INTERNATIONAL CONFERENCE
ON ISLAMIC ECONOMICS
febi.uinsu.ac.id/proceeding-international-conference/
Vol. 1, No. 1, 2023

CRYPTO INVESTMENT CYBERCRIME

Iqlima Azhar[1], Muhammad Salman[2]
Universitas Islam Negeri Sumatera Utara[1,2], Universitas Samudra[1,2], Indonesia
Iqlima_a@unsam.ac.id[1], muhammadsalman@unsam.ac.id[2]

Abstract

Abstract - This bibliometric analysis was conducted a study related to crypto investment cybercrime. This research is a literature review using the Harzing Publish or Perish and Mendeley search tools which are limited to being related only to crypto investment cybercrime in the 2017-2023 research period and published in scopus indexed journals. The research findings show that only four publications are directly related to crypto investment cybercrime so it is recommended for further research to be carried out empirically and published in scopus indexed journals.

Keyword: crypto investment cybercrime

Introduction

The government must protect investors who make cryptocurrency investment, namely in term of rules, the government must make regulations specifically in dealing with legal protection for investors and in the view of Islamic economics, other cryptocurrency are an illegal investment tool because they contain gharar, maysir high recovery (chancy) (Ammy & Soemitra, 2023). Cryptocurrency investment in the Islamic Economy as a legal currency is permitted as long as there is no harm and does not affect the people as money methods. Several muslim countries such as Egypt, Iran and Turkiye prohibit and regulate the use of the digital currency, while Saudi Arabia, the United Arab Emirates and Qatar have approved their use. The study of cybercrime for cryptocurrency investment has recently been interesting to study because crypto investment cybercrime refers to criminal activity that targets individuals or entities involved in cryptocurrency investments. These crimes are committed through digital means, utilizing various cyber techniques and tactics to illegally acquire or manipulate cryptocurrencies, disrupt crypto markets, or defraud investors, (Blog.avast.com, 2023; fultonmay.com, 2023; Simplilearn.com, 2022). In general, cybercrimes on crypto investments include: Hacking: Cybercriminals gain unauthorized access to cryptocurrency wallets, exchanges, or other platforms to steal digital assets or manipulate transactions. Phishing: Criminals use deceptive emails, websites, or messages to trick cryptocurrency users into revealing their login credentials or private keys, allowing them to gain control of their funds. Ransomware Attacks: Malicious software is used to encrypt victims' data, and a ransom is demanded in cryptocurrency for launch. Ponzi Schemes and Investment Scams: Fraudsters create fake investment opportunities or schemes that promise high returns, targeting individuals looking to invest in cryptocurrencies. Pump-and-Dump schemes: Criminals artificially inflate the price of cryptocurrencies through false information or coordinated trading, then sell their holdings to unsuspecting investors before prices fall. Fraudulent Initial Coin Offerings (ICOs): Fraudsters launch ICOs for non-existent projects or scams, tricking investors into buying worthless tokens or coins. Cryptojacking: Unauthorized

use of computing resources to mine cryptocurrencies without the knowledge or consent of the device owner, often through malware injection, (Christin, 2013; Kharraz et al., 2015).

Researchers can define cybercrime in crypto investments in different ways, but generally include the following elements: Illicit Activity which refers to criminal acts committed through digital means, targeting individuals or entities involved in cryptocurrency investments. These activities can include hacking, phishing, identity theft, ransomware attacks, Ponzi schemes, pump-and-dump schemes, fraudulent Initial Coin Offerings (ICOs), and other forms of fraud or theft. Targeting Cryptocurrency Investors where cybercrime focuses on individuals or organizations involved in cryptocurrency investments, such as cryptocurrency traders, investors, exchanges, wallets, or other crypto service providers. Digital Vulnerability Exploitation where cybercriminals exploit various digital vulnerabilities, such as weaknesses in crypto exchange platforms, insecure wallets, social engineering techniques, or malware, to perform their illicit activities and gain unauthorized access to cryptocurrency assets. And Financial gains, which are the main source of motivation behind crypto investment cybercrime, are often financial gains. Cybercriminals aim to steal cryptocurrencies, manipulate markets for their own benefit, or trick investors into investing in fraudulent schemes to obtain their funds, (Bijmans et al., 2019; Dorofeeva et al., 2019; Jafari et al., 2018; Rueckert, 2019; Trozze et al., 2022; Tu, 2018; Wilson, 2019).

Literature review

Research Kharraz et al., (2015) presents a long-term study of ransomware attacks. The study provides insight into how ransomware attacks work, including the techniques used by attackers to encrypt files and demand payment, as well as the strategies used by victims to recover their data. The study also highlights the challenges of detecting and preventing ransomware attacks, as well as the importance of situational awareness in mitigating the impact of such attacks. This article provides a comprehensive analysis of the impact of ransomware attacks on individuals and organizations, as well as the need for effective cybersecurity measures to prevent and mitigate the impact of such attacks. Overall, research by Kharraz et al., (2015) provides a detailed analysis of ransomware attacks and their impact on cybersecurity.

Research conducted by Trozze et al., (2022) shows that hacking and exploitation are the most common type of crypto-related financial crime in 2022, with funds stolen in hacks estimated to be around $4.3 billion. Cryptocurrencies are vulnerable to undetected money laundering, terrorist financing, sanctions evasion and fraud, making them targets for financial crime. Research on the potential of cryptocurrencies for fraud has not been examined in systematic studies, but a review of academic research and literature reviews on cryptocurrency scams identified 29 types of cryptocurrency scams. Cybercriminals use cryptocurrencies for a variety of purposes, including laundering dirty money, defrauding victims out of funds, defrauding investors, and other types of financial crimes. Cryptocurrencies are not only limited to cybercrime but are used for all kinds of crimes involving the transmission of monetary value, including money laundering, evasion of financial sanctions, bribery, and embezzlement. The lack of regulation and oversight in the

cryptocurrency market makes them highly vulnerable to fraud, and the use of anonymous transactions and difficulties in tracking the movement of funds make it difficult to detect and prevent fraud. Potential precautions to mitigate risks associated with crypto investment cybercrime include the use of advertising, (Cong et al., 2023). Researchers studying crypto investment cybercrime can examine the prevalence, trends, techniques used by cybercriminals, their impact on victims and the crypto market, and potential precautions to reduce the risks associated with such crimes. It is important to note that the field of cybercrime is growing rapidly, and researchers are constantly adjusting their definition and understanding of crypto investment cybercrime to keep up with emerging threats and trends. Theactivation behind crypto investment cybercrime includes financial gains, crypto market disruption, and exploitation of digital vulnerabilities. Cybercriminals take advantage of the relatively unregulated and pseudonymous nature of cryptocurrencies to carry out their illicit activities, (Bijmans et al., 2019). The cybercrime impact of crypto investments can be significant, resulting in financial losses for individuals and organizations, erosion of trust in cryptocurrencies, and regulatory and legal challenges. As a result of these crimes, strong security measures, user education, and regulatory frameworks are needed to mitigate the risks associated with these crimes. It is important to remain vigilant, use secure platforms, implement best security practices, and exercise caution when engaging in cryptocurrency investments to minimize the risk of becoming a victim of crypto investment cybercrime, (Sanusi &; Dickason-koekemoer, 2022).

Research Methods

This research article is analyzed using bibliometric methods to find articles related and relevant to crypto investment cybercrime desired by researchers and this bibliometric analysis allows researchers to analyze the intensity of publication of articles related to crypto investment cybercrime with data sources sourced from Scopus. In several reviews related to this study, the authors used access to a comprehensive database derived from Scopus, arguing that choosing Scopus lies in the availability of its data base which is almost 60 percent larger than the Web of Science Database (WoS), (Zhao & Strotmann, 2015). Therefore, the author searches for relevant articles and journals for this research from the Scopus database with the following keywords; "Crypto Investment Cybercrime" and this study limited its analysis to the discipline of "accounting and management" which emphasizes only the variable "crypto investment cybercrime".

Research Results and Discussion

Search results using the Harzing Publish or Perish application with a focus on scopus publications, showing the number of publications from the range of 2017 – 2023 with the keyword "crypto investment cybercrime" only as many publications.

Table 1. Search results in the scopus data base with the keyword crypto investment cybercrime

Citation	Author	Heading	Year	Source
13	(Mackenzie, 2022)	Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial	2022	British Journal of Criminology
1	(Morgan, 2022)	Assessing the Risks Associated with Green Digital Finance and Policies for Coping with Them	2022	Economics, Law, and Institutions in Asia Pacific
0	(Taleby Ahvanooey et al., 2022)	Do Dark Web and Cryptocurrencies Empower Cybercriminals?	2022	Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST
0	(Maurushat & Halpin, 2022)	Investigation of Cryptocurrency Enabled and Dependent Crimes	2022	Law, Governance and Technology Series

Source: Harzing Publish or Perish, (2023)

Table 1 shows that from 2017 to 2023 there are only four research teams that write and review topics related to "crypto investment cybercrime". Research conducted by Mackenzie, (2022) provides information that the gray economy of cryptocurrency trading is part of a larger technosocial phenomenon. Here are some key points from the results of the researchers' analysis: (1) the shadow economy of cryptocurrency trading is part of a larger technosocial phenomenon and criminology needs to adapt to the new reality. (2) The article argues that the rise of cryptocurrencies has created new opportunities for criminal activities, including money laundering, fraud, and other types of financial crimes. (3) This article highlights the need for criminology to adapt to the changing landscape of cryptocurrency trading and to develop new approaches to understand and prevent crypto-related crimes. (4) the article also points out that the use of blockchain technology can help prevent fraud and other types of financial crime in the cryptocurrency space, (Carter, 2021; Mason, 2019).

Subsequent research by Morgan, (2022) provides insight into the risks associated with green digital finance and the policies that can be implemented to address them. Here are some of the key findings: (1) Risks associated with green digital finance include hacking and other financial data leaks, inadequate internalization of environmental spillovers, maturity mismatches, unclear green definitions, and regulatory and legal challenges. (2) The environmental impact of digital finance has attracted the attention of researchers before, and the results of this study show that advocating for digitally accessible green finance helps develop green and renewable energy resources and reduce CO2 emissions. (3) Lack of attention to the internal relationship between digital finance and green development is a shortcoming in the literature, and more research is needed to explore the mechanisms Digital finance that affects green development. (4) Policies to address risks associated with green digital finance include greater protection of electronic data, greater emphasis on consumer education, international cooperation, and standards

development. And (5) The huge advantages of digital finance can provide targeted financial support for the low-carbon transformation of companies or the development of green technologies, (Yu et al., 2022; Zhuang et al., 2022).

Another study by Taleby Ahvanooey et al., (2022) shows that the dark web is often associated with criminal activities such as the sale of exploit kits using cryptocurrency as payment. Cybercriminals are drawn to the decentralized nature and anonymity of cryptocurrencies, which makes it difficult for law enforcement to track them. Cryptocurrencies have gained traction as a legitimate form of currency, but they have also been used for cybercrime. Transactions made using cryptocurrency do not require personal information, making it difficult to trace the individual behind it. Carbon Black found that modern cybercriminals are increasingly using the dark web to facilitate cryptocurrency theft on a large scale. Cryptocurrencies have been recognized as ideal vehicles through which cybercriminals can carry out malicious attacks, (Dargahi et al., 2019; Kaur &; Randhawa, 2020). In general, the results of the analysis show that the dark web and cryptocurrencies will indeed trigger the empowerment of cybercriminals. The anonymity and decentralized nature of cryptocurrencies make them attractive to cybercriminals, who can use them to carry out malicious attacks and facilitate cryptocurrency theft. The use of cryptocurrencies for cybercrime highlights the need for strong security measures, user education, and regulatory frameworks to mitigate the risks associated with these crimes, (Taleby Ahvanooey et al., 2022).

Then research conducted by Maurushat & Halpin, (2022) shows that cryptocurrencies are used for various purposes, including laundering dirty money, defrauding victims from funds, and defrauding investors. Cybercriminals are drawn to the decentralized nature and anonymity of cryptocurrencies, which makes it difficult for law enforcement to track them. Cryptocurrencies are used for all kinds of crimes involving the transmission of monetary value, including money laundering, evasion of financial sanctions, bribery, and embezzlement. Cryptocurrency scams are a common type of cybercrime, and they involve actors using information and technology to defraud individuals who have purchased or transacted using cryptocurrency. The use of cryptocurrencies in criminal activities is on the rise, and it is becoming an increasingly popular tool for organized crime groups to carry out illicit activities. Hacking and exploitation are the most common type of crypto-related financial crime, with funds stolen in hacks estimated to be around $4.3 billion by 2022, (Cong et al., 2022; Trozze et al., 2022). In general, the results of the analysis show that cryptocurrencies are used for various types of crimes, and cybercriminals are interested in the decentralized nature and anonymity of cryptocurrencies. Cryptocurrency-enabled and dependent crimes include money laundering, evasion of financial sanctions, (Maurushat &; Halpin, 2022).

Conclusions and Recommendations

From a review of research results found based on searches in the Scopus data base in the 2017-2023 range, 4 articles related to "crypto investment cybercrime" were found. All articles found are two of them are types of non-empirical research or review articles (Mackenzie, 2022)

and (Taleby Ahvanooey et al., 2022), and the other two are reference books related to the material "crypto investment cybercrime", namely (Maurushat &; Halpin, 2022) and (Morgan, 2022).

Thus, based on these findings, it is recommended for further researchers to analyze "crypto investment cybercrime" empirically and then it can be examined in financial sector analysis units such as in the banking sector and other financial institutions. Then the limitation in this study is that the study was only carried out by literature review with a research period in the last five years.

Bibliography

Ammy, Baihaqi., Soemitra, Andri., Nawawi, M, Zuhrinal. (2023). Investing In Cryptocurrency Through the Lens of Islamic Economics. *Proceeding Medan International Conference Economics and Business.*

Bijmans, H. L. J., Booij, T. M., & Doerr, C. (2019). Inadvertently making cyber criminals rich: A comprehensive study of cryptojacking campaigns at internet scale. *Proceedings of the 28th USENIX Security Symposium*.

Blog.avast.com. (2023). *How have cryptocurrencies influenced cybercrime ?* https://blog.avast.com/cryptocurrencies-cybercrime

Carter, E. (2021). Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud. *British Journal of Criminology*. https://doi.org/10.1093/bjc/azaa072

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. *WWW 2013 - Proceedings of the 22nd International Conference on World Wide Web*.

Cong, L., Harvey, C. R., Rabetti, D., & Wu, Z.-Y. (2022). An Anatomy of Crypto-Enabled Cybercrimes. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4188661

Cong, L., Harvey, C. R., Rabetti, D., & Wu, Z.-Y. (2023). An Anatomy of Crypto-Enabled Cybercrimes. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4320582

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*. https://doi.org/10.1007/s11416-019-00338-7

Dorofeeva, V. V., Kaverzina, L. A., Zhmurov, D. V., Krasnova, T. G., & Burakov, V. I. (2019). Cryptocurrencies: Legal and shadow-criminal aspects of turnover. *Russian Journal of Criminology*. https://doi.org/10.17150/2500-4255.2019.13(6).884-894

fultonmay.com. (2023). *What Is Cryptocurrency And How Does It Affect Cyber Security?* https://fultonmay.com/what-is-cryptocurrency-and-how-does-it-affect-cyber-security/

Jafari, S., Vo-Huu, T., Jabiyev, B., Mera, A., & Mirzazade farkhani, R. (2018). Cryptocurrency: A Challenge to Legal System. *SSRN Electronic Journal*.

https://doi.org/10.2139/ssrn.3172489

Kaur, S., & Randhawa, S. (2020). Dark Web: A Web of Crimes. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07143-2

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-319-20550-2_1

Mackenzie, S. (2022). Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial. *The British Journal of Criminology*. https://doi.org/10.1093/bjc/azab118

Mason, D. L. (2019). Fraud: An American History from Barnum to Madoff. *Journal of American History*. https://doi.org/10.1093/jahist/jaz588

Maurushat, A., & Halpin, D. (2022). Investigation of Cryptocurrency Enabled and Dependent Crimes. In *Law, Governance and Technology Series*. https://doi.org/10.1007/978-3-030-88036-1_10

Morgan, P. J. (2022). Assessing the Risks Associated with Green Digital Finance and Policies for Coping with Them. In *Economics, Law, and Institutions in Asia Pacific*. https://doi.org/10.1007/978-981-19-2662-4_3

Rueckert, C. (2019). Cryptocurrencies and fundamental rights. In *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyz004

Sanusi, K. A., & Dickason-koekemoer, Z. (2022). *Cryptocurrency Returns , Cybercrime and Stock Market Volatility : GAS and Regime Switching Approaches*. *12*(6), 52–64.

Simplilearn.com. (2022). *The Growing Relationship Between Cryptocurrency and Cybercrime*. https://www.simplilearn.com/relationship-between-cryptocurrency-and-cybercrime-article

Taleby Ahvanooey, M., Zhu, M. X., Mazurczyk, W., Kilger, M., & Choo, K. K. R. (2022). Do Dark Web and Cryptocurrencies Empower Cybercriminals? *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*. https://doi.org/10.1007/978-3-031-06365-7_17

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. In *Crime Science*. https://doi.org/10.1186/s40163-021-00163-8

Tu, K. V. (2018). Perfecting Bitcoin. *Georgia Law Review*.

Wilson, C. (2019). Cryptocurrencies: The Future of Finance? In *Contemporary Issues in International Political Economy*. https://doi.org/10.1007/978-981-13-6462-4_16

Yu, H., Wei, W., Li, J., & Li, Y. (2022). The impact of green digital finance on energy resources and climate change mitigation in carbon neutrality: Case of 60 economies. *Resources*

Policy. https://doi.org/10.1016/j.resourpol.2022.103116

Zhao, D., & Strotmann, A. (2015). Analysis and Visualization of Citation Networks. *Synthesis Lectures on Visualization*, *3*(2), 1–127. https://doi.org/10.2200/s00688ed1v01y201512vis006

Zhuang, R., Mi, K., Zhi, M., & Zhang, C. (2022). Digital Finance and Green Development: Characteristics, Mechanisms, and Empirical Evidences. *International Journal of Environmental Research and Public Health*. https://doi.org/10.3390/ijerph192416940