Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

BLOCKCHAIN AND BLACK ECONOMY: CRYPTOCURRENCY-RELATED CRIMES AND COUNTERMEASURES[1]

Leo S.F. Lin

Assistant Professor, Department of Criminal Justice, School of Social Sciences, Ming Chuan University, Taiwan (E-mail: leo.lin@mail.mcu.edu.tw)

Article history
Received date : 5-2-2024
Revised date : 5-3-2024
Accepted date : 21-3-2024
Published date : 31-3-2024

To cite this document:
Lin, L. S. F. (2024). Blockchain and black economy: cryptocurrency-related crimes and countermeasures. *Journal of Islamic, Social, Economics and Development (JISED)*, 9 (61), 217 – 227.

Abstract: *This paper proposes an analytical framework based on rational choice theory to examine the opportunities and threats presented by cryptocurrencies and use illicit activities in Taiwan as an example. It discusses the shift from centralized to decentralized financial technology and the utilization of blockchain in various criminal activities such as fraud, exit scams, Ponzi schemes through Initial Coin Offerings (ICOs), and money laundering. The development of virtual currency platforms and exchange companies is explored, with prevalent crime types being organized crime, drug trafficking, fraud, and ransomware. The paper provides case examples of money laundering relating to cryptocurrencies, including online gambling, investment scams, the nexus between cryptocurrency crime and ransomware, and Bitcoin ATMs. Investigative challenges include difficulties in investigating personal off-exchange transactions and enhancing Know Your Customer (KYC) and the Travel Rule in crypto transactions through Financial Institutions (FIs) and Virtual Asset Service Providers (VASPs). Several countermeasures are suggested, such as strategies to increase crime difficulty and cost, enhance regulatory measures for crypto exchange platforms, and promote investigation training and international cooperation. Additionally, the paper underscores the importance of integrating Environmental, Social, and Corporate Governance (ESG) considerations into these countermeasures to address the broader societal and environmental impacts of cryptocurrency-related crimes. This paper contributes to understanding the relationship between blockchain technology, the black economy, and cryptocurrency-related crimes in Taiwan, offering practical countermeasures to combat such illicit activities.*

Keywords: *Blockchain technology, Cryptocurrency crimes, Fraud, Money laundering, ESG*

[1] The earlier version of this paper was presented at the International Conference on Environment, Social and Governance (I-ESG) in Genting Highlands, Pahang Malaysia, 28-30 August, 2023.

Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

Introduction

Technology has revolutionized various industries, and cryptocurrency is no exception. While cryptocurrencies offer exciting opportunities for innovation and financial inclusion, they also present unique challenges in cybercrime. Cryptocurrencies are attractive to criminals because they offer many advantages over traditional fiat currencies, such as anonymity, borderless nature, and ease of use. With new technologies, criminals have found novel ways to exploit vulnerabilities and perpetrate crypto-related crimes. There are at least three evolving faces of threat following blockchain technology advancement.

First, the transition from 1G to 5G networks has significantly increased data transmission speed and efficiency. For criminals involved in crypto-related crimes, 5G networks have opened up new avenues for cyberattacks. With faster and more reliable networks, criminals can execute large-scale data theft, launch Distributed Denial of Service (DDoS) attacks, or exploit vulnerabilities in cryptocurrency exchanges more effectively. The quick data transfer capabilities of 5G networks enable criminals to execute their schemes quickly and efficiently, making detection and prevention more challenging for law enforcement.

Second, decentralized financial technology (DeFi) has revolutionized the financial landscape, offering various financial services without intermediaries. However, this advancement also brings new threats to the crypto ecosystem. Criminals can exploit the lack of centralized oversight and regulations on DeFi platforms to conduct illicit activities such as money laundering, fraud, and market manipulation. DeFi platforms often lack robust KYC (Know Your Customer) and AML (Anti-Money Laundering) measures, making it easier for criminals to evade detection while engaging in unlawful financial activities.

Third, the borderless nature of cryptocurrencies has made international transactions faster and more accessible. However, this feature has also made it easier for criminals to engage in cross-border crimes without geographical restrictions. Criminals can transfer funds globally without traditional banking channels, making monitoring and tracking suspicious transactions challenging for law enforcement agencies. The ease of moving money across borders using cryptocurrencies has facilitated money laundering, terrorist financing, and other illegal activities globally.

