronka, 2022a, 2022b; Zavoli, 2022). Alternatively, the value of the virtual currencies can be returned via prepaid credit cards, which can then be used to withdraw cash from regular ATMs. Also, Bitcoins can be spent directly at various outlets, including online casinos, hosting services, and e-commerce platforms. Furthermore, an increasing number of brick-and-mortar establishments, such as pubs, restaurants, and shops, now accept Bitcoin as a form of payment. This provides cybercriminals with the opportunity to easily spend their laundered and anonymized Bitcoins on goods and services.

To suppress money laundering, enhancing blockchain forensics capabilities is essential (Agarwal et al., 2024; Alqahtany, Syed, 2024; Soni, 2024; Thamizhisai et al., 2024). Advanced tools and techniques can trace the flow of funds across the blockchain, identifying suspicious patterns and transactions. Enforcing strict AML policies across all cryptocurrency exchanges can also reduce the anonymity that criminals rely on (Florea, Nitu, 2020; Rieckmann, Stuchtey, 2023; Teichmann, Falker, 2020b). Additionally, developing a centralized crypto wallet infrastructure, where wallets are linked to verified identities, can simplify tracking funds and deter unauthorized transactions. These measures can significantly disrupt money laundering activities facilitated by cryptocurrencies.

4.4.4. CSAM

The availability of CSAM remains a critical issue, with perpetrators utilizing various platforms, including crypto markets, peer-to-peer networks, and even the open internet (ICE, 2020; Sayid, 2023). The UNODC (2020) report highlights the allure of the dark web for CSAM distribution due to its perceived anonymity and resilience to censorship. Dismantling this illicit content is particularly challenging as it is often replicated across numerous platforms, making it difficult to eradicate completely (Celiksoy, Schwarz, 2023; Nouwen, 2017). Regrettably, dating back to the COVID-19 pandemic, the issue worsened, with reports indicating a significant increase in CSAM websites emerging during lockdown periods (Botha et al., 2023; Gryszczyńska, 2021; Riahi et al., 2024; UNODC, 2020). Currently, a substantial portion of data shared on the dark web is believed to be CSAM, primarily in the form of images and videos. Certain sites reportedly boast collections in the terabyte range, equivalent to roughly 80 days' worth of video or nearly 1 million digital photographs (Nouwen,

2017; Sayid, 2023; UNODC, 2020). Overall, darknet activity and user bases, particularly on platforms like Tor, are experiencing consistent growth (Zimba et al., 2020). While not all darknet activity is illegal, it is concerning that organized criminal elements within this space are continuously developing their capabilities, security measures, and business strategies.

The anonymity offered by cryptocurrencies, as highlighted by S. Broadhead (2018), has facilitated the sale of child pornography on the dark web, not only impacting adults but also harming children directly exploited in the creation of such content. The nature of this material and its devastating consequences for victims solidify the dark market as a significant threat. CSAM remains readily available through crypto markets, peer-to-peer networks, and even the open internet.

According to a press release, a Dutch national Michael Rahim Mohammed, aka Mr. Dark, 32, was indicted by a federal grand jury in the District of Columbia for his operation of Dark Scandals, a site on both the darknet and open internet that featured violent rape videos and depictions of child pornography (ICE, 2020). The indictment alleges Mohammed, who resides in the Netherlands, operated the Dark Scandals websites that hosted and distributed the material featuring nonconsensual and violent sexual abuse. Dark Scandals began operating in or about 2012 and boasted over 2,000 videos and images and advertised "real blackmail, rape, and forced videos of girls" all around the world. Dark Scandals offered users two ways to access this illicit and obscene content, which was delivered in "packs" via email to customers to download. Users could either pay for the video packs using cryptocurrency, such as Bitcoin, or upload new videos to add to the content of the Dark Scandals websites. Law enforcement was able to trace payments of Bitcoin and Ethereum to the Dark Scandals websites by following the flow of funds on the blockchain. The 303 virtual currency accounts identified were allegedly used by customers across the world to fund the websites and promote the exploitation of children and other vulnerable victims (ICE, 2020).

The exploitation and abuse of children depicted in CSAM represents a profound violation of their fundamental rights, resulting in enduring physical and emotional trauma (Draper, 2022; Jung, 2022; Maxwell, 2022). Addressing the role of cryptocurrency in facilitating these crimes is paramount, necessitating a multi-faceted approach to combat this atrocity. Effective regulation of cryptocurrency is crucial in preventing its misuse and protecting children from such unimaginable harm (ICE, 2020; Maxwell, 2022; Nouwen, 2017; Sayid, 2023). To combat CSAM, it is imperative to deploy AI-based content detection systems capable of identifying and removing CSAM from the internet, thereby significantly reducing its availability (Singh, Nambiar, 2024). Establishing global task forces focused on dismantling CSAM networks can strengthen international cooperation and coordination in these efforts. Additionally, leveraging blockchain analysis tools to trace financial transactions associated with CSAM can disrupt the financial networks that support this illicit activity (Balaskas, Franqueira, 2018; Bayramova et al., 2021; Patsakis et al., 2023). These proactive measures are essential steps towards dismantling the infrastructure behind CSAM distribution and mitigating the exploitation of children.

4.5. Regulatory measures

Countries worldwide have adopted various strategies to address the challenges posed by cryptocurrency through regulatory means. However, the lack of a centralized global regulatory authority and the inherent anonymity of cryptocurrency users complicate the development of comprehensive regulatory frameworks. An analysis of the literature reveals significant efforts by nations like the US, China, and India in formulating regulatory strategies tailored to their larger populations. Additionally, several European countries, such as Poland and Switzerland, have enacted robust regulatory measures to address issues related to cryptocurrency and combat cybercrime risks. A detailed examination of these countries' regulatory approaches is provided as supplementary material (see Supplementary Data—S3). Furthermore, countries such as Australia, Canada, Japan, Singapore, South Korea, and the UK have also implemented noteworthy regulatory measures to govern cryptocurrency operations, though these are not elaborated on further.

4.6. Future directions for technology and regulation in cryptocurrency

Future directions in technology and regulation for cryptocurrencies hold significant promise in advancing both security and usability while addressing the persistent risks posed by cybercrime. Technological advancements are poised to play a crucial role, particularly through the development of sophisticated blockchain analytics tools powered by machine learning and AI (Singh, Nambiar, 2024). These tools enhance the capabilities of law enforcement and regulatory agencies by detecting fraudulent activities, tracing illicit transactions, and predicting security breaches. Such advancements

are pivotal in fortifying the cryptocurrency ecosystem against increasingly sophisticated cyber threats (Florea, Nitu, 2020; Reddy, Minaar, 2018; Trozze et al., 2022).

Privacy-preserving technologies, such as zero-knowledge proofs and homomorphic encryption, offer another layer of security by enabling transaction verification without compromising sensitive information. This innovation strikes a balance between user privacy and regulatory compliance, ensuring that transactions remain secure while adhering to regulatory standards (Corbet et al., 2020). Moreover, formal verification methods for smart contracts are critical in eliminating vulnerabilities and mitigating exploitation risks within decentralized. By ensuring smart contracts are free from bugs, these methods enhance transactional security and build trust among participants in decentralized ecosystems applications (Al-Zubaidie, Jebbar, 2024; Chand et al., 2024; Kavitha, Golden, 2024; Zheng, 2024). Concurrently, decentralized identity frameworks provide robust solutions for identity verification while preserving user anonymity. These frameworks facilitate effective implementation of KYC and AML measures, bolstering overall security protocols and reducing fraudulent activities (ICE, 2020; Sayid, 2023).

Regulatory improvements are equally essential in creating a resilient and secure environment for cryptocurrency transactions. Enhanced international cooperation among regulatory bodies is crucial for harmonizing cryptocurrency regulations and closing jurisdictional loopholes that cybercriminals exploit. A unified approach to enforcement globally strengthens efforts to combat cryptocurrency-related crimes effectively. Clear and standardized regulatory frameworks are indispensable, providing transparency and certainty for cryptocurrency exchanges, wallet providers, and other entities (Ahuja et al., 2021; Kavitha, Golden, 2024; Kayani, Hasan, 2024). These frameworks outline specific guidelines that ensure compliance with legal standards, fostering a stable regulatory environment conducive to innovation and investment.

