Understanding Criminogenic Features: Case Studies of Cryptocurrencies Based Financial Crimes

Abstract

The primary objective of this paper is to comprehensively examine the intricate relationship between cryptocurrency and criminal enterprises, shedding light on the methods, mechanisms, and implications of cryptocurrency use in various financial crimes. Based on the theory of planned behaviour, this paper conducts a thematic analysis and criminal investigation on 51 cryptocurrency-related financial crime cases to identify criminogenic features of cryptocurrencies, key tools, and features of cryptocurrency-related financial crimes. Based on the case study, policy-changing recommendations and big-data analytics tools are proposed for law enforcement agencies to prevent and combat cryptocurrency crimes. The criminal investigation indicates that the decentralisation, pseudo-anonymity, and borderless nature of cryptocurrencies enable cross-border financial flows and make transaction tracking a complex challenge. Popularity and market capitalisation used to play a dominant role in criminals' choice of cryptocurrency as Bitcoin was associated with most cryptocurrency-related crimes before 2019. Recently, an increasing number of other cryptocurrencies, such as privacy coins and stablecoins, have been utilised for financial crimes, while cryptocurrencies have also become an essential source of terrorist financing. Therefore, it is important and urgent for cryptocurrency exchange companies, mixing services, and wallet providers to implement strict anti-money laundering and know-your-customer measures to help combat cryptocurrency-related crimes and create a sustainable future for cryptocurrencies. Due to the open access to cryptocurrency transaction data on the blockchain, powerful big-data analytics tools can help law enforcement departments proactively detect cryptocurrency-related crimes and reduce terrorism' threats to domestic and international security.

Keywords: Cryptocurrencies; Financial crime; Case study; Thematic analysis; Criminal investigation; Crime prevention.

1. Introduction

Cryptocurrencies are one of the most significant innovations stemming from blockchain technology (Joo *et al.*, 2020). They are decentralised digital currencies that safeguard exchange by using cryptography (Ku-Mahamud *et al.*, 2019). Thus, they substitute traditional money by removing the control and the need of third parties as they perform their functions online on the blockchain (Tredinnick, 2019). Bitcoin was the first cryptocurrency ever created in 2009 and continues to be the biggest in terms of capitalisation, followed by Ether used in the Ethereum blockchain. Nonetheless, different cryptocurrencies have been created since then to fulfill a plethora of purposes. Their use and popularity have grown exponentially over the years, and some countries have started welcoming their use for everyday transactions and innovation purposes. The popularity of cryptocurrencies results from the advantages they have generated. Firstly, they have made higher transaction speeds and lower transaction fees due to the elimination of third-party intermediaries. Further, they ensured financial inclusion for those who had no access to traditional financial services. Finally, although they are extremely volatile, the fact that there is a limited supply of cryptocurrencies allows for a layer of built-in inflation protection that traditional fiat money does not have.

Notwithstanding, cryptocurrencies have presented new challenges for governments, mainly due to their increased usage in carrying out criminal activities. The most prominent issue is that cryptocurrencies are being used to carry out money laundering activities across different countries. Further, these digital currencies are being exploited for illicit trading and the sale of drugs and other illegal material, especially through the dark web and black market. US and European authorities have shut down several darknet markets[1] throughout the years. Nonetheless, enforcement measures by authorities always fall short, with new markets being opened right after others are shut down. Finally, criminals are demanding payments in cryptocurrency to restore victims' computer networks after carrying out ransomware attacks on them.

Therefore, the primary aim of this study is to conduct criminal investigations and examine the criminogenic features of cryptocurrencies and their potential exploitation to finance criminal enterprises. To achieve this aim, this research collects 51 cryptocurrency-related financial crime cases from a range of academic and industrial resources and adopts the theory of planned behaviour and thematic analysis to answer the following questions.

- What are the criminogenic features of cryptocurrencies?
- What tools and methods are currently used to facilitate cryptocurrency crime?
- What policy-changing recommendations can be made to help regulatory bodies prevent cryptocurrency-related financial crimes?
- What tools can be developed to enable law enforcement bodies to conduct criminal investigations and combat cryptocurrency crimes?

2. Literature Review

The literature review consists of two parts. The first part presents the previous research works regarding cryptocurrency and financial crime, while the second part introduces the different approaches to exploiting cryptocurrencies for various criminal activities.

[1] Darknet market: websites where individuals can anonymously use cryptocurrency to buy and sell illicit goods and services.

2.1 Previous works

An early study by Brown (2016) pointed out that Bitcoin presented a large partial of the purchase and processing of illicit goods and unsavoury services, while most cybercriminals and darknet entrepreneurs preferred Bitcoin. Trozze et al. (2022) conducted a scoping review of grey literature and academic research on cryptocurrency fraud, as well as an expert consensus exercise on preventing cryptocurrency crimes. They identified 47 categories of cryptocurrency fraud and Ponzi schemes that are the most discussed in the literature. Teichmann et al. (2020) conducted interview studies with 18 international compliance experts and 10 presumed providers of illegal financial services. They suggested that the Liechtenstein Blockchain Act can serve as a benchmark for legislators to regulate blockchain more effectively. Trozze et al. (2023) explored 37 resolved cryptocurrency-based financial crime cases in the USA and found out that a case will be less likely to be resolved by dismissal, trial summary, and default judgment if they are committed by individual defendants only and using only one cryptocurrency other than Bitcoin. Kutera (2022) conducted a systematic literature review regarding cryptocurrency-based financial frauds. He found that although cryptocurrency-related financial fraud is developing quite intensively, only a little scientific research has been conducted and most literature focused on the Ponzi scheme. Nolasco and Vaughn (2019) examined cryptocurrency cases decided in the U.S. District and Circuit Courts to examine whether Gottschalk's convenience theory of white-collar crime applies to cryptocurrency crime litigation. They found that typical cryptocurrency-related financial crimes include operating unlicensed money transmitting and money service businesses, commodity fraud, bitcoin scams, and securities fraud. Thowseaf (2023) conducted a scoping study regarding bitcoin mixing services and exchanges and revealed that the study of cryptocurrency-related crimes lack an examination of future concerns and circumstances. Ndiaye et al. (2021) examined the behaviour of malicious contracts such as criminal and vulnerable smart contracts and proposed a framework for detecting malicious smart contracts based on an intrusion detection system. Therefore, most of the previous studies mainly used systematic literature reviews or scoping reviews to identify the criminogenic features of cryptocurrencies and different types of cryptocurrency-related financial crimes. However, there is a lack of studies to reveal the current trend of cryptocurrency crimes; the relationship between criminogenic features of cryptocurrency and types of financial crimes; as well as the approaches used to facilitate different types of cryptocurrency-related financial crimes.