This paper asks two research questions: How can we perceive cryptocurrency-related crimes from a rational choice theoretical perspective? Second, what can we draw from the theory in the case of Taiwan, and what are the implications for countermeasures? To answer the above questions, this paper adopts a rational choice theoretical model proposed by Fichtenkamm et al. (2022) to analyze cryptocurrency-related crimes (Fichtenkamm, Burch, & Burch, 2022). Based on the proposed model, this paper analyses Taiwan as a case study and provides policy implications. This paper makes contributions by examining the impact of blockchain technological advancements from a rational choice theoretical perspective on the landscape of crypto-related crimes, particularly in the case of Taiwan.

Literature Review

Several studies have examined the use of cryptocurrencies in money laundering. Masciandaro and Barone (2018) present a novel dynamic setting to compare old – usury – and new – cryptocurrency – money laundering techniques and use it for calibration to shed light on their relative role as an effective device for criminal organizations to clean their illegal revenues. The calibration compares the leverage effect on the overall capital owned by the criminal

Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

organizations triggered by the two money laundering techniques (Masciandaro & Barone, 2018). Albrecht et al. (2019) found that cryptocurrencies are often used to launder the proceeds of crime, such as drug trafficking and ransomware attacks. They argue that the anonymity and borderless nature of cryptocurrencies make them ideal for money laundering (Albrecht, Duffin, Hawkins, & Morales Rocha, 2019). Brenig and Müller (2015) also found that cryptocurrencies are attractive to criminals because they offer several benefits, such as the ability to launder large sums of money quickly and easily. They argue that cryptocurrencies will likely increase in use (Brenig & Müller, 2015). Desmond, Lacey, and Salmon (2019) explore the complex socio-technical system of crypto laundering and find that the systems thinking perspective is lacking in previous research, hindering a comprehensive understanding of crypto laundering processes and risk assessment (Desmond, Lacey, & Salmon, 2019). Wronka (2022) examines a comprehensive analysis of the phenomenon and explores appropriate preventative measures in response to the increasing use of cryptocurrencies in money laundering schemes. The study aims to assess cryptocurrencies' relevance to money laundering risk within the market, shedding light on prevalent money laundering techniques and recognizable patterns of abuse (Wronka, 2022).

In addition to money laundering, cryptocurrencies are used in crypto markets and online marketplaces for illicit goods and services. Cryptomarkets offer many advantages to criminals, such as the ability to operate anonymously and avoid law enforcement. Janze (2017) examines the co-evolution of Bitcoin and darknet markets. Using Rational Choice Theory and darknet market design, the study reveals a dynamic relationship between cryptocurrency transactions and sales on darknet markets, with escrow mechanisms playing a vital role (Janze, 2017). Tsuchiya and Hiramoto (2021) concluded that crypto markets are most active at night in European countries, the US, and Canada. They also found more transactions on Mondays, Tuesdays, and Wednesdays and fewer on Saturdays and Sundays. This suggests that the retail drug trade accounts for much of the crypto market activity (Tsuchiya & Hiramoto, 2021). Hiramoto and Tsuchiya (2023) found that illicit drugs are a driving force for crypto market leadership. They argue that crypto markets are popular since they offer a safe and anonymous way to buy and sell illicit drugs (Hiramoto & Tsuchiya, 2023). In case studies, Valdez's (2020) critical analysis examines the absence of cryptocurrency regulations in Chile and proposes potential benefits Chile could derive from adopting Estonia's proactive stance towards cryptocurrencies. The analysis also evaluates additional factors that could influence Estonia's decline and Chile's rise in economic crimes, including money laundering (Valdez, 2020). These studies suggest that using cryptocurrencies in money laundering and crypto markets is a growing concern.

These studies underscore the growing concern regarding using cryptocurrencies in money laundering and the crypto markets. Cryptocurrencies' unique features that attract criminals require vigilance from law enforcement agencies and regulatory bodies. Understanding the dynamics of cryptocurrency-related crimes can help develop effective strategies to combat such illicit activities and ensure the integrity and security of the financial ecosystem. This paper also demonstrates the importance of government officials and stakeholders being equipped with the necessary knowledge and tools to combat cryptocurrency-related crimes.