Stricter enforcement of KYC and AML regulations across all cryptocurrency platforms, coupled with advanced identification technologies like biometrics, holds the potential to significantly disrupt criminal activities such as money laundering (Goldbarsht, 2024; Leuprecht et al., 2022; Nazzari, Riccardi, 2024; Zavoli, 2022). By enhancing participant accountability and reducing anonymity risks, these measures bolster regulatory oversight and control over fund movements within the cryptocurrency ecosystem. Implementing a centralized crypto wallet infrastructure linked to verified identities further simplifies KYC and AML procedures, streamlining fund tracking and deterring unauthorized transactions. In addition to regulatory frameworks and technological advancements, fostering collaboration through public-private partnerships is essential. These partnerships facilitate the exchange of information and resources crucial for combating cybercrime effectively. Comprehensive educational initiatives play a pivotal role in raising awareness among users and businesses about cybersecurity best practices, thereby reducing vulnerabilities to scams and cyber threats (Del Monaco, 2020; Higbee, 2018).

In all, prioritizing technological advancements and regulatory enhancements is crucial for fostering the widespread adoption of cryptocurrencies while safeguarding against evolving cyber threats. These advancements and improvements will not only help in building a secure, transparent, and resilient cryptocurrency ecosystem but also in adapting to the rapidly changing landscape of digital finance. Continuous adaptation and collaborative efforts among stakeholders are essential to stay ahead of cybercriminals and ensure the integrity of the cryptocurrency environment. Embracing these future directions will create a robust foundation for the sustained growth and acceptance of cryptocurrencies on a global scale. For a comprehensive analysis of the benefits and limitations of existing solutions and mechanisms, refer to the supplementary material provided (see Supplementary Data—S4).

5. Conclusions

In this comprehensive review paper, the intricate landscape of cryptocurrency regulation across various countries has been thoroughly examined, providing insights into the diverse approaches taken by governments to address the challenges and opportunities presented by cryptocurrencies. The analysis conducted sheds light on the complexity and evolution of cryptocurrency regulation, influenced by factors such as technological advancements, market dynamics, and geopolitical considerations. While some countries embrace cryptocurrencies as innovative financial instruments, others adopt cautious approaches, wary of potential risks. Balancing innovation with risk mitigation remains a central challenge for policymakers worldwide.

Furthermore, the exploration of the relationship between cybercrime and cryptocurrency has been meticulous, employing a systematic categorization approach to understand their interconnectedness. By organizing crimes into specific categories, insights into the complex dynamics at play within this realm have been offered, providing valuable perspectives

on key issues, trends, and policy considerations shaping this rapidly evolving domain. From financial security to identity theft and fraud, elucidation of how cryptocurrencies intersect with different forms of illicit behavior has been provided.

The review underscores the necessity for adaptive and agile approaches to combatting cyber threats in the digital age. As technological advancements reshape the cybercrime landscape, it becomes imperative for stakeholders to remain vigilant and proactive in addressing emerging challenges. Staying abreast of evolving trends and employing innovative strategies is essential to better safeguard individuals and organizations against the risks posed by cryptocurrency-related crime.

Looking ahead, the regulatory landscape for cryptocurrencies will continue to evolve in response to emerging technologies and changing market dynamics. Collaborative efforts between governments, regulatory bodies, industry stakeholders, and the broader community will be paramount in navigating this complex terrain and unlocking the full potential of cryptocurrencies as a transformative force in the global economy. The review contributes to ongoing discussions and endeavors to develop more effective and sustainable approaches to addressing these pressing issues, ensuring a safer and more secure digital future for all.

Data availability statement

The supplementary material for this study (Supplementary Data—S1, S2, S3, and S4) is available in the Figshare online repository. The materials can be accessed via the following repository link: https://doi.org/10.6084/m9.figshare.27075646.v1

References

Adam I.O., Dzang Alhassan M., 2020, Bridging the Global Digital Divide Through Digital Inclusion: The Role of ICT Access and ICT Use, *Transforming Government: People, Process and Policy,* 15(4), Article 4. doi: 10.1108/TG-06-2020-0114

Agarwal U., Rishiwal V., Tanwar S., Yadav M., 2024, Blockchain and Crypto Forensics: Investigating Crypto Frauds, *International Journal of Network Management,* 34(2), e2255. doi: 10.1002/nem.2255

Aggarwal S., Jaiswal U., 2011, Kryptos + Graphein = Cryptography, *Science and Technology*, 3(9), Article 9.

Ahuja A., Ribeiro V.J., Pal R., 2021, *A Regulatory System for Optimal Legal Transaction Throughput in Cryptocurrency Blockchains* (arXiv:2103.16216; Issue arXiv:2103.16216). arXiv. http://arxiv.org/abs/2103.16216

Aitken, F. (2020). *Trusting Cryptocurrencies: Aspects of the Common Law and Equity Affecting Cryptocurrency Owners* [University of Otago]. https://www.otago.ac.nz/__data/assets/pdf_file/0015/331530/trusting-cryptocurrencies-aspects-of-the-common-law-and-equity-affecting-cryptocurrency-owners-828533.pdf (accessed 1 July 2024)

Alfieri C., 2022, Cryptocurrency and National Security, *International Journal on Criminology,* 9(1), Article 1. doi: 10.18278/IJC.9.1.3

Ali A., 2021, *Cryptocurrencies Security and Dispute Resolution* [University of Cumberlands], https://www.researchgate.net/publication/351334217_Cryptocurrencies_security_and_dispute_resolution (accessed 1 July 2024)

Alqahtany S.S., Syed T.A., 2024, ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management, *Information*, 15(2), Article 2. doi: 10.3390/info15020109

Alvarez F., Argente D., Van Patten D., 2022, *Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador* (4094160), SSRN Scholarly Paper. doi: 10.2139/ssrn.4094160

Al-Zubaidie M., Jebbar W., 2024, Transaction Security and Management of Blockchain-Based Smart Contracts in E-Banking-Employing Microsegmentation and Yellow Saddle Goatfish, *Mesopotamian Journal of CyberSecurity,* 4(2), Article 2. doi: 10.58496/MJCS/2024/005

Ambrus I., Mezei K., 2022, The New Hungarian Legislation on Money Laundering and the Current Challenges of Cryptocurrencies, *Danube Publishing*, 13(4), Article 4. doi: 10.2478/danb-2022-0016

Andres Rodriguez-Nieto J., Eremina K., 2023, *The Effects of COVID-19 and the Increasing Relationship Between Individual Investor Sentiment, Cryptocurrencies, and the US Market (*4729404), SSRN Scholarly Paper. https://papers.ssrn.com/abstract=4729404 (accessed 1 July 2024)

Andronova I., Gusakov N., Peoples' Friendship University of Russia (RUDN University), Zavyalova E., 2020, Terrorism Financing: New Challenges for International Security. *International Organisations Research Journal,* 15(1), Article 1. doi: 10.17323/1996-7845-2020-01-05

Auer R., Tercero-Lucas D., 2022, Distrust or Speculation? The Socioeconomic Drivers of US Cryptocurrency Investments. *Journal of Financial Stability*, 62, 101066. doi: 10.1016/j.jfs.2022.101066

Australian Home Affairs, 2022, *Exploring Cryptocurrency,* Cyber Security Industry Advisory Committee.