2.2 Approaches to exploiting cryptocurrencies for criminal activities.

The most widespread types of cryptocurrency-related financial crimes include money laundering, darknet, financial frauds, ransomware attacks, and terrorism financing. Cryptocurrency-related financial crimes are relatively new in scientific research and most of the previous literature focused on explaining the purposes and features of different types of financial crimes.

2.2.1 Money Laundering

Money laundering specialists are integrating cryptocurrencies as part of their services because cryptocurrencies are particularly useful in the placement and layering stages of money laundering (Almaqableh *et al.*, 2023; Dudani *et al.*, 2023; Wronka, 2023; Collins, 2022; Silfversten *et al.*, 2020; Dyntu and Dykyi, 2018; Foley et al., 2018; Leuprecht et al., 2023). The Pseudo-anonymity feature makes cryptocurrency easier to enter the proceeds of crime into the legitimate economy while its virtual nature puts cryptocurrency beyond the control of current jurisdiction. Through international transfers, exchanging cryptocurrencies into fiat currencies, trade, and investments, the connection between original crime and illicit cryptocurrencies will be lost. The most common platforms used for cryptocurrency-related financial crime include cryptocurrency exchange companies (Matakovic, 2022; Raza and Raza, 2021), online gambling services (McCord *et al.*, 2022; Fanusie and Robinson, 2018; Brown, 2016), and mixing services (Cong *et al.*, 2023).

2.2.2 Darknet

Darknet is a network that can only be accessed anonymously (Butler, 2019; Barratt *et al.*, 2016). Most darknet markets have now become crypto markets where customers can purchase illegal goods and services, such as drugs, weapons, exotic animals, fake identification cards, and illegal pornography (Europol 2021; Kethineni and Cao, 2020). The first and biggest darknet marketplace was the Silk Road, where all transactions were made using Bitcoin (Sàndor and Fehér, 2019; Dyntu and Dykyi, 2018). Just one year after it began operation, the market revenue of Silk Road reached $15 million per year. Although Silk Road was discovered by the FBI and shut down in 2012, several other illegal markets came about, such as AlphaBay and Russia-based Hydra Marketplace (Foley *et al.*, 2018).

2.2.3 Financial fraud

Fraud involving cryptocurrency has become a growing concern (Trozze *et al.*, 2022). Between 2017 and 2018, a 190% increase in losses for victims of cryptocurrency-related scams was reported in Australia only. Matakovic (2022) highlighted that $4.3 billion was lost in cryptocurrency frauds in 2019, only to rise to between $7 and $10 billion in 2021 and 2022 (Cong *et al.*, 2023; McCord *et al.*, 2022). The typical cryptocurrency-related frauds include posing as experienced brokers and using manipulated software to show victims fake gains and motivate victims to invest in their cryptocurrency (Ali, 2022); hacking social media accounts of influential people to scam victims into sending cryptocurrencies; as well as manipulating cryptocurrency market (i.e., pumping the value of minor cryptocurrencies to encourage victims to buy them, followed by a collapse phase).

2.2.4 Ransomware Attacks

Ransomware attacks are a hacking method by which attackers insert a malicious computer programme into the victim's computer or network to encrypt their files (Black, 2022; The Police Foundation, 2021). For example, phishing fraud to collect confidential data or steal cryptocurrencies. Although ransomware attacks existed before the rise of cryptocurrencies, the Pseudo-anonymous and hard-to-trace nature of cryptocurrencies is facilitating ransomware and malware attacks.

2.2.5 Terrorism Financing and Organised Crime

Some terrorist groups have turned to cryptocurrencies for their funding activities (Leuprecht *et al.* (2023), Wronka (2023), Matakovic (2022), Sàndor and Fehér (2019) and Foley *et al.* (2018)). For instance, they are raising donations in Bitcoin through social media platforms. Moreover, by targeting American victims, a terrorist group spread across Russia and Ukraine has collected over $16 million in Bitcoin. Notwithstanding, no piece of literature focuses on Mafias (Pieroni, 2018).

3. Study design

The overall objective of this paper is to fill the existing gap concerning the relationship between the criminogenic features of cryptocurrencies and different types of financial crimes. Thematic analysis and criminal investigation are conducted on 51 cryptocurrency-related financial crime cases. Data collection includes the type of financial crimes, how the financial crime was perpetrated, the type of platform which was attacked, the type of cryptocurrency, the total amount of cryptocurrencies utilised in financial crime, whether the financial crime was conducted cross-border, who identified the financial crime, and the perpetrators of the cryptocurrency crime of each case study. Data is collected from a wide range of sources, including journal papers, newsletters, and criminal reports. Based on the theory of planned behaviour, the attitudes, subject norms, and perceived behaviour control towards conducting these 51 cryptocurrency-based financial crimes are investigated.

Table 1. Summary of 51 case studies (Source: Authors' won creation)

Source	Financial crime	How crime perpetrated	The platform that is involved	Crypto involved	Amount	Cross-border?	Who identified crime?	Perpetrator(s)	Year
Dudani *et al.* (2023)	Money laundering	Virtual game currency to purchase in-game items using money gained from carding activities and then sold to other players for "clean money".	Virtual game	WebMoney	$18,000	Yes, money laundered outside the US.	FBI	Singular individual	2011
Raza and Raza (2021)	Money laundering	Convert money gained from Colombian drug cartels into the cryptocurrency market	Cryptocurrency exchange platforms: Binance, Kraken and BitMEX	Unknown	€350 million	Yes	Polish police	Polish individual	2019
Raza and Raza (2021)	Money laundering	Mixing cryptocurrency from the darknet into the cryptocurrency market	Mixing services provided by DropBit	Coin Ninja	Equivalent to over 354,468 BTC, approx. $311 million	Yes	US police forces	CEO of Coin Ninja and DropBit cryptocurrency wallet	2020
Cong *et al.* (2023), Kethineni and Cao (2020) and Sàndor and Fehér (2019)	Darknet transactions	Illegal marketplaces opened on the dark web where drugs, weapons, exotic animals, fake IDs, illegal pornography, and many other illegal items are purchased.	Darknet: Silk Road	Bitcoin	$15 million	Yes	FBI	Ross Ulbricht, creator of Silk Road	2014
Europol (2021)	Fraud	Perpetrators posed as experienced brokers, used manipulated software to show victims fake gains and motivate them into investing in their cryptocurrency	Cryptocurrency trading platform	Bitcoin	€30 million	Yes, victims across Europe	Europol	A criminal group	2020
Tsuchiya and Hiramoto (2021)	Money laundering	Hackers stole cryptocurrencies from Coincheck Exchange, and swap the stolen NEM with other cryptocurrencies at a discount market rate.	Cryptocurrency exchange platforms	NEM, Bitcoin and Lightcoin	$530 million	Yes	Metropolitan Police Department (MPD) of Japan	Several hackers	2018
Wronka (2023)	Money laundering	Funds and eradicating ties to criminal activities are mixed into the cryptocurrency market	Mixing service Bestmixer.io	Bitcoins, Bitcoin Cash, and Litecoins	over $200 million	Yes	Europol and Dutch authorities	Several individuals	2019
Maruf (2023)	Money laundering	The illicit cryptocurrency was mixed into the cryptocurrency market through Axie Infinity's	Mixing service Tornado Cash	Several (not specified)	$7 billion	Yes, hundreds of millions	FBI	North Korean hackers	2022