Method

This paper employs qualitative comparative analysis and integrates it with rational choice theory. Qualitative comparative analysis (QCA) provides a systematic approach to case-oriented analysis (Lucas & Szatrowski, 2014). The author collected existing research results on

Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

cryptocurrency-related crime and summarized and sorted out the existing research to identify blank areas of research and determine our research focus and direction. In addition, this author compares the different cryptocurrency-related crimes in Taiwan horizontally and vertically. Therefore, the prominent schemes of cryptocurrency-related crimes that cyber criminals use are identified and analyzed. Data were collected from Taiwan government websites, official publications, informal interviews with practitioners, and grey literature.

Rational Choice theory can be used to explain criminal behavior (Cornish & Clarke, 2002, 2014). This theory posits that criminals make decisions before committing a crime, considering various factors such as time, cognitive ability, and available information (Jennings & Beaudry-Cyr, 2014). These decisions are based on a cost-benefit analysis, where the perceived benefits of the criminal act outweigh the potential consequences.[2] Rational choice theory constitutes a cognitive decision-making process (see Figure 1). In cybersecurity, decision-makers actively acquire information, intentionally and unintentionally, and act based on how this information shapes their interests and beliefs concerning cybersecurity. The nature of these interests is subjective, with some decision-makers prioritizing security while others emphasize cost or productivity. Additionally, the information gathered significantly influences whether the decision-maker perceives their actions as conducive to achieving the desired change, an aspect molded by their beliefs concerning opportunities and outcomes. Consequently, if decision-makers perceive that their actions will not yield the desired outcome, they will likely refrain from making the particular decision.

Upon reaching a decision, the decision-maker acts, and an outcome follows. However, it is essential to acknowledge that the actual outcome may deviate from initial expectations due to the influence of the environment. This can introduce alterations in the relationship between actions and outcomes. Therefore, it is important to understand the environment before deciding, as it can help anticipate the potential outcomes. It is also important to consider the potential consequences of the decision-maker's actions.

Furthermore, it is important to recognize that real-world scenarios are significantly more intricate than theoretical models. This complexity stems from the presence of multiple decision-makers, both within and beyond organizational boundaries. Managers' actions, for instance, provide information to employees, who can then adjust their interests and beliefs based on this newfound information, leading to consequent actions. In turn, employees' actions become informational cues for cybercriminals, prompting them to adapt their interests and beliefs and undertake their actions. Cybersecurity decision-making exists within an interconnected and dynamic framework where various actors engage in reciprocal exchanges of information and actions.

[2] See https://www.crimeprevention.nsw.gov.au/Documents/rational_choice_factsheet_nov2014.pdf

Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

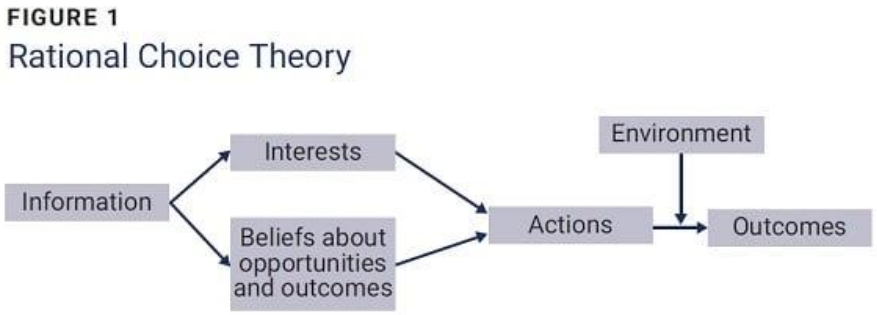

Figure 1: Rational Choice Theory

Source:*https://www.isaca.org/-/media/images/isacadp/project/isaca/articles/journal/2022/volume-2/rational_choice-theory-figure1.jpg*

Blockchain Rational Choice Environment

Blockchain is a distributed ledger technology that can be used to record transactions securely and transparently. This can revolutionize our decisions, providing us access to more information and allowing us to coordinate our actions more effectively. In a blockchain environment, rational-choice decision-makers take action and gather information about each other and the details of their environment. This creates an environment rich with information, where the actions of one group can significantly alter the outcomes and actions of other groups. A final consideration is how the environment can change the information people receive, alter their interests, and limit their beliefs about how much they can influence outcomes with their decisions.