Badawi E., Jourdan G.-V., 2020, Cryptocurrencies Emerging Threats and Defensive Mechanisms: A Systematic Literature Review, *IEEE Access,* 8, 200021–200037. doi: 10.1109/ACCESS.2020.3034816

BaFin, 2018, *Money Laundering Act. Federal Financial Supervisory Authority.* https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html (accessed 1 July 2024)

Bahamazava K., Nanda R., 2022, The Shift of Darknet Illegal Drug Trade Preferences in Cryptocurrency: The Question of Traceability and Deterrence, *Forensic Science International: Digital Investigation*, 40, 301377. doi: 10.1016/j.fsidi.2022.301377

Bajra U., Rogova P.D.E., Avdiaj P.D.S., 2024, *Cryptocurrency Blockchain and Its Carbon Footprint: Anticipating Future Challenges* (4735982). SSRN Scholarly Paper. doi: 10.2139/ssrn.4735982

Balaskas A., Franqueira V.N.L., 2018, Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges, *2018 International Conference on Cyber Security and Protection*

of Digital Services (Cyber Security), 1–8. doi: 10.1109/CyberSecPODS.2018.8560672

Barone R., Masciandaro D., 2019, Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques, *European Journal of Law and Economics,* 47(2), Article 2. doi: 10.1007/s10657-019-09609-6

Bartoletti M., Lande S., Loddo A., Pompianu L., Serusi S., 2021, Cryptocurrency Scams: Analysis and Perspectives, *IEEE Access,* 9, 148353–148373. doi: 10.1109/ACCESS.2021.3123894

Bayramova A., Edwards D.J., Roberts C., 2021, The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime, *Buildings*, 11(7), Article 7. doi: 10.3390/buildings11070283

Bertola F., 2020, Drug Trafficking on Darkmarkets: How Cryptomarkets are Changing Drug Global Trade and the Role of Organized Crime, *American Journal of Qualitative Research,* 4(2), Article 2. doi: 10.29333/ajqr/8243

Bhaskar V., Linacre R., Machin S., 2019, The Economic Functioning of Online Drugs Markets, *Journal of Economic Behavior & Organization,* 159, 426–441. doi: 10.1016/j.jebo.2017.07.022

Biswas R., 2018, Emerging Markets Megatrends, *Springer, Cham*. doi: 10.1007/978-3-319-78123-5

Blasco N.J., Fett N.A., 2019, Blockchain Security: Situational Crime Prevention Theory and Distributed Cyber Systems, *The International Journal of Cybersecurity Intelligence and Cybercrime*, 2(2), Article 2. doi: 10.52306/02020419tegr1675

Boehm F., Pesch P., 2014, Bitcoin: A First Legal Analysis, [in:] R. Böhme, M. Brenner, T. Moore, M. Smith (Eds.), *Financial Cryptography and Data Security.* Springer, Cham, 43–54. doi: 10.1007/978-3-662-44774-1_4

Böhme R., Christin N., Edelman B., Moore T., 2015, Bitcoin: Economics, Technology, and Governance, *Journal of Economic Perspectives,* 29(2), Article 2. doi: 10.1257/jep.29.2.213

Bokovnya A.Y., Shutova A.A., Zhukova T.G., Ryabova L.V., 2020, Legal Measures for Crimes in the Field of Cryptocurrency Billing, *Utopia Y Praxis Latinoamericana,* 25(Extra7), Article Extra 7. doi: 10.5281/zenodo.4009713

Botha J.G., Botha D., Leenen L., 2023, An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020–2022, *International Conference on Cyber Warfare and Security,* 18(1), Article 1. doi: 10.34190/iccws.18.1.1087

Bray J.D., 2016, Anonymity, Cybercrime, and the Connection to Cryptocurrency, *Online Theses and Dissertations,* 344, Article 344.

Broadhead S., 2018, The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments, *Computer Law & Security Review,* 34(6), Article 6. doi: 10.1016/j.clsr.2018.08.005

Brown S.D., 2016,. Cryptocurrency and Criminality, *The Police Journal: Theory, Practice and Principles,* 89(4), Article 4. doi: 10.1177/0032258x16658927

Butler S., 2019, Criminal Use of Cryptocurrencies: A Great New Threat or Is Cash Still King?, *Journal of Cyber Policy,* 4(3), Article 3. doi: 10.1080/23738871.2019.1680720

Caporale G.M., Kang W.-Y., Spagnolo F., Spagnolo N., 2020, *Cyber-Attacks and Cryptocurrencies* (Working Paper 8124; Issue 8124), CESifo Working Paper. https://www.econstor.eu/handle/10419/216520 (accessed 1 July 2024)

Celiksoy E., Schwarz K., 2023, *Investigation into Financial Transactions Used in the Online Sexual Exploitation of Children*, University of Nottingham, Nottingham.

CERT-Bund, 2022, Ransomware Bedrohungslage (Eng. Ransomware threat), *Bundesamt für Sicherheit in der Informationstechnik.*

CFTC, 2017, *CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products*, Commodities Futures Trading Commission, https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/bitcoin_factsheet120117.pdf (accessed 1 July 2024)

Chand P., G. M., Sai B., D. B., G L., 2024, *Blockchain Security: Work on Securing Blockchain Networks and Smart Contracts* (SSRN Scholarly Paper 4751504), https://papers.ssrn.com/abstract=4751504 (accessed 1 July 2024)

Chen P., 2023, The Relationship Between Blockchain and Government Regulation and Governance: The Distinctions Between Different Countries, *Applied and Computational Engineering,* 5(1), Article 1. doi: 10.54254/2755-2721/5/20230685

Cherniei V., Cherniavskyi S., Babanina V., Tykho O., 2021, Criminal Liability for Cryptocurrency Transactions: Global Experience, *European Journal of Sustainable Development,* 10(4), Article 4. doi: 10.14207/ejsd.2021.v10n4p304

Chertoff M., Simon T., 2015, The Impact of the Dark Web on Internet Governance and Cyber Security, *Global Commission on Internet Govrnance*, 6, Article 6.

Chimienti M.T., Kochanska U., Pinna A., 2019, Understanding the Crypto-Asset Phenomenon, Its Risks and Measurement Issues, *Economic Bulletin*, 5, 1–23. doi: 10.2866/429865

Choi S., Choi K.-S., Sungu-Eryilmaz Y., Park H.-K., 2020, Illegal Gambling and Its Operation Via the Darknet and Bitcoin: An Application of Routine Activity Theory, *The International Journal of Cybersecurity Intelligence and Cybercrime,* 3(1), Article 1. doi: 10.52306/03010220htli7653

Choi S., Parti K., 2022, Understanding the Challenges of Cryptography-Related Cybercrime and Its Investigation, *International Journal of Cybersecurity Intelligence & Cybercrime*, 5(2), Article 2. doi: 10.52306/2578-3289.1134

Choi T., Shorubalko I., Gustavsson S., Schön S., Ensslin K., 2009, Correlated Counting of Single Electrons in a Nanowire Double Quantum Dot, *New Journal of Physics,* 11(1), Article 1. doi: 10.1088/1367-2630/11/1/013005

Chuan T., O'Leary R.R., 2021, *China's Bitcoin Exchanges Receive Shutdown Orders and Closure Timeline* [CoinDesk], https://www.coindesk.com/markets/2017/09/15/chinas-bitcoin-exchanges-receive-shutdown-orders-and-closure-timeline/ (accessed 1 July 2024)

Ciphertrace, 2023, *Crypto Crimes & Anti-Money Laundering Report* 2023, Ciphertrace, https://ciphertrace.com/crime-and-anti-money-laundering-report-march-2023/ (accessed 1 July 2024)

CISA, 2023, *Malware, Phishing, and Ransomware* [Cybersecurity and Infrastructure Security Agency], https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware (accessed 1 July 2024)

Clements R., 2021, *Emerging Canadian Crypto-Asset Jurisdictional Uncertainties and Regulatory Gaps* (3891809), SSRN Scholarly Paper. https://papers.ssrn.com/abstract=3891809 (accessed 1 July 2024)

Collins J., 2022, *Crypto, Crime and Control,* Global Initiative Against Transnational Organized Crime, Geneva.