		Ronin Bridge protocol, Harmony Bridge, and Nomad Bridge.				went to a North Korean cybercrime organisation			
Sanction Scanner (2023)	Darknet transactions	Selling of illegal goods and drug trafficking on the Silk Road.	Darknet: Silk Road	Bitcoin	$15 million	Yes	FBI	Ross Ulbricht, creator of Silk Road	2013
Sanction Scanner (2023)	Money laundering	Illicit money was changed into the cryptocurrency market because the exchange company did not comply with US anti-money laundering laws	Cryptocurrency exchange platform: BitMEX	Several (not specified)	More than $100m	Yes	FBI	BitMEX executives	2020
Sanction Scanner (2023)	Money laundering	Using schemes such as shell companies, bogus supply chain invoices, smurfing, and mirror trades to hide funds stem from illegal acts.	Conventional banks	Several (not specified)	$2 trillion	Yes	US secret service	Banks such as JPMorgan Chase, Citigroup, HSBC, Standard Chartered, etc.	2020
Bolder (2023)	Money laundering	Treasure men on Hydra darknet marketplace	Darknet marketplace: Hydra	Several (not specified)	$350 million	Yes	US police forces	Russian citizen	2022
Prendi *et al.* (2023)	Ransomware	Using ransomware fraud to conduct identity theft, drug trafficking, public corruption, etc.	Cryptocurrency exchange platform: BTC-e	Bitcoin	$4 billion	Yes, 700,000 customers worldwide were involved	US police forces	Russian national Alexander Vinnik	2017
Prendi *et al.* (2023)	Money laundering	Mexican drug cartel funds were changed into the cryptocurrency market	Cryptocurrency exchange platforms: Binance and Huobi	Bitcoin and another unspecified cryptocurrency	$2.8 billion	Yes	US police forces	Six Chinese citizens	2020
Prendi *et al.* (2023) and Europol (2021)	Fraud	Professional-looking trading platforms are developed to lure victims through advertisements on social media and search engines	Fake cryptocurrency trading platform	Several (not specified)	€30 million	Yes, across Europe	Europol	6 people on the criminal network	2021
Prendi *et al.* (2023)	Ransomware	Mixing illicit cryptocurrencies (i.e., stolen from malicious hackers from bank accounts) into the crypto market	Mixing service: Tumbling services	Several (not specified)	Tens of millions of Euros	Yes	Europol	QQAAZZ network	2019
Outlook Money Team (2022)	Money laundering	Illicit money was changed into the cryptocurrency market	Cryptocurrency exchange platform	Several (not specified)	$400 million	Yes	UN security council	North Korea-affiliated hackers	2021

Chainalysis (2022)	Ransomware	Ransomware attacks and scams through over-the-counter (OTC) broker	OTC services	Unknown	Millions of dollars	Yes	US Office of Foreign Asset Control	Suex company	2021
Chainalysis (2022)	Money laundering	Drug money related- Bitcoin was sent to an intermediary wallet, and then to an OTC service nested at a popular cryptocurrency exchange. Used WhatsApp and Telegram to plan.	OTC services	Bitcoin	At least £1 million	No, all within the UK	UK Manchester police	Criminal groups across Northern England	2022
Sigalos (2022)	Ransomware	Ransomware payments, stolen funds by North Korea, Conti cybercrime group attack on Costa Rican government were mixed into the cryptocurrency market	Cross-chain bridge: RenBridge	Several (not specified)	At least $540 million	Yes	Blockchain analysis group Elliptic	Russian and North Korean hackers, Conti cybercrime group and several others	2022
CryptoWallet (2023)	Darknet transactions	Dark web transactions such as purchase of drugs, fake IDs, fake credit cards, sex crimes, blackmail, human slavery	Darknet marketplace: White House market	Monero (Privacy cryptocurrency)	€140 million	Yes	Europol	Several people	2022
Richard (2021)	Money laundering	Illicit money was changed into the cryptocurrency market	Several cryptocurrency exchange platforms	Tether (stablecoin)	$1.2 billion	No	Hong Kong policing bodies	Four people	2021
Brewster (2022)	Money laundering	Drug money was changed into the cryptocurrency market	Cryptocurrency exchange platform	Unknown	Between $15 and $40 million	Yes	US Drug Enforcement	Criminal gang	2022
United States v. Francisley da Silva, et al., S1 22 Cr. 622 (AT)	Money laundering	Siphoning of victim's cryptocurrency funds by cash withdrawal, then spent on luxury goods and real estate or laundered through shell companies and bulk cell phone purchases	Cryptocurrency exchange platform: IncomTech and Forcount	Unknown	Hundreds of thousands of dollars	Yes	US policing bodies	Founders and promoters of IncomTech and Forcount	2022
Office of Public Affairs (2023)	Darknet transactions	Ransomware, drug trafficking, transactions on Hydra Market dark web marketplace + failure to implement AML safeguards (minimal identification required)	Cryptocurrency exchange platform: Bitzlato	Unknown	More than $700 million connected to Hydra Marketplace and more than $15 million in ransomware proceeds	Yes	US policing bodies	Founder of Bitzlato Ltd	2022
U.S. Attorney's	Fraud	Fraud schemes	Cryptocurrency exchange platform	Bitcoin	$750,000	No, all within the	US policing bodies	Two people	2022