The following are four elements of rational-choice decision-making in a blockchain environment:

- Information: Information is the first item to consider when making rational decisions in a complex environment. This includes information about the environment, other decision-makers, and the potential outcomes of different actions.
- Interests: Interests are the things we value and want to achieve. They can be influenced by information, as well as by our values and beliefs.
- Beliefs About Opportunities: Beliefs about the opportunities and outcomes of different actions can also influence our decision-making. For example, if we believe that a particular action is likely to lead to a desired outcome, we are more likely to take that action.
- Actions: The final element of rational-choice decision-making is actions. This is the process of taking steps to achieve our desired outcomes.

The four elements of rational choice decision-making are interrelated. For example, our beliefs about the opportunities and outcomes of different actions can be influenced by the information that we have. Similarly, our actions can also influence the information that we receive and the beliefs that we hold.

Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

Results

Blockchain Rational Choice Environment for Cybercriminals: Taiwan as an Example

Based on the rational choice theory, the following reflects the decision-making process for cyber criminals in Taiwan:

Regarding information, cybercriminals in Taiwan perceive the blockchain environment as a double-edged sword for conducting cyber-enabled crimes, acknowledging its transparency and data immutability, which can potentially expose their activities and transactions. However, they also recognize the opportunities provided by blockchain's decentralized nature to conceal their identities and evade detection effectively in cyber-enabled crimes. Moreover, they know the blockchain environment holds valuable information and access to digital assets and cryptocurrencies, making them attractive targets for cyber-dependent crimes.

Concerning interests, in Taiwan, cybercriminals engaged in cyber-enabled crimes may focus on targeting blockchain platforms and exchanges to steal valuable virtual assets and cryptocurrencies, driven by the potential financial gains these thefts could bring. For cyber-dependent crimes, they might be interested in launching ransomware attacks on individuals or organizations within the blockchain space, demanding cryptocurrencies as ransom payments, thus advancing their monetary interests. Additionally, their interests may extend to exploring blockchain-based malware and hacking tools to exploit weaknesses in blockchain networks and digital wallets, enhancing their capabilities in cyber-enabled and cyber-dependent crimes.

In beliefs about opportunities, cybercriminals in Taiwan perceive the blockchain environment as an opportunity to conduct cyber-enabled crimes with a certain level of anonymity and pseudonymity, reducing the risk of their identification and apprehension. They firmly believe that hacking and compromising blockchain projects or ICOs can lead to significant financial gains without leaving a clear trail for law enforcement to follow, driving their motivation to engage in cyber-enabled and cyber-dependent crimes. Furthermore, they believe that targeting blockchain-related assets and platforms offers unique financial rewards and asset theft opportunities, further incentivizing their criminal pursuits.

Finally, about action, the information-rich environment of the blockchain motivates cybercriminals in Taiwan to develop sophisticated attack strategies and advanced malware targeting blockchain networks and users, seeking to exploit vulnerabilities for their benefit in both cyber-enabled and cyber-dependent crimes. They actively take action to exploit flaws in smart contracts, leading to financial losses for victims and tarnishing the reputation of blockchain projects in cyber-enabled crimes. Moreover, cybercriminals collaborate and share information through dark web forums, enabling coordinated attacks and the exchange of knowledge and experiences, contributing to the evolution of their tactics in both cyber-enabled and cyber-dependent crimes.

Main types of cryptocurrency-related crimes in Taiwan

According to the officials in the Criminal Investigation Bureau in Taiwan, three main types of cryptocurrency-related crimes in Taiwan include fraud, money laundering, online gambling,

Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

underground wire transfer scams, and ransomware.[3] Fraud remains a significant concern in Taiwan's cryptocurrency landscape, with fraudsters employing various deceptive tactics to defraud individuals of their cryptocurrencies. Phishing, phone, and online scams are common methods criminals use to trick victims into transferring funds to fraudulent wallets. To address this issue, law enforcement agencies are actively investigating and prosecuting fraudsters while conducting public awareness campaigns to educate citizens about common scams and promoting caution when engaging in cryptocurrency transactions.