Cong L.W., Harvey C.R., Rabetti D., Wu Z.-Y., 2022, *An Anatomy of Crypto-Enabled Cybercrimes* (4188661; Issue 4188661). SSRN Scholarly Paper. doi: 10.2139/ssrn.4188661

Connolly L., Wall D.S., 2019, The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising

Countermeasures, *Computers & Security,* 87, 101568. doi: 10.1016/j.cose.2019.101568

Conventus Law, 2021, Financial Crimes Compliance For Cryptocurrency: Why Can't We All Agree? *Conventus Law,* https://conventuslaw.com/report/financial-crimes-compliance-for-cryptocurrency-why/ (accessed 1 July 2024)

Corbet S., Cumming D.J., Lucey B.M., Peat M., Vigne S.A., 2020, The Destabilising Effects of Cryptocurrency Cybercriminality, *Economics Letters,* 191, 108741. doi: 10.1016/j.econlet.2019.108741

Courtois N.T., 2014, *Crypto Currencies and Bitcoin*, UCL, http://www.nicolascourtois.com/bitcoin/paycoin_may_2014.pdf (accessed 1 July 2024)

Critien J.V., Gatt A., Ellul J., 2022, Bitcoin Price Change and Trend Prediction Through Twitter Sentiment and Data Volume, *Financial Innovation,* 8(1), Article 1. doi: 10.1186/s40854-022-00352-7

Custers B., Oerlemans J.J., Pool R., 2020, Laundering the Profits of Ransomware; Money Laundering Methods for Vouchers and Cryptocurrencies, *European Journal of Crime, Criminal Law and Criminal Justice,* 28(2), Article 2. doi: 10.1163/15718174-02802002

Davies G., 2020, Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers, *The Journal of Criminal Law,* 84(5), Article 5. doi: 10.1177/0022018320952557

Del Monaco S., 2020, Money Mules and Tumblers Money Laundering During the Cryptocurrency Era: Money Laundering During the Cryptocurrency Era, Ricerche Giuridiche, 2, Article 2. doi: 10.30687/Rg/2281-6100/2022/01/004

Dion-Schwarz C., Manheim D., Johnston P.B., 2019, T*errorist Use of Cryptocurrencies*, Rand Corporation, Santa Monica, Calif.

DOJ, 2015, *Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL* [United States Department of Justice]. https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil (accessed 1 July 2024)

DOJ, 2017, *Alphabay, the Largest Online "Dark Market," Shut Down* [United States Department of Justice]. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down (accessed 1 July 2024)

dos Reis E.F., Teytelboym A., ElBahrawy A., De Loizaga I., Baronchelli A., 2024, Identifying Key Players in Dark Web Marketplaces Through Bitcoin Transaction Networks, *Scientific Reports,* 14(1), Article 1. doi: 10.1038/s41598-023-50409-5

Draper L., 2022, Protecting Children in the Age of End-to-End Encryption, Joint PIJIP/TLS Research Paper Series. https://digitalcommons.wcl.american.edu/research/80 (accessed 1 July 2024)

Dudani S., Baggili I., Raymond D., Marchany R., 2023, The Current State of Cryptocurrency Forensics, *Forensic Science International: Digital Investigation,* 46, 301576. doi: 10.1016/j.fsidi.2023.301576

Dupont B., Holt T., 2022, The Human Factor of Cybercrime, *Social Science Computer Review,* 40(4), Article 4. doi: 10.1177/08944393211011584

Dupuis D., Gleason K., 2020, Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic, *Journal of Financial Crime,* 28(1), Article 1. doi: 10.1108/JFC-06-2020-0113

Durrant S., 2018, *Understanding the Nexus Between Cryptocurrencies and Transnational Crime Operations* [City University of New York]. https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1070&context=jj_etds (accessed 1 July 2024)

Dyntu V., Dykyi O., 2019, Cryptocurrency in the System of Money Laundering, *Baltic Journal of Economic Studies,* 4(5), Article 5. doi: 10.30525/2256-0742/2018-4-5-75-81

Dyntu V., Dykyj O., 2021, Cryptocurrency as an Instrument of Terrorist Financing, *Baltic Journal of Economic Studies,* 7(5), Article 5. doi: 10.30525/2256-0742/2021-7-5-67-72

Dyson S., Buchanan W., Bell L., 2018, The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime, *The Journal of the British Blockchain Association,* 1(2), Article 2. doi: 10.31585/jbba-1-2-(8)2018

ElBahrawy A., Alessandretti L., Rusnac L., Goldsmith D., Teytelboym A., Baronchelli A., 2020, Collective Dynamics of Dark Web Marketplaces, *Scientific Reports,* 10(1), Article 1. doi: 10.1038/s41598-020-74416-y

Etto F., 2017, *Know Your Coins: Public vs. Private Cryptocurrencies, Distributed Bitcoin.* https://www.nasdaq.com/articles/know-your-coins-public-vs-private-cryptocurrencies-2017-09-22 (accessed 1 July 2024)

Europol, 2021, *Cryptocurrencies: Tracing the evolution of criminal finances, Europol*. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol Spotlight - Cryptocurrencies - Tracing the evolution of criminal finances.pdf (accessed 1 July 2024)

FBI, 2022, 2021 *Internet Crime Report, Federal Bureau of Investigation.* https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf(accessed 1 July 2024)

FinCen, 2024, *Financial Crimes Enforcement Network* [United States Department of the Treasury Financial Crimes Enforcement Network], https://www.fincen.gov/ (accessed 1 July 2024)

Finklea K., 2017, *Dark Web.* Congressional Research Service, https://sgp.fas.org/crs/misc/R44101.pdf (accessed 1 July 2024)

Florea I.O., Nitu M., 2020, Money Laundering Through Cryptocurrencies. *Romanian Economic Journal,* 22(76), Article 76.

Fosso Wamba S., Kala Kamdjoug J.R., Epie Bawack R., Keogh J.G., 2020, Bitcoin, Blockchain and Fintech: A Systematic Review and Case Studies in the Supply Chain, *Production Planning & Control,* 31(2–3), Article 2–3. doi: 10.1080/09537287.2019.1631460

Gercke M., 2009, *Understanding Cybercrime: A Guide for Developing Countries,* International Telecommunication Union (ITU), Telecommunication Development Centre. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (accessed 1 July 2024)

Ghalwesh A., Ouf S., Sayed A., 2020, A Proposed System for Securing Cryptocurrency Via the Integration of Internet of Things with Blockchain, *International Journal of Economics and Financial Issues*, 10(3), Article 3.

Godlove N., 2014, Regulatory Overview of Virtual Currency, Oklahoma Journal of Law & Technology, 10(1), Article 1.

Gohwong S.G., 2019, *The State of the Art of Cryptography-Based Cyber-Attacks* (3546334; Issue 3546334), SSRN Scholarly Paper. doi: 10.2139/ssrn.3546334

Goldbarsht D., 2024, Adapting Confiscation and Anti-Money Laundering Laws to the Digital Economy: Exploring the Australian Interplay Between Proceeds and Technology, *Journal of Money Laundering Control,* 27(3), 472–488. doi: 10.1108/JMLC-09-2023-0142

Gómez-Hernández J.A., García-Teodoro P., 2024, Lightweight Crypto-Ransomware Detection in Android Based on Reactive Honeyfile Monitoring, *Sensors*, 24(9), Article 9. doi: 10.3390/s24092679

Goodell G., Aste T., 2019, Can Cryptocurrencies Preserve Privacy and Comply With Regulations?, *Frontiers in Blockchain*, 2, 1–14. doi: 10.3389/fbloc.2019.00004

Grasselli M.R., Lipton A., 2021, *Cryptocurrencies and the Future of Money* (arXiv:2109.10177; Issue arXiv:2109.10177). arXiv. doi: 10.48550/arXiv.2109.10177

Gray I.W., Cable J., Brown B., Cuiujuclu V., McCoy D., 2023, *Money Over Morals: A Business Analysis of Conti Ransomware* (arXiv:2304.11681; Issue arXiv:2304.11681). arXiv. http://arxiv.org/abs/2304.11681

Gryszczyńska A., 2021, The Impact of the COVID-19 Pandemic on Cybercrime, *Bulletin of the Polish Academy of Sciences:* Technical Sciences, 69(4), Article 4. doi: 10.24425/bpasts.2021.137933

Gupta A., Maynard S.B., Ahmad A., 2021, *The Dark Web Phenomenon: A Review and Research Agenda* (arXiv:2104.07138; Issue arXiv:2104.07138). arXiv. doi: 10.48550/arXiv.2104.07138