Office (2022)						US			
Nave (2021)	Money laundering	Cryptocurrency mixing service integrated with dark web marketplaces	Cryptocurrency mixing service: Helix and Coin Jinja LLC	Unknown	$300 million	Yes	US DC District Court	Operator of Helix and Coin Jinja LLC	2020
Nave (2021)	Money laundering	Cryptocurrency exchange companies advertised intent on bitcointalk.com and bitcoin-otc.com. Failed to implement an effective AML program and failed to report suspicious transactions	Cryptocurrency exchange platform	Bitcoin	Over 237 Bitcoins	Yes	US Secret Service	Eric Powers	2019
Nave (2021)	Money laundering	No AML program was set up	Cryptocurrency wallet: XRP II LLC	XRP	$450,0000	Yes	US Secret Service	Ripple Labs Inc. and XRP II LLC	2019
Office of Public Affairs (2021)	Darknet transactions	Illicit cryptocurrencies from darknet marketplace activity, illegal narcotics, computer fraud, abuse activities, and identity theft were put into the crypto market	Cryptocurrency mixing service: Bitcoin Fog	Bitcoin	Over 1.2 billion Bitcoin, approx. $335 million	Yes	US police forces	Operator of Bitcoin Fog	2021
Argentino *et al.* (2023) and Wiwoho *et al.* (2023)	Terrorism financing	Fundraisers on Twitter and Telegram, including a list of weapons and other equipment needed for an attack	Fundraising platform	Bitcoin	Unknown	Yes	FBI	Gaza-based Mujahideen Shura Council	2016
Argentino *et al.* (2023) and Wiwoho *et al.* (2023)	Terrorism financing	Fundraisers on Facebook, Telegram, and Twitter and solicit donations from supporters through charity wallets	Fundraising platform	Bitcoin	Unknown	Yes	FBI	Al-Qaeda	2017
Fabe *et al.* (2022)	Terrorism financing	Transfer of funds from the Middle East to support Indonesian terrorism	Fundraising platform	Bitcoin	Unknown	Yes	Indonesian Financial Intelligence	Bahrun Naim (the individual, who planned the 2016 attacks in Jakarta)	2016
Wiwoho *et al.* (2023)	Terrorism financing	Creation of a book explaining how to send cryptocurrency to ISIS	Fundraising platform	Bitcoin	Unknown	Yes	FBI	ISIS extremists	2014
Davis (2020); Hasbi and Mahzam (2018)	Terrorism financing	Raising cryptocurrency funds to finance terrorist groups	Fundraising platform	Bitcoin and other digital currencies	Over $85,000	Yes	US Federal Court in Central Islip	Zoobia Shahnaz (individual)	2017
Fabe *et al.* (2022)	Terrorism financing	Blackmailed owner of shopping centres to raise funds in cryptocurrency for bomb attack	Fundraising platform	Bitcoin	Unknown	No	US police	Leopold Wisnu Kumala (individual)	2016

Coinbase (2021)	Terrorism financing	Raising cryptocurrency funds to finance terrorist groups	Fundraising platform	Bitcoin, Ether, XRP, various ERC20 tokens	Unknown	Yes	FBI	Saudi-led jihadi activist movement	2021
Cohen and Godoy (2023)	Fraud	Stealing from customers of the FTX cryptocurrency exchange platform by siphoning money from the FTX exchange to a crypto-focused hedge fund	Cryptocurrency exchange platform	Unknown	$8 billion	Yes	US police forces	Sam Bankman-Fried (FTX founder)	2023
BBC (2023)	Fraud	Defrauded users of its stablecoin and token by way of false promises about guaranteed returns	Cryptocurrency exchange platform	TerraUSD and Luna	Unknown	Yes	US police forces and arrested in Montenegro	Do Hyeong Kwon (founder of TerraUSD and Luna)	2023
Coingraph (2023)	Fraud	Price manipulation on cryptocurrency trading platform:	Cryptocurrency trading platform: Mango Markets	Several	$110 million	Yes	Puerto Rico	Avi Eisenberg	2022
Coingraph (2023)	Fraud	Diverted funds for personal expenses and obtained investors' funds dishonestly	Cryptocurrency trading platform	SafeMoon token	Millions of dollars	Yes	US police forces	Thomas Smith, Kyle Nagy and Braden Karony (founders of SafeMoon token)	2023
Coingraph (2023)	Fraud	Unlawfully manipulated Mt. Gox cryptocurrency exchange platforms's electronic records, inflating the company's holding by $33.5 million, leading to its collapse	Cryptocurrency trading platform	Several	N/A	No	Tokyo police	Mark Karpeles (former CEO of Mt. Gox)	2015
Coingraph (2023)	Fraud	Bought tokens taking advantage of his insider knowledge before they were featured on OpenSea (i.e., NFT marketplace) and sold them for a profit	NFT marketplace	Several NFTs	Unknown	Yes	FBI	Nathaniel Chastain (employee of NFT marketplace OpenSea)	2022
Coingraph (2023)	Fraud	Abruptly shut down the Thodex exchange platform, leaving 400,000 users without access to deposits	Cryptocurrency exchange platform	Several	$2 billion	Yes	Albania police	Faruk Faith Ozer (founder and CEO of Thodex)	2022
Kozhipatt (2023)	Fraud	Used Elon Musk's appearance on SNL to scam users through fake cryptocurrency giveaways on Twitter and YouTube	Fundraising platform	Several	$10 million	Yes	US Federal Trade Commission	Several hackers	2022
Kozhipatt (2023)	Fraud	Hacked Twitter accounts of Kanye West, Barack Obama, Apple, and Uber to disseminate cryptocurrency giveaway scams	Fundraising platform	Several	Unknown	Yes	US Federal Trade Commission	Several hackers	2021

Shaheen (2023)	Fraud	Defrauded users by making them believe investment in crypto was lucrative	Cryptocurrency trading platform	OneCoin	€4.037 billion	Yes	US police forces	Irina Dilkinska (Head of Compliance for OneCoin)	2023
Greenberg (2021)	Money laundering	Created a cryptocurrency mixing platform (i.e., Bitcoin Fog) to facilitate obscuration of the source or destination of customers' cryptocurrency and took a commission on transactions on Bitcoin Fog of 2 to 2.5%	Cryptocurrency mixing platform	Bitcoin	1.2 million Bitcoins – worth $336 million at time of payment	Yes	FBI	Roman Sterlingov (founder of Bitcoin Fog)	2021
Elliptic (2023)	Terrorism financing	Money laundering through Binance and fundraising on social media	Cryptocurrency exchange platform: Binance	Bitcoin, stablecoin tether, altcoin dogecoin, and others.	$41 million	Yes	US Justice Department	Hamas	2023
Malik (2018)	Terrorism financing	Using false information to acquire loans and multiple credit cards to obtain cryptocurrency funds and send them to the Islamic State. She transferred the cryptocurrencies into Bitcoin and other digital currencies to send via Pakistan, China, and Turkey to fund the terrorist group	Fundraising platform	Bitcoin and other digital currencies	$62,000	Yes	US police forces	Single individual	2017
US Department of Justice (2017)	Ransome	BTC-e was utilised to facilitate transactions for cybercriminals worldwide and receive criminal proceeds from numerous computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics distribution rings.	Cryptocurrency exchange platform: BTC-e	Bitcoin	$4 billion	Yes	US police forces	Russian national Alexander Vinnik	2017

4. Case studies

51 cryptocurrencies-related financial crimes are collected, across different types of financial crime, a wide range of countries, and cryptocurrencies, as summarised in Table 1.