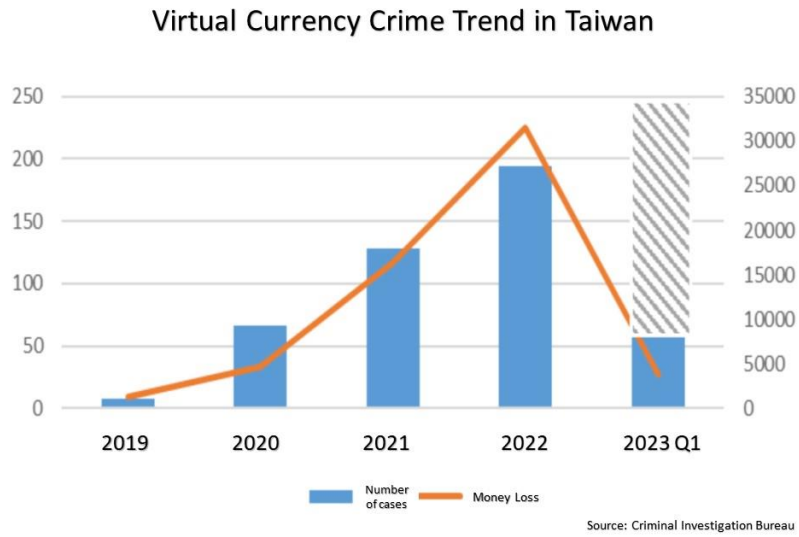

Figure 1: Virtual Currency Crime Trend in Taiwan

Source: *Criminal Investigation Bureau*

Third-party money laundering is another prevalent cryptocurrency-related crime in Taiwan. Criminals utilize shell companies and other intermediaries to obscure the true origin of funds, facilitating illicit financial transactions. In response, authorities are enhancing Anti-Money Laundering (AML) regulations, conducting thorough due diligence on cryptocurrency service providers, and implementing Know Your Transaction (KYT) tools to identify and prevent third-party money laundering activities.

Despite its illegality in Taiwan, online gambling continues to be a persistent problem. Criminal operators run unlicensed gambling websites, targeting Taiwanese citizens and using cryptocurrencies as a means of payment to evade traditional financial scrutiny. To tackle this issue, Taiwanese authorities are actively identifying and shutting down illegal gambling platforms, seizing assets obtained through such activities, and conducting public awareness campaigns to educate the population about the dangers of engaging in unregulated online gambling using cryptocurrencies.

Underground wire transfer scams pose another threat, with criminals exploiting fake websites and deceptive techniques to trick individuals into transferring money, including cryptocurrencies, to fraudulent accounts. These scams mainly target individuals seeking services or goods online, resulting in substantial financial losses. Authorities are working

[3] Closed-door presentation at a cryptocurrency crimes investigation conference in Taipei on June 17, 2023, hosted by the Taiwan High Prosecutors Office.

Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

diligently to investigate and apprehend scam operators, collaborating with financial institutions to detect suspicious transactions, and promoting public awareness to safeguard against common scam tactics.

Ransomware attacks have also become a prominent issue in Taiwan, where cybercriminals encrypt victims' computer files and demand ransom payments, typically in cryptocurrencies, to restore access. Such attacks can cause severe disruptions and financial losses to individuals and organizations. To address this cyber threat, Taiwanese authorities are engaging in international cooperation with cybersecurity agencies, advocating for cybersecurity best practices and raising awareness about the importance of regular data backups to mitigate the impact of ransomware incidents.

Discussion and Recommendation

Discussion

Lin and Nomikos (2018) highlight key challenges cybercriminals pose in East Asia, especially in Taiwan. Firstly, the issue of legal jurisdiction remains critical, as the transnational nature of cybercrime necessitates harmonized laws and enhanced cooperation among states. Secondly, political tensions in the region hinder cooperation between countries. Lastly, there is an economic and social challenge related to the digital divide (Lin & Nomikos, 2018). Broadhurst (2006a) notes the growing divide between nation-states and emphasizes the essential role of advanced IT-based economies in bridging this gap (Broadhurst, 2006). The prevalence of cryptocurrency-related crimes in the blockchain environment has been a growing concern in recent years. Blockchain technology's decentralized and pseudonymous nature provides an attractive landscape for cybercriminals to exploit various opportunities and execute illicit activities. Rational choice theory suggests that decision-makers behaviors are shaped by their interests and beliefs. In cryptocurrency-related crimes, decision-makers in organizations and governments must know blockchain technology's potential risks and vulnerabilities. However, the lack of information about cybersecurity threats and best practices can lead decision-makers to underestimate the severity of these crimes and neglect investing in robust security measures. This lack of focus on security may shift interests away from safeguarding blockchain assets and data, leaving organizations vulnerable to cyberattacks.

During the COVID-19 pandemic, decision-makers faced unprecedented challenges, such as transitioning to remote work and adopting new digital platforms. This sudden shift in the work environment might have contributed to a lack of information and awareness about potential cyber threats. Cybercriminals, taking advantage of the situation, could have increased attacks on soft targets within the blockchain environment, including humans, software, and hardware. The increased frequency and sophistication of cyberattacks during the pandemic highlight the importance of decision-makers being proactive in enhancing cybersecurity measures.

The convergence of interests and beliefs about the pandemic's impact on decision-makers actions is also evident in the blockchain environment. The pandemic's disruptions led decision-makers to prioritize temporary solutions that were perceived as sufficient, potentially compromising the security and integrity of blockchain systems. This shift in behavior provided opportunities for cybercriminals to exploit vulnerabilities and execute cryptocurrency-related crimes.

Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

Cryptocurrency-related crimes pose increasing challenges to the security and integrity of the financial landscape in Taiwan. A comprehensive and multi-faceted approach is required to combat these illicit activities and enhance security measures.

Firstly, to fortify transaction security, it is essential to implement robust measures such as multi-factor authentication, additional verification steps, and the utilization of smart contract technology. These measures ensure transparency and irreversibility of transactions, reducing the potential for fraudulent activities and unauthorized access to digital assets. By strengthening the transactional framework, the cryptocurrency community can deter criminal elements seeking to exploit vulnerabilities in transactional processes.

Secondly, reducing anonymity is critical in curbing cryptocurrency-related crimes. Strengthening KYC protocols for cryptocurrency exchanges and platforms can provide a clear record of user identities, making it harder for criminals to operate undetected. Mandating stricter KYC procedures, exchanges, and platforms can discourage illicit activities, as perpetrators are less likely to risk exposing their identities in a more transparent and accountable environment.

Thirdly, enhanced monitoring and data analysis are essential in detecting and addressing suspicious activities promptly. By deploying advanced tools, regulatory authorities, and cryptocurrency service providers can swiftly identify patterns indicative of potentially criminal behavior, enabling timely intervention to prevent significant harm. Proactive data analysis contributes to early detection and reduces the impact of illicit transactions on the cryptocurrency ecosystem.

Efficient collaborations between law enforcement agencies and cryptocurrency platforms effectively combat criminal activities. By promoting better communication and information sharing, authorities can respond swiftly to illegal transactions and illicit schemes. This partnership can identify and prosecute criminals engaged in cryptocurrency-related crimes, acting as a strong deterrent for potential wrongdoers.

Finally, raising awareness among cryptocurrency users about associated risks and vulnerabilities is crucial. Educational campaigns should emphasize best practices for securing digital wallets and provide insights into common scams and phishing attempts. By empowering users with knowledge, they can better protect themselves from falling victim to cryptocurrency-related crimes and contribute to a more secure environment.

Recommendation: ESG Consideration

Integrating Environmental, Social, and Corporate Governance (ESG) considerations into these policy recommendations is paramount for fostering a more sustainable and responsible cryptocurrency ecosystem.

From an environmental perspective, the energy-intensive nature of cryptocurrency mining has raised concerns about its carbon footprint and contribution to climate change. Decision-makers should prioritize adopting eco-friendly mining practices, such as transitioning to renewable energy sources or implementing energy-efficient mining technologies. Additionally, promoting transparency regarding the environmental impact of cryptocurrency operations can encourage industry players to minimize their ecological footprint and invest in green initiatives.

Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

On the social front, cryptocurrency-related crimes can exacerbate social inequalities and disproportionately impact marginalized communities. Decision-makers should prioritize initiatives to promote financial inclusion and accessibility, ensuring that vulnerable populations have equitable access to blockchain technology and its benefits. Moreover, addressing money laundering and fraud can help protect consumers and investors, fostering trust and confidence in the cryptocurrency market.

From a corporate governance perspective, enhancing transparency, accountability, and ethical behavior within the cryptocurrency industry is crucial for building investor confidence and regulatory compliance. Decision-makers should advocate for robust governance frameworks prioritizing ethical business practices, anti-corruption measures, and stakeholder engagement. Implementing stringent KYC/AML protocols and adhering to regulatory standards can help mitigate risks associated with illicit activities and promote a culture of compliance and integrity within the industry.

Furthermore, decision-makers should consider their actions and policies' long-term societal and environmental impacts, striving to create a cryptocurrency ecosystem that aligns with broader sustainable development goals. By integrating ESG principles into their decision-making processes and regulatory frameworks, stakeholders can build a more resilient, responsible, and socially conscious cryptocurrency ecosystem that benefits investors and society.

Conclusion

The ever-evolving technological landscape, particularly cryptocurrency-related crimes, presents opportunities and challenges. The advancement of blockchain technology has opened new avenues for cybercriminals to exploit vulnerabilities and execute illicit activities. Understanding the decision-making process of cybercriminals through the lens of rational choice theory provides valuable insights into their interests, beliefs, and actions within the blockchain environment.

Policymakers in Taiwan and other jurisdictions must proactively address the rising threats posed by cryptocurrency-related crimes. Implementing measures such as enhancing transaction security, reducing anonymity through stricter KYC protocols, and deploying advanced monitoring and data analysis tools is crucial in fortifying the cryptocurrency ecosystem against criminal elements. Furthermore, collaborations between law enforcement agencies and cryptocurrency platforms, along with educational campaigns for users, are vital components of a comprehensive approach to combating cryptocurrency-related crimes effectively.

In conclusion, integrating Environmental, Social, and Corporate Governance (ESG) considerations into these efforts is imperative for fostering a more sustainable and responsible cryptocurrency ecosystem. Stakeholders can build a cryptocurrency ecosystem that aligns with broader sustainable development goals by prioritizing eco-friendly mining practices, promoting financial inclusion, and enhancing transparency and ethical behavior within the industry.

Future research in the field of cryptocurrency-related crimes in Taiwan should focus on exploring how technological advancements impact cybercrime, evaluating the effectiveness of regulatory frameworks and compliance measures, understanding the role of cryptocurrency exchanges and platforms in facilitating illicit activities and studying the economics of cryptocurrency crime. Additionally, investigating the use of anonymization services, understanding user behavior and awareness, fostering international cooperation, and examining

Volume: 9 Issues: 61 [March, 2024] pp. 217 - 227
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096120

successful public-private partnerships can further enhance the knowledge and strategies needed to combat cryptocurrency-related crimes effectively.

References

Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control, 22*(2), 210-216.

Brenig, C., & Müller, G. (2015). Economic analysis of cryptocurrency backed money laundering.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management, 29*(3), 408-433.

Cornish, D. B., & Clarke, R. V. (2002). Crime as a rational choice. *Criminological theories: Bridging the past to the future*, 77-96.

Cornish, D. B., & Clarke, R. V. (2014). The reasoning criminal: Rational choice perspectives on offending.

Desmond, D. B., Lacey, D., & Salmon, P. (2019). Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. *Journal of Money Laundering Control, 22*(3), 480-497.

Fichtenkamm, M., Burch, G. F., & Burch, J. (2022). Cybersecurity in a COVID-19 world: Insights on how decisions are made. *ISACA Journal, 2*(1), 1-11.

Hiramoto, N., & Tsuchiya, Y. (2023). Are Illicit Drugs a Driving Force for Cryptomarket Leadership? *Journal of Drug Issues, 53*(3), 451-474.

Janze, C. (2017). Are cryptocurrencies criminals best friends? Examining the co-evolution of bitcoin and darknet markets.

Jennings, W. G., & Beaudry-Cyr, M. (2014). Rational choice. *Encyclopedia of Theoretical Criminology. Malden: MA: Wiley-Blackwell*.

Lin, L. S., & Nomikos, J. (2018). Cybercrime in East and Southeast Asia: The Case of Taiwan *Asia-Pacific Security Challenges* (pp. 65-84): Springer.

Lucas, S. R., & Szatrowski, A. (2014). Qualitative comparative analysis in critical perspective. *Sociological Methodology, 44*(1), 1-79.

Masciandaro, D., & Barone, R. (2018). Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques. *Crime and Alternative Money Laundering Techniques (December 2018). BAFFI CAREFIN Centre Research Paper*(2018-101).

Tsuchiya, Y., & Hiramoto, N. (2021). Dark web in the dark: Investigating when transactions take place on cryptomarkets. *Forensic Science International: Digital Investigation, 36*, 301093.

Valdez, M. (2020). Estonia's success and Chile's failure. *DESC-Direito, Economia e Sociedade Contemporânea, 3*(1), 131-152.

Wronka, C. (2022). Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control, 25*(1), 79-94.