Harryarsana I.G.K.B., 2022, A Comparison of Regulation of Bitcoin as Crypto (Digital) Currency, *UNTAG Law Review,* 6(2), Article 2. doi: 10.56444/ulrev.v6i2.3452

Hatta M., 2020, Deep Web, Dark Web, Dark Net, *Annals of Business Administrative Science,* 19(6), 277–292. doi: 10.7880/abas.0200908a

Helwig N.E., Hong S., Hsiao-wecksler E.T., 2022, *Combatting Illicit Activity Utilizing Financial Technologies and Cryptocurrencies, Department of Homeland Security.* https://www.dhs.gov/sites/default/files/2022-09/Combatting%20Illicit%20Activity%20.pdf (accessed 1 July 2024)

Hendrickson J.R., Luther W.J., 2022, Cash, Crime, and Cryptocurrencies, *The Quarterly Review of Economics and Finance*, 85, 200–207. doi: 10.1016/j.qref.2021.01.004

Hernandez-Castro J., Cartwright A., Cartwright E., 2020, An Economic Analysis of Ransomware and Its Welfare Consequences, *Royal Society Open Science*, 7(3), Article 3. doi: 10.1098/rsos.190023

Higbee A., 2018, The Role of Crypto-Currency in Cybercrime, *Computer Fraud & Security,* 2018(7), Article 7. doi: 10.1016/S1361-3723(18)30064-2

Holt T.J., Lee J.R., Griffith E., 2023 An Assessment of Cryptomixing Services in Online Illicit Markets, *Journal of Contemporary Criminal Justice,* 39(2), 222–238. doi: 10.1177/10439862231158004

ICE, 2020, *Dutch National Charged in Takedown of Obscene Website Selling Over 2,000 "Real Rape" and Child Pornography Videos, Funded by Cryptocurrency* [United States Department of Homeland Security, United States Immigration and Customs Enforcement], https://www.ice.gov/news/releases/dutch-national-charged-takedown-obscene-website-selling-over-2000-real-rape-and-child (accessed 1 July 2024)

Ilijevski I., Ilik G., Babanoski K., 2023, Cryptocurrency Abuse for the Purposes of Money Laundering and Terrorism Financing: Policies and Practical Aspects in the European Union and North Macedonia, *European Scientific Journal ESJ,* 3. doi: 10.19044/esipreprint.3.2023.p23

Interpol, 2020, *Online African Organized Crime from Surface to Dark Web, European Commission.* https://south.euneighbours.eu/publication/interpol-report-online-african-organized-crime-surface-darkweb/ (accessed 1 July 2024)

Irwin A., Slay J., 2010, Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft, *International Cyber Resilience Conference,* 8, 41–51.

Ivaniuk V., Banakh S., 2020, Cryptocurrency-Related Cybercrimes in Ukraine, *Osteuropa Recht,* 66(1), Article 1. https://doi.org/10.5771/0030-6444-2020-1-217

Johari R.J., Zul N.B., Talib N., Hussin S.A.H.S., 2019, Money Laundering: Customer Due Diligence in the Era of Cryptocurrencies, *Proceedings of the 1st International Conference on Accounting, Management and Entrepreneurship* (ICAMER 2019). 1st International Conference on Accounting, Management and Entrepreneurship (ICAMER 2019), Cirebon, Indonesia. doi: 10.2991/aebmr.k.200305.033

Jung B., Choi K.-S., Lee C., 2022, Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business, *International Journal of Cybersecurity Intelligence & Cybercrime*, 5(2), Article 2. doi: 10.52306/2578-3289.1135

Jung K., 2022, Freedom to Morph? An Analysis of Morphed Imagery, Child Pornography, and the First Amendment, *Catholic University Journal of Law and Technology,* 30(2), 33–64.

Kabra S., Gori S., 2023, Drug Trafficking on Cryptomarkets and the Role of Organized Crime Groups, *Journal of Economic Criminology*, 2, 100026. doi: 10.1016/j.jeconc.2023.100026

Kamps J., Kleinberg B., 2018, To the Moon: Defining and Detecting Cryptocurrency Pump-and-Dumps, Crime Science, 7(1), Article 1. doi: 10.1186/s40163-018-0093-5

Kavitha M., Golden J., 2024, Smarter and Resilient Smart Contracts Applications for Smart Cities Environment Using Blockchain Technology, Automatika, 65(2), 572–583. doi: 10.1080/00051144.2024.2307228

Kayani U., Hasan F., 2024, Unveiling Cryptocurrency Impact on Financial Markets and Traditional Banking Systems: Lessons for Sustainable Blockchain and Interdisciplinary Collaborations, *Journal of Risk and Financial Management,* 17(2), Article 2. doi: 10.3390/jrfm17020058

Keane K., 2020, Does Bitcoin Use Affect Crime Rates?, *The Corinthian,* 20(1). https://kb.gcsu.edu/thecorinthian/vol20/iss1/2 (accessed 1 July 2024)

Kerr D.S., Loveland K.A., Smith K.T., Smith L.M., 2023, Cryptocurrency Risks, Fraud Cases, and Financial Performance, *Risks*, 11(3), Article 3. doi: 10.3390/risks11030051

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

Kethineni S., Cao Y., Dodge C., 2018, Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes, *American Journal of Criminal Justice,* 43(2), Article 2. doi: 10.1007/s12103-017-9394-6

Kfir I., 2020, Cryptocurrencies, National Security, Crime and Terrorism, *Comparative Strategy,* 39(2), Article 2. doi: 10.1080/01495933.2020.1718983

Kien L.T., Binh N.H., 2021, Crime in Era of Digital Technology: What Can Change with Cryptocurrency Status Clarification for Development of Information Environment of Vietnam?, *Webology*, 18(Special Issue), Article Special Issue. doi: 10.14704/WEB/V18SI04/WEB18141

Kristoufek L., 2015, What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis, *PLoS ONE*, 10(4), Article 4. doi: 10.1371/journal.pone.0123923

Kutera M., 2022, Cryptocurrencies as a Subject of Financial Fraud, Journal of Entrepreneurship, *Management and Innovation,* 18(4), Article 4. doi: 10.7341/20221842

Lacson W., Jones B., 2016, The 21st Century Dark Net Market: Lessons from the Fall of Silk Road, *International Journal of Cyber Criminology,* 10(1), Article 1. doi: 10.5281/zenodo.58521

Lapuh Bele J., 2021, Cryptocurrencies as Facilitators of Cybercrime, *SHS Web of Conferences*, 111, 01005. doi: 10.1051/shsconf/202111101005

Lee J.R., Holt T.J., Smirnova O., 2022, An Assessment of the State of Firearm Sales on the Dark Web, *Journal of Crime and Justice*, 44, 1–15. doi: 10.1080/0735648X.2022.2058062

Lee L., 2019, Cybercrime Has Evolved: It's Time Cyber Security Did Too, *Computer Fraud and Security,* 2019(6), Article 6. doi: 10.1016/S1361-3723(19)30063-6

Lee S., Yoon C., Kang H., Kim Y., Kim Y., Han D., Son S., Shin S., 2019, Cybercriminal Minds: An Investigative Study of Cryptocurrency Abuses in the Dark Web, *Proceedings 2019 Network and Distributed System Security Symposium,* Network and Distributed System Security Symposium, San Diego, CA. doi: 10.14722/ndss.2019.23055

Legge M., 2023, *Crypto Taxes India: Ultimate Guide 2023* [Koinly Blog], https://koinly.io/guides/crypto-tax-india/ (accessed 1 July 2024)

Leuprecht C., Jenkins C., Hamilton R., 2022, Virtual Money Laundering: Policy Implications of the Proliferation in the Illicit Use of Cryptocurrency, *Journal of Financial Crime,* 30(4), 1036–1054. doi: 10.1108/JFC-07-2022-0161