5. Statistical analysis

Statistical analysis and criminal investigations are conducted to explore the trend of cryptocurrency-related financial crimes, especially in terms of types of financial crime, the approaches used for financial crime, the platform involved for financial crime, whether the financial crime is cross border, the types of cryptocurrencies involved, and whether the financial crime is committed by individuals, company founders or organisations.

The trend of different types of cryptocurrency-related financial crime is shown in Fig. 1. It is seen that money laundering is the leading type of cryptocurrency-related financial crime most of the time, while most terrorism financing-related cryptocurrency crime is intensively identified in 2016 and 2017. The pseudo-anonymous nature and no intermediately-feature of cryptocurrencies make them more attractive to money launderers and terrorist organisations.

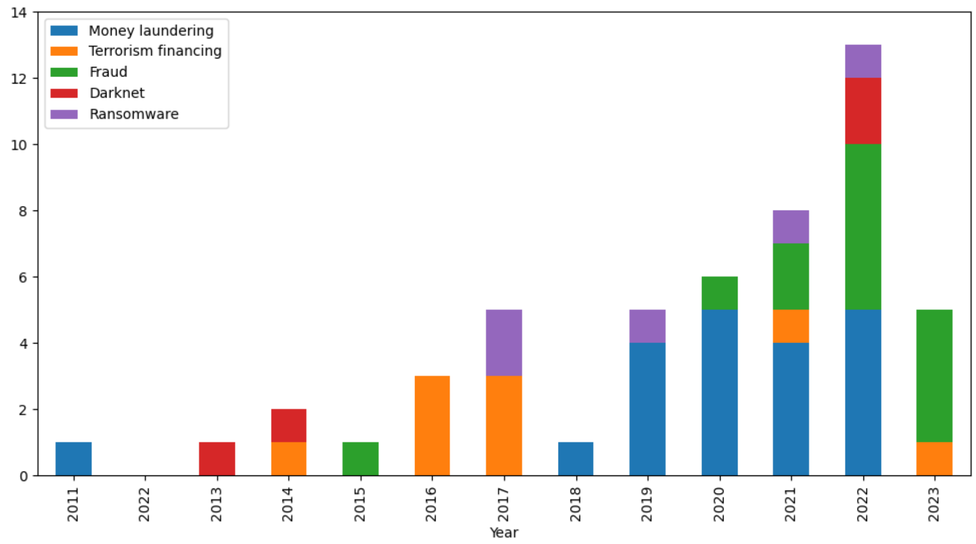


Fig. 1. Trend of different types of cryptocurrency-related financial crime (Source: Figure created by authors).

The trend of platforms involved in financial crime in different years is shown in Fig. 2. It is seen that cryptocurrency exchange companies and mixing services are the leading platforms of cryptocurrency-related financial crime most of the time, while fundraising platforms are frequently used in 2016 and 2017 to facilitate terrorism financing. The pseudo-anonymous nature of cryptocurrencies and lack of regulations towards exchange companies and mixing services makes them vulnerable to criminals.

Although there exists extensive legislation towards exchange companies in terms of knowing your customers, the level of legislation varies among different countries.

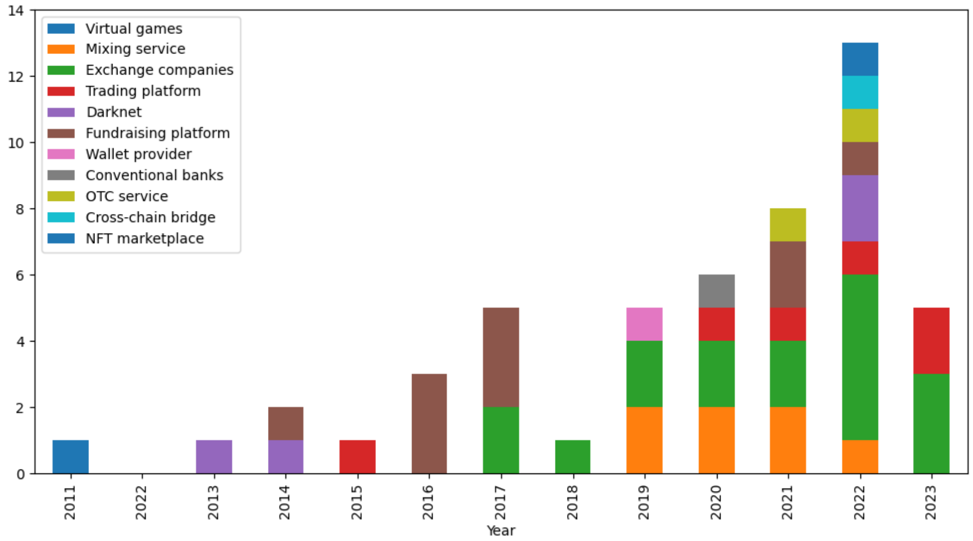


Fig. 2. Trend of different platforms involved in financial crime (Source: Figure created by authors).

The trend of cross-border-featured cryptocurrency crimes is shown in Fig. 3. It is seen that most of the cryptocurrency-related crimes are cross-border. This is mainly due to the decentralised and pseudo-anonymous nature of cryptocurrency, along with uneven and inadequate regulation of cryptocurrency in different countries.

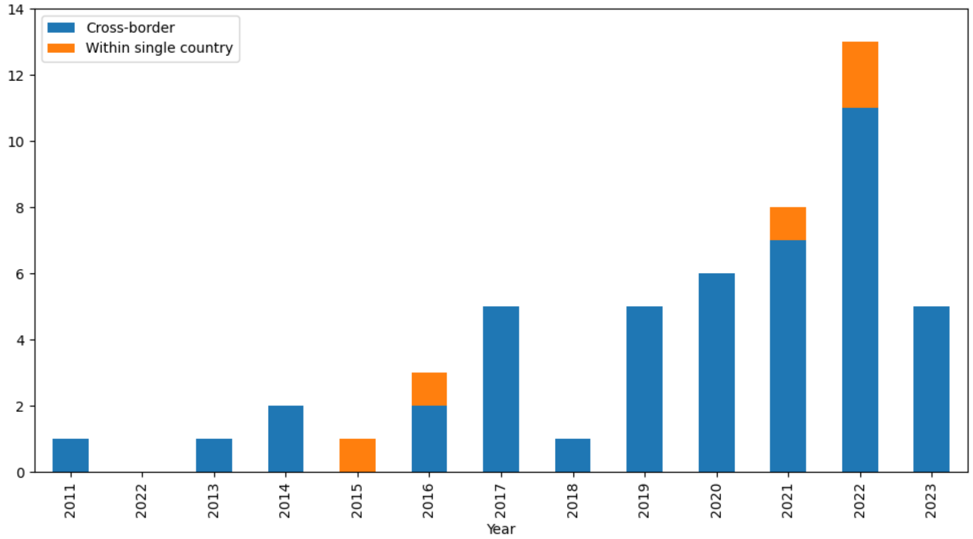


Fig. 3. Trend of cross-border features of cryptocurrency-related financial crime (Source: Figure created by authors).

The trend of different types of cryptocurrencies related to financial crime in different years is shown in Fig. 4. Bitcoins were frequently utilised for cryptocurrency-related financial crimes before 2019.

This was mainly due to the popularity and high market capitalisation of Bitcoin, and criminals may feel confident in using Bitcoin. However, after 2019, an increasing number of altcoins, such as privacy coins (i.e., Monero), stablecoins (i.e., Tether), and non-fungible tokens (i.e., ERC20 tokens), are utilised to facilitate financial crime. This might be owing to the maturity of cryptocurrencies and more people become to trust the value of cryptocurrencies.

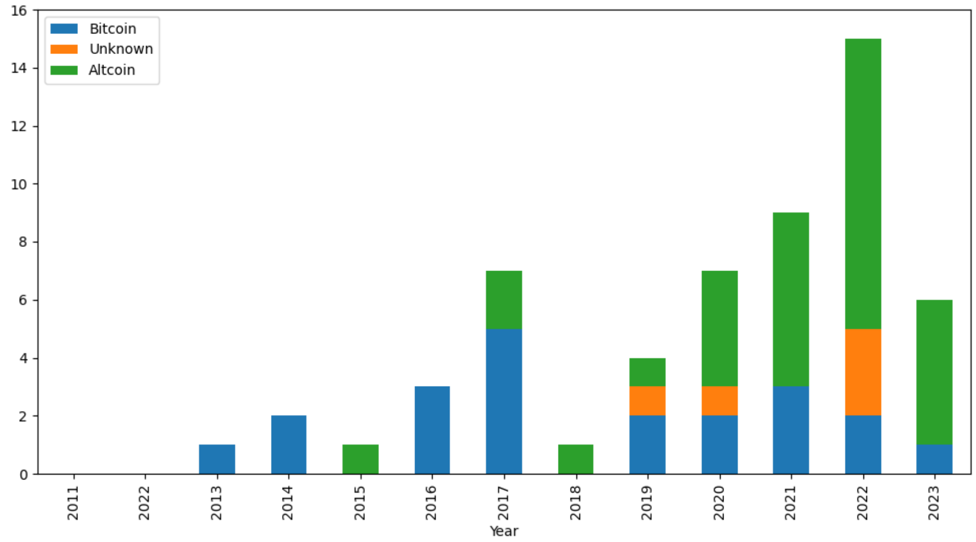


Fig. 4. Trend of different types of cryptocurrencies related to financial crime (Source: Figure created by authors).

The trend of perpetrators (i.e., individuals, founders of criminal companies, and organisation) in different years is shown in Fig. 5. Before 2019, most of the crimes were conducted by individuals and founders of criminal companies. However, after 2019, organisations became the main perpetrators of cryptocurrency-related financial crimes.

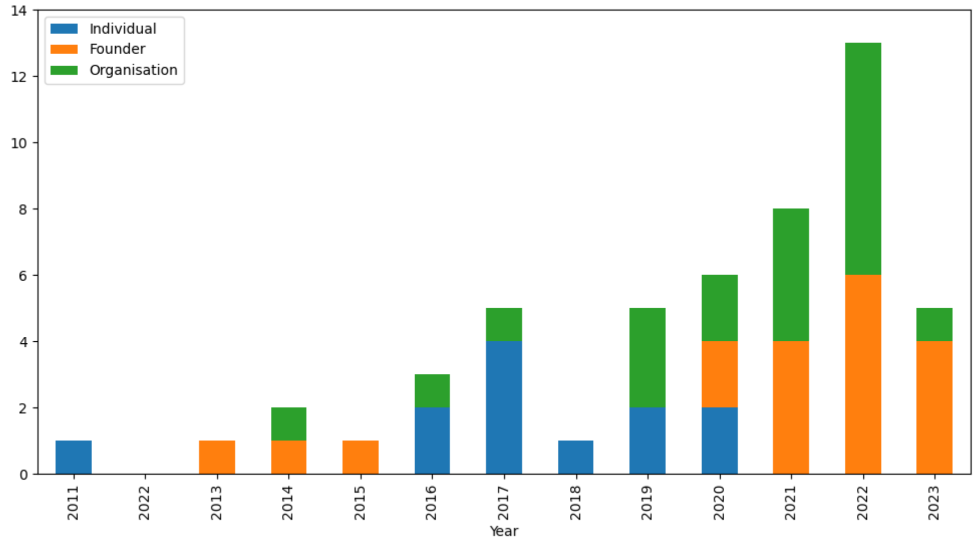


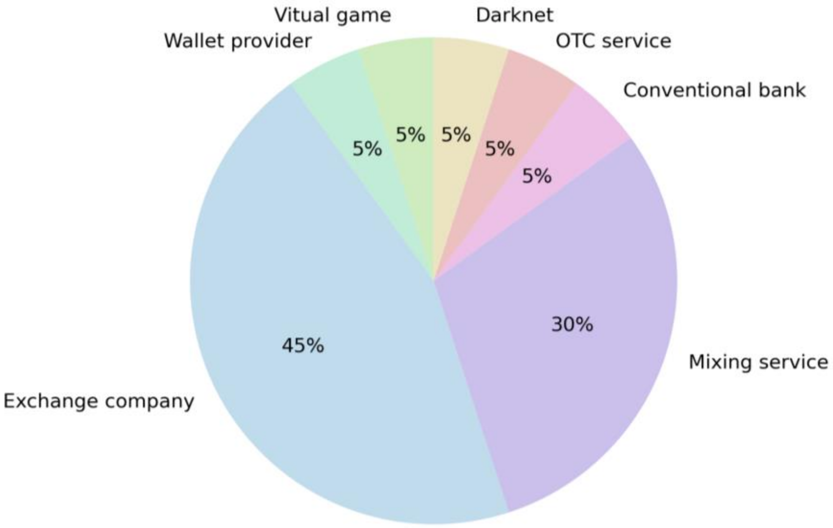
Fig. 5. Trend of perpetrators involved in cryptocurrency-related financial crimes (Source: Figure created by authors).

The approaches used to commit different cryptocurrency-related financial crimes are summarised in Fig. 6. In terms of money laundering, cryptocurrency exchange companies and mixing services are mainly utilised, followed by virtual games, cryptocurrency wallets, OTC services, and conventional banks. Criminals may exchange their illicit fiat money for different cryptocurrencies, and the pseudo-anonymity feature of cryptocurrencies makes it challenging for law enforcement departments to track the flow of illicit fiat money. This is consistent with the literature identifying cryptocurrency exchange companies, whether regulated or unregulated, as the major cryptocurrency laundering medium (Leuprecht *et al.*, 2023; The Financial Crime Academy, 2023; McCord *et al.*, 2022; Europol, 2021; Raza and Raza, 2021). Moreover, a mixing service provider may mix illicit cryptocurrencies with legal cryptocurrencies and transfer the mixed cryptocurrencies to the desired addresses to reduce the possibility of establishing a link between the original transaction and the address.

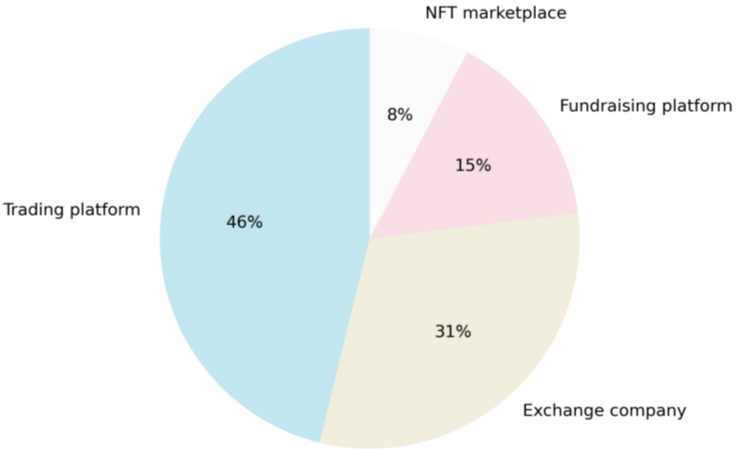
In terms of fraud, cryptocurrency trading platforms and exchange companies are mainly utilised, followed by fundraising platforms and non-fungible token (NFT) marketplaces. Cryptocurrency trading platforms and exchange companies usually manipulate the cryptocurrency market by pumping the value of minor cryptocurrencies to encourage victims to buy them and then implement an intentional collapse. Cryptocurrency trading platforms may also make false promises about high investment returns to motivate victims to invest in their cryptocurrency.

Silk Road was mostly involved in darknet cryptocurrency transactions, followed by the White House and Hydra Market. Ransomware attacks were usually conducted on cryptocurrency exchange companies, mixing services, OTC services, and cross-chain bridges.

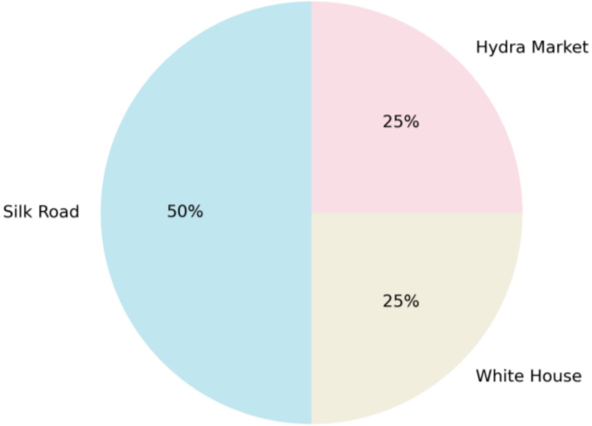
Most of the terrorism financing is conducted through fundraising platforms and may present threats to domestic and international security. Terrorists are exploiting social media to solicit funds and crowdfunding platforms to raise money, often by disguising themselves as charities (Manea and Paun, 2019). For instance, a Russian terrorist group conducted a large-scale crowdfunding scheme through social networks by registering e-wallets, mobile phone numbers, and credit cards (Fabe *et al.*, 2022). To get people to send them money, they generated the fake narrative that those profits would support Syrian refugees by building schools and mosques. These funds were transferred to e-wallets and credit cards, moved among bank accounts, withdrawn in cash, and transported by couriers to finance terrorists and their families.



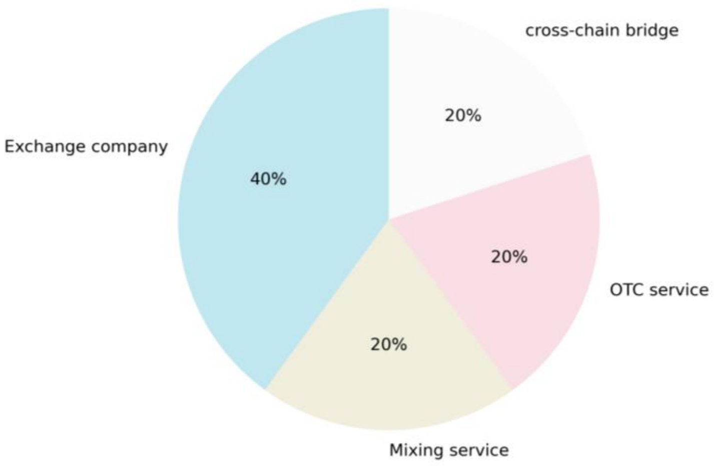
(a) Platforms that are used for money laundering



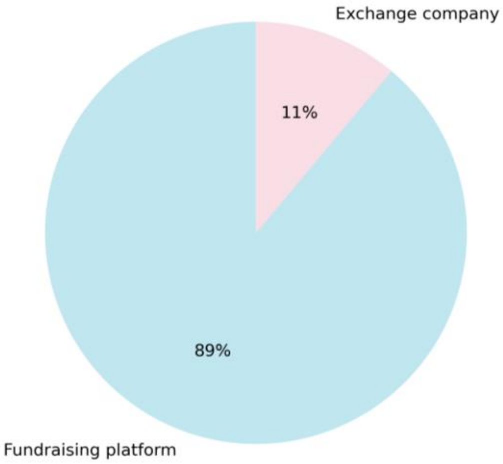
(b) Platforms that are used for fraud.



(c) Platforms that are used for darknet.



(d) Platforms used for ransomware attacks



(e) Platforms used for terrorism financing

Fig. 6. Platforms involved for different types of cryptocurrency-related financial crimes (Source: Figure created by authors).

6. Practical implication

6.1 Criminal investigation: Criminogenic features of cryptocurrencies

Through criminal investigation on case studies, decentralisation, pseudo-anonymous, and borderless nature are identified as key criminogenic features of cryptocurrencies.

Decentralisation: In the traditional financial environment, fiat money is primarily governed by state actors and is under a country’s jurisdiction. On the contrary, the decentralisation nature of cryptocurrency means that there is no single entity accountable for the ledger and no third-party intermediaries. Thus, there are no intermediaries to control the cryptocurrency transactions and detect suspicious financial transactions. The decentralised feature of cryptocurrencies makes it challenging for financial institutions to govern transactions and detect financial crimes. As a result, law enforcement departments may not be able to conduct prosecution because the prosecutions should be based on crime detection. Without prosecution, the victims cannot claim their lost money back. Therefore, the decentralisation nature of cryptocurrencies can stimulate cryptocurrency-related crimes such as money laundering, terrorism financing, fraud, and ransomware attacks as the criminals believe they have a lower chance of being prosecuted. However, money laundering, fraud, and ransomware attacks will affect the socioeconomic status of a country while terrorism financing may endanger national security.