Liao K., Zhao Z., Doupe A., Ahn G.-J., 2016, Behind Closed Doors: Measurement and Analysis of Cryptolocker Ransoms in Bitcoin, *2016 APWG Symposium on Electronic Crime Research (eCrime)*, 1–13. doi: 10.1109/ECRIME.2016.7487938

Lin D., Wu J., Fu Q., Yu Y., Lin K., Zheng Z., Yang S., 2023, *Towards Understanding Crypto Money Laundering in Web3 Through the Lenses of Ethereum Heists* (arXiv:2305.14748; Issue arXiv:2305.14748), arXiv, http://arxiv.org/abs/2305.14748 (accessed 1 July 2024)

Lipton A., 2021, Cryptocurrencies Change Everything, *Quantitative Finance,* 21(8), Article 8. doi: 10.1080/14697688.2021.1944490

Luong H.T., 2023, Foundations and Trends in the Darknet-Related Criminals in the Last 10 Years: A Systematic Literature Review and Bibliometric Analysis, *Security Journal*. doi: 10.1057/s41284-023-00383-4

Mackenzie S., 2022, Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial, *The British Journal of Criminology,* 62(6), Article 6. doi: 10.1093/BJC/AZAB118

Manjula B., Shilpa B., Sundaresh M., 2022, Analysis of Cryptocurrency, Bitcoin and the Future, *East Asian Journal of Multidisciplinary Research,* 1(7), Article 7. doi: 10.55927/eajmr.v1i7.803

Masciandaro D., Barone R., Masciandaro D., 2019, Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques, *European Journal of Law and Economics,* 47(December), Article December. doi: 10.2139/ssrn.3303871

Mataković I. C., 2022, Crypto-Assets Illicit Activities: Theoretical Approach with Empirical Review, I*nternational E-Journal of Criminal Sciences Artículo,* 5(2022), Article 2022.

Matarese V., 2013),Reporting—The Final Phase of Scientific Research—Can and Should Be Supported: A Case for Integrating Language Professionals into the Research Setting, *RT: A Journal on Research Policy and Evaluation,* 1(1), Article 1. doi: 10.13130/2282-5398/3200

Maxwell F., 2022, Children's Rights, The Optional Protocol and Child Sexual Abuse Material in the Digital Age: Moving from Criminalisation to Prevention, *The International Journal of Children's Rights*, 31(1), 61–88. doi: 10.1163/15718182-30040004

Mazambani L., 2024, *Determinants of Public Trust in Digital Money: The Case of Central Bank Digital Currency* (4708114), SSRN Scholarly Paper. doi: 10.2139/ssrn.4708114

Meland P.H., Bayoumy Y.F.F., Sindre G., 2020, The Ransomware-as-a-Service Economy Within the Darknet, *Computers & Security,* 92, 101762. doi: 10.1016/j.cose.2020.101762

Mirea M., Wang V., Jung J., 2019, The Not so Dark Side of the Darknet: A Qualitative Study, *Security Journal,* 32(2), Article 2. doi: 10.1057/s41284-018-0150-5

Moffett T., 2023, CFTC & SEC: The Wild West of Cryptocurrency Regulation, *University of Richmond Law Review,* 57(2), Article 2.

Moore D., Rid T., 2016, Cryptopolitik and the Darknet, *Survival*, 58(1), Article 1. doi: 10.1080/00396338.2016.1142085

Morelato M., Bozic S.M., Rhumorbarbe D., Broséus J., Staehli L., Esseiva P., Roux C., Rossy Q., 2020, An Insight into Prescription Drugs and Medicine on the Alphabay Cryptomarket, *Journal of Drug Issues,* 50(1), Article 1. doi: 10.1177/0022042619872955

Mthembu N., Sanusi K.A., Eita J.H., 2022, Do Stock Market Volatility and Cybercrime Affect Cryptocurrency Returns? Evidence from South African Economy, *Journal of Risk and Financial Management,* 15(12), Article 12. doi: 10.3390/jrfm15120589

Mubarak D., Manjunath H., 2021, A Study on Cryptocurrency in India, International *Journal of Research and Analytical Reviews,* 8(1), Article 1.

Munawa F., 2023, *Bitcoin Use Cases Are Seeing Explosive Growth, Trust Machines Says.* CoinDesk, https://www.coindesk.com/tech/2023/04/28/bitcoin-use-cases-are-seeing-explosive-growth-trust-machines-says/ (accessed 1 July 2024)

Muslim A.K., Mohd Dzulkifli D.Z., Nadhim M.H., Abdellah R.H., 2019, A Study of Ransomware Attacks: Evolution and Prevention, *Journal of Social Transformation and Regional Development,* 1(1), Article 1. doi: 10.30880/jstard.2019.01.01.003

Naheem M.A., 2021, Do Cryptocurrencies Enable and Facilitate Modern Slavery?, *Journal of Money Laundering Control,* 24(3), Article 3. doi: 10.1108/JMLC-07-2020-0073

Nakamoto S., 2009, Bitcoin: A Peer-to-Peer Electronic Cash System, *Cryptography*, 1, 1–9.

Naqvi S., 2018, Challenges of Cryptocurrencies Forensics: A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals, P*roceedings of the 13th International Conference on Availability, Reliability and Security*, 1–5. doi: 10.1145/3230833.3233290

Nazzari M., 2023, From Payday to Payoff: Exploring the Money Laundering Strategies of Cybercriminals, *Trends in Organized Crime*. doi: 10.1007/s12117-023-09505-1

Nazzari M., Riccardi M., 2024, Cleaning Mafia Cash: An Empirical Analysis of the Money Laundering Behaviour of 2800 Italian Criminals, *European Journal of Criminology,* 14773708231224981. doi: 10.1177/14773708231224981

Nialldawson, 2015, *Silkroad 3.0, a "Darknet" Blackmarket Website* [Wikimedia Commons]. https://commons.wikimedia.org/wiki/File:Silkroad30.png (accessed 1 July 2024)

Nouwen Y., 2017, Online Child Sexual Exploitation: An Analysis of Emerging and Selected Issues, *ECPAT International Journal,* 12, Article 12.

Nurhadiyanto L., 2020, The Identification of Money Laundering on Drug Trafficking, *Asia Pacific Fraud Journal,* 5(1), Article 1. doi: 10.21532/apfjournal.v5i1.137

Omeljaniuk J., 2020, Cryptocurrencies as a Generic Object of Crime in Polish Criminal Law, *Annual Center Review*, 12–13, Article 12–13. doi: 10.15290/acr.2019-2020.12-13.05

Otabek S., Choi J., 2024, Multi-Level Deep Q-Networks for Bitcoin Trading Strategies, *Scientific Reports*, 14(1), Article 1. doi: 10.1038/s41598-024-51408-w

Özer M., Vukovic D., Frömmel M., Kamişli M., 2024, Does Bitcoin Shocks Truly Cointegrate with Financial and Commodity Markets? (4735090), SSRN Scholarly Paper. doi: 10.2139/ssrn.4735090

Ozturk L., Sulungur E., 2021, The Regulation Problem of Cryptocurrencies, *M3 Publishing,* 5(2021), Article 2021. doi: 10.5038/9781955833035

Paquet-Clouston M., Haslhofer B., Dupont B., 2019,. Ransomware Payments in the Bitcoin Ecosystem, *Journal of Cybersecurity,* 5(1), Article 1. doi: 10.1093/cybsec/tyz003

Patel P.C., Richter J., 2020, The Relationship Between Terrorist Attacks and Cryptocurrency Returns, *Applied Economics,* 53(8), Article 8. doi: 10.1080/00036846.2020.1819952

Patsakis C., Politou E., Alepis E., Hernandez-Castro J., 2023, Cashing Out Crypto: State of Practice in Ransom Payments, *International Journal of Information Security.* doi: 10.1007/s10207-023-00766-z

Perkins N., 2021, Cryptocurrency: The Economics of Money and Selected Policy Issues, Congressional Research Service.

Pernice I.G.A., Scott B., 2021, Cryptocurrency, *Internet Policy Review,* 10(2), Article 2. doi: 10.14763/2021.2.1561

Phugger B., 2021, *China's Central Bank Declares All Cryptocurrency Transactions Illegal* [Blockchain: Baker Mckenzie], https://blockchain.bakermckenzie.com/2021/10/04/chinas-central-bank-declares-all-cryptocurrency-transactions-illegal/ (accessed 1 July 2024)

Piazza F., 2017, Bitcoin in the Dark Web: A Shadow Over Banking Secrecy and a Call for Global Response, *Southern California Interdisciplinary Law Journal,* 26(3), Article 3.

Pieroni C., 2018, La Crypto Nostra: How Organized Crime Thrives in the Era of Cryptocurrency, *Technology*, 20(5), Article 5.

Pilinkiene V., Dumciuviene D., Schenk-Hoppé K.R., Ilbiz E., Kaunert C., 2022, Sharing Economy for Tackling Crypto-Laundering: The Europol Associated Global Conference on Criminal Finances and Cryptocurrencies, *Sustainability*, 14(11), Article 11. doi: 10.3390/su14116618

Pop C., Colonescu I.-E., 2021, Cryptocurrencies' Puzzle, *Studia Universitatis Babeș-Bolyai Negotia,* 66(2), Article 2. doi: 10.24193/subbnegotia.2021.2.06

Priyambudi, Sinaga H.D.P., 2021, Prosecutorial Discretion in Tackling the Cryptocurrency Crime in Indonesia, *Webology*, 18(2), Article 2. doi: 10.14704/WEB/V18I2/WEB18308

Pushkarev V.V., Artemova V.V., Ermakov S.V., Alimamedov E.N., Popenkov A.V., 2020, Criminal Prosecution of Persons, Who Committed Criminal, Acts Using the Cryptocurrency in the Russian Federation, *Revista San Gregorio,* 1(42), e1566. doi: 10.36097/rsan.v1i42.1566

Rajagopal K., 2020, Supreme Court Sets Aside RBI Ban on Cryptocurrency Transactions. *The Hindu*. https://www.thehindu.com/news/national/supreme-court-sets-aside-rbi-ban-on-cryptocurrency-transactions/article61967124.ece (accessed 1 July 2024)

Raman R., Kumar Nair V., Nedungadi P., Ray I., Achuthan K., 2023, Dark Web Research: Past, Present, and Future Trends and Mapping to Sustainable Development Goals, *Heliyon*, 9(11), e22269. doi: 10.1016/j.heliyon.2023.e22269

Recskó M., Aranyossy M., 2024, User Acceptance of Social Network-Backed Cryptocurrency: A Unified Theory of Acceptance and Use of Technology (Utaut)-Based Analysis, *Financial Innovation,* 10(1), Article 57. doi: 10.1186/s40854-023-00511-4

Reddy E., 2020, Analysing the Investigation and Prosecution of Cryptocurrency Crime as Provided for by the South African Cybercrimes Bill, *Statute Law Review,* 41(2), Article 2. doi: 10.1093/slr/hmz001

Reddy E., Minaar A., 2018, Cryptocurrency: A Tool and Target for Cybercrime, *Acta Criminologica: Southern African Journal of Criminology,* 31(3), Article 3.

Reddy E., Minaar A., Omeljaniuk J., Rueckert C., Taylor S.K., Ariffin A., Zainol Ariffin K.A., Sheikh Abdullah S.N.H., Moore D., Rid T., Teichmann F.M.J., Falker M.C., Pilinkiene V., Dumciuviene D., Schenk-Hoppé K.R., Ilbiz E., Kaunert C., Zimba A., Wang Z., …, Sindre G., 2020,. Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial, *Journal of Cybersecurity,* 10(2), Article 2. doi: 10.57019/jmv.1108783

Reiff N., Mansa J., Velasquez V., 2023, *Howey Test Definition: What It Means and Implications for Cryptocurrency, Investopedia*, https://www.investopedia.com/terms/h/howey-test.asp (accessed 1 July 2024)

Renear A.H., Palmer C.L., 2009, Strategic Reading, Ontologies, and the Future of Scientific Publishing, *Science*, 325(5942), 828–832. doi: 10.1126/science.1157784

Reynolds P., Irwin A.S.M., 2017, Tracking Digital Footprints: Anonymity Within the Bitcoin System, *Journal of Money Laundering Control,* 20(2), Article 2. doi: 10.1108/JMLC-07-2016-0027

Riahi R., Bennajma A., Jahmane A., Hammami H., 2024, Investing in Cryptocurrency Before and During the COVID-19 Crisis: Hedge, Diversifier or Safe Haven?, *Research in International Business and Finance,* 67, 102102. doi: 10.1016/j.ribaf.2023.102102

Rieckmann J., Stuchtey T., 2023, *Dark Crypto: The Use of Cryptocurrency for Illegal Purposes,* Friedrich Naumann Foundation For Freedom.

Rizzo P., 2017, *Indonesia's AML Watchdog Links Bitcoin to Islamic State* [CoinDesk], https://www.coindesk.com/markets/2017/01/09/indonesias-aml-watchdog-links-bitcoin-to-islamic-state/ (accessed 1 July 2024)

Rubasundram G.A., 2019, The Dark Web and Digital Currencies: A Potent Money Laundering and Terrorism Opportunity, *International Journal of Recent Technology and Engineering,* 7(5), Article 5.

Rudesill D.S., Caverlee J., Sui D., 2015, *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box* (2676615; Issue 2676615), SSRN Scholarly Paper, https://doi.org/10.2139/ssrn.2676615 (accessed 1 July 2024)

Rueckert C., 2019, Cryptocurrencies and Fundamental Rights, *Journal of Cybersecurity,* 5(1), Article 1. doi: 10.1093/cybsec/tyz004

Saiedi E., Broström A., Ruiz F., 2021, Global Drivers of Cryptocurrency Infrastructure Adoption, *Small Business Economics,* 57(1), Article 1. doi: 10.1007/s11187-019-00309-8

Sanusi K.A., Dickason-Koekemoer Z., 2022, Cryptocurrency Returns, Cybercrime and Stock Market Volatility: GAS and Regime Switching Approaches, *International Journal of Economics and Financial Issues,* 12(6), Article 6. doi: 10.32479/IJEFI.13555

Sanz-Bas D., del Rosal C., Náñez Alonso S.L., Echarte Fernández M.Á., 2021, Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain, *Laws*, 10(3), Article 3. doi: 10.3390/laws10030057

Sayid M.R.N., 2023, The Fusion of Blockchain, Pornography and Human Trafficking in a Global Digital Dragnet That Forms the Online Child Sex Trafficking, *Russian Law Journal,* 11(5s), Article 5s. doi: 10.52783/rlj.v11i5s.891

Șcheau M.C., Crăciunescu S.L., Brici I., Achim M.V., 2020, A Cryptocurrency Spectrum Short Analysis, *Journal of Risk and Financial Management,* 13(8), Article 8. doi: 10.3390/jrfm13080184

Schneider N., 2019, Decentralization: An Incomplete Ambition, *Journal of Cultural Economy,* 12(4), 265–285. doi: 10.1080/17530350.2019.1589553

Sherer J.A., McLellan M.L., Fedeles E.R., Sterling N.L., 2016, Ransomware: Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web Annual Survey, *Richmond Journal of Law & Technology,* 23(3), Article 3.

Shinder L.D., Cross M., 2008, *Scene of the Cybercrime,* Syngress. doi: 10.1016/B978-1-59749-276-8.00018-2

Sicignano G.J., 2021, Money Laundering using Cryptocurrency: The Case of Bitcoin!, *Athens Journal of Law,* 7(2), Article 2. doi: 10.30958/ajl.7-2-7

Sidhpurwala H., 2023, *A Brief History of Cryptography* [Red Hat], https://www.redhat.com/en/blog/brief-history-cryptography (accessed 1 July 2024)

Sigler K., 2018, Crypto-Jacking: How Cyber-Criminals Are Exploiting the Crypto-Currency Boom, *Computer Fraud and Security,* 2018(9), Article 9. doi: 10.1016/S1361-3723(18)30086-1

Silfversten E., Favaro M., Slapakova L., Ishikawa S., Liu J., Salas A., 2020, *Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes,* Rand Corporation. doi: 10.7249/RR4418

Singh S., Nambiar V., 2024, Role of Artificial Intelligence in the Prevention of Online Child Sexual Abuse: A Systematic Review of Literature, *Journal of Applied Security Research,* 0(0), 1–42. doi: 10.1080/19361610.2024.2331885

Soni N., 2024, Letter to the Editor: "Potential Applicability of Blockchain Technology in the Maintenance of Chain of Custody in Forensic Casework", *Egyptian Journal of Forensic Sciences,* 14(1), Article 22. doi: 10.1186/s41935-024-00396-z

Sovbetov Y., 2018, *Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero* (3125347; Issue 3125347), SSRN Scholarly Paper, https://papers.ssrn.com/abstract=3125347 (accessed 1 July 2024)

Stroukal D., Nedvědová B., 2016, Bitcoin and Other Cryptocurrency as an Instrument of Crime in Cyberspace, *Proceedings of 4th Business & Management Conference. 4th Business & Management Conference*, Istanbul. doi: 10.20472/BMC.2016.004.018

Suslenko V., Zatonatska T., Dluhopolskyi O., Kuznyetsova A., 2022, Use of Cryptocurrencies Bitcoin and Ethereum in the Field of E-Commerce: Case Study of Ukraine, *Financial and Credit Activity Problems of Theory and Practice,* 1(42), Article 42. doi: 10.55643/fcaptp.1.42.2022.3603

Tan B., 2024, *Central Bank Digital Currency Adoption: A Two-Sided Model* (4734056), SSRN Scholarly Paper. doi: 10.5089/9798400268113.001

Taylor S.K., Ariffin A., Zainol Ariffin K.A., Sheikh Abdullah S.N.H., 2021, Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets, *3rd International Cyber Resilience Conference*, 1–5. doi: 10.1109/CRC50527.2021.9392446

Team C., 2024, *2024 Crypto Crime Trends from Chainalysis, Chainalysis.* https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (accessed 1 July 2024)

Teichmann F., Falker M.-C., 2020a, Cryptocurrencies and Financial Crime: Solutions from Liechtenstein, *Journal of Money Laundering Control*, 24(4), Article 4. doi: 10.1108/JMLC-05-2020-0060

Teichmann F., Falker M.-C., 2020b, Money Laundering Through Cryptocurrencies, [in:] E. G. Popkova, S. Sergi (Eds.), *Artificial Intelligence: Anthropogenic Nature vs. Social Origin*, Springer International Publishing, Cham, 500–511. doi: 10.1007/978-3-030-39319-9_57

Teichmann F., Falker M.-C., 2024, Terrorist Financing Via the Banking Sector. *Crime, Law and Social Change.* doi: 10.1007/s10611-023-10133-7

Thamizhisai M.D., Bharathi S., Bhuvaneshwaran U., Immanuvel S.M., Patchaiyappan M., 2024, Enhancing Forensic Investigations Leveraging Blockchain and Smart Contracts for Security and Transparency, *International Journal of Scientific Research in Science and Technology,* 11(3), Article 3.

Trozze A., Kamps J., Akartuna E.A., Hetzel F.J., Kleinberg B., Davies T., Johnson S.D., 2022, Cryptocurrencies and Future Financial Crime, *Crime Science*, 11(1), Article 1. doi: 10.1186/s40163-021-00163-8

Turchyn N., Turchyn A., 2021, Legal Regulation of Cryptocurrency in Ukraine, *Economics, Finance, Law,* 5(1), Article 1. doi: 10.37634/efp.2021.5(1).6

Turner A.B., McCombie S., Uhlmann A.J., 2020, Analysis Techniques for Illicit Bitcoin Transactions, *Frontiers in Computer Science,* 2(November), Article November. doi: 10.3389/fcomp.2020.600596

UNODC, 2020, *Darknet Cybercrime Threats to Southeast Asia, United Nations Office on Drugs and Crime*, https://www.unodc.org/documents/southeastasiaandpacific//Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf (accessed 1 July 2024)

UNODC, 2023, *World Drug Report 2023*, United Nations Office on Drugs and Crime, https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2023.html (accessed 1 July 2024)

van Nguyen T., Truong T.V., Lai C.K., 2022, Legal Challenges to Combating Cybercrime: An Approach from Vietnam, Crime, *Law and Social Change*, 77(3), Article 3. doi: 10.1007/S10611-021-09986-7/TABLES/3

van Wegberg R., Oerlemans J.J., van Deventer O., 2018, Bitcoin Money Laundering: Mixed Results?: An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin, *Journal of Financial Crime,* 25(2), Article 2. doi: 10.1108/JFC-11-2016-0067

Verduyn M.C., 2018, *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global*

Governance, Routledge, https://library.oapen.org/bitstream/handle/20.500.12657/29557/1000376.pdf?sequence=1&isAllowed=y (accessed 1 July 2024)

Virga J.M., 2015, International Criminals and Their Virtual Currencies: The Need for an International Effort in Regulating Virtual Currencies and Combating Cyber Crime, *Revista de Direito Internacional,* 12(2), Article 2. doi: 10.5102/rdi.v12i2.3557

Volevodz A., 2024, *About the State and Some Trends of Cryptocurrency-Related Crime* (4693186), SSRN Scholarly Paper. doi: 10.2139/ssrn.4693186

Wang S., Zhu X., 2021, Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing, *Policing: A Journal of Policy and Practice*, 15(4), Article 4. doi: 10.1093/police/paab059

Watters C., 2023, When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment, *Laws*, 12(2), Article 2. doi: 10.3390/laws12020033

Wen L., Bao L., Chen J., Grundy J., Xia X., Yang X., 2024, Market Manipulation of Cryptocurrencies: Evidence from Social Media and Transaction Data, *ACM Transactions on Internet Technology.* doi: 10.1145/3643812

Widhiyanti H.N., Hussein S.M., Ganindha R., 2023, Indonesian Cryptocurrencies Legislative Readiness: Lessons from the United States, *Sriwijaya Law Review,* 7(1), Article 1. doi: 10.28946/slrev.Vol7.Iss1.2138.pp150-172

Wronka C., 2022a, "Cyber-Laundering": The Change of Money Laundering in the Digital Age, *Journal of Money Laundering Control,* 25(2), Article 2. doi: 10.1108/JMLC-04-2021-0035

Wronka C., 2022b, Money Laundering Through Cryptocurrencies: Analysis of the Phenomenon and Appropriate Prevention Measures, J*ournal of Money Laundering Control,* 25(1), Article 1. doi: 10.1108/JMLC-02-2021-0017

Xie R., 2019, Why China Had to Ban Cryptocurrency but the US Did Not: A Comparative Analysis of Regulations on Crypto-Markets Between the US and China, [in:] *Wash. U. Global Stud. L. Rev.* (Vol. 18). Washington University Global Studies Law Review.

Yunandi F., Leksono A.B., 2023, Criminal Sanctions Against Money Laundering Crimes in the Perspective of Economic Analysis of Law, *Rechtsnormen Journal of Law,* 1(2), Article 2. doi: 10.55849/rjl.v1i2.391

Zaunseder A., Bancroft A., 2020, Pricing of Illicit Drugs on Darknet Markets: A Conceptual Exploration, *Drugs and Alcohol Today,* 21(2), Article 2. doi: 10.1108/DAT-12-2019-0054

Zavoli I., 2022, T*he Use of Cryptocurrencies in the UK Real Estate Market: An Assessment of Money Laundering Risks* (4033765), SSRN Scholarly Paper, https://papers.ssrn.com/abstract=4033765 (accessed 1 July 2024)

Zheng X., 2024, Research on Blockchain Smart Contract Technology Based on Resistance to Quantum Computing Attacks, *PLOS ONE*, 19(5), e0302325. doi: 10.1371/journal.pone.0302325

Zimba A., Wang Z., Mulenga M., Odongo N.H., 2020, Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security, *Journal of Computer Information Systems,* 60(4), Article 4. doi: 10.1080/08874417.2018.1477076