Pseudo-anonymous: Although the wallet address of the sender and receiver of the cryptocurrency is traceable, the real identity of the wallet owner is pseudonymous. The cryptocurrency transactions do not require providing and verifying the actual participants. This gives criminals a sense of impunity and leads them to utilise cryptocurrencies for illegal activities. As identified in Table 1, hackers can hack famous social media accounts to scam victims through fake cryptocurrency giveaways. Moreover, due to the lack of an anti-money laundering scheme, cryptocurrency exchange companies are usually utilised by criminals to convert their illicit fiat money into cryptocurrencies, and then withdraw their cryptocurrencies into "clean" money through another cryptocurrency exchange company.

Borderless: As shown in Fig. 3, 92% of cryptocurrency-related financial crimes are conducted through cross borders. The borderless nature of cryptocurrencies enables criminals to exploit softer regulatory climates in certain countries to commit their financial crimes. Criminals also tend to seek this borderless nature to launder illicit money into different countries. The disparities in current regulations across different countries can render punitive actions in one jurisdiction ineffective.

6.2 Cryptocurrency crime prevention: Policy Changing Recommendations

As cryptocurrency exchange companies and mixing services are two of the most popular platforms utilised by cryptocurrency criminals, law enforcement departments need to develop strategic partnerships and public engagement with cryptocurrency exchange companies and mixing services through voluntarily reporting interagency collaboration. Cryptocurrency exchange platforms and wallet providers should be required to keep a record of IP addresses, transaction details, cryptocurrency wallet addresses, and chat message logs for each customer. Moreover, information standardisation can be implemented to enable a two-way exchange of information and benefit regulation implementation. For instance, cryptocurrency exchange companies and mixing services have access to transactional data, which is crucial for criminal investigations, while law enforcement agencies can offer exchange companies and mixing services insights into emerging threat vectors and potential security breaches (Tapscott and Tapscott, 2016). Information standardisation can streamline collaboration between cryptocurrency exchange companies, mixing services, and law enforcement agencies to ensure data is consistent, reliable, and actionable (FATF, 2019).

6.3 Cryptocurrency criminal investigation: Big data analytics-based crime detection tools

Blockchain analysis tools, such as Chainalysis and Elliptic, have been developed to recognise and examine cryptocurrency transactions, which are associated with addresses linked to criminal activities (Chainanalysis, 2021; Elliptic, 2021). Behaviour analytics using transaction data can identify a user who moves large volumes of cryptocurrency among wallets or splits transactions to avoid scrutiny (Foley and Karlson, 2019). The heuristic method can pinpoint suspicious transactions by analysing transaction patterns, including frequency, timing, and amount. However, current blockchain analytical tools support Bitcoin blockchain in a more detailed way than other blockchains, and cannot prevent, track, and detect illicit activities if transactions are made across different blockchains and cryptocurrencies. Novel big data analytics-based models should be developed to conduct criminal investigations and prevent cryptocurrency from being used illegally across different blockchain platforms, exchange companies, and cryptocurrency mixing services. Network analysis and topology-based features can be used to assess the role, status, and features of specific addresses in the cryptocurrency transaction network by evaluating its number of transactions, transaction time, and trading direction.

7. Conclusion

This paper presents insights into the criminal investigation of cryptocurrency-related financial crimes through a discussion of the relationship between the criminogenic features of cryptocurrencies and their potential exploitation to finance criminal enterprises. Based on the theory of planned behaviour, criminal investigation and thematic analysis are conducted on 51 cryptocurrency-related financial crime cases to identify criminogenic features of cryptocurrencies, key tools, and features of cryptocurrency-related financial crimes. Money laundering is the most common type of cryptocurrency-related financial crime, followed by financial fraud, ransomware attacks, terrorism financing, and the darknet transactions. Decentralisation, pseudo-anonymity, and borderless nature are the three critical features that make cryptocurrencies attractive to criminals as these three features collaboratively make cryptocurrency transaction tracking a complex challenge. Bitcoin was associated with most cryptocurrency-related crimes before 2019 as popularity and market capitalisation used to play a dominant role in criminals' choice of cryptocurrency. Recently, an increasing number of other cryptocurrencies, such as privacy coins (i.e., Monero), stablecoins (i.e., Tether), and non-fungible tokens (i.e., ERC20 tokens) have been utilised for financial crimes. Cryptocurrency has also become an essential source of terrorist financing as evidenced by Hamas most recently, which presents threats to domestic and international security.

Therefore, it is important and urgent for cryptocurrency exchange companies and mixing services to implement strict anti-money laundering and know-your-customer measures to prevent cryptocurrency-related crimes and create a sustainable future for cryptocurrencies. Only by reducing the crime rate can cryptocurrency gain investors' confidence and improve market capitalisation in return. Due to the transparent feature of blockchain, most cryptocurrency transaction data provide open access. Powerful big-data analytics models should be developed to conduct cryptocurrency crime investigations and prevent cryptocurrency from being used illegally across different blockchain platforms, exchange companies, and cryptocurrency mixing services.

One of the limitations of this paper is that cryptocurrency crime detection is still not mature. Although a lot of resources have been reviewed, 50% of them claim their case focuses on several cryptocurrencies but did not specify their names. This makes it uncertain which types of cryptocurrencies are mostly used in cryptocurrency-related financial crime. Also, only one case specifies the privacy coins. It is not sure whether there are other financial crimes related to privacy coins and has not been identified.

An interesting aspect to consider for further research would be assessing more thoroughly the risk associated with different cryptocurrencies when it comes to their exploitation for crime. Meanwhile, regulatory frameworks combatting cryptocurrency crime should be re-examined in light of the findings of this paper to suggest changes to ensure the practice of cryptocurrency-related financial crime is hindered. Robust big data analytics tools should be developed to identify and prevent different types of cryptocurrency crime among a range of cryptocurrencies.

References

Ali, N. (2022) Crimes Related to Cryptocurrency and Regulations to Combat Crypto Crimes. *Journal of Policy Research*. 8(3), pp. 289-302.

Almaqableh, L., Wallace, D., Pereira, V., Ramiah, V., Wood, G., Veron, J. F., Moosa, I. and Watson A. (2023) Is It Possible to Establish the Link Between Drug Busts and the Cryptocurrency Market? Yes, We Can. *International Journal of Information Management*. 71, pp. 1-14.

Argentino, M., Davis, J. and Hamming, T. R. (2023) Financing violent extremism: an examination of maligned creativity in the use of financial technologies. *Reports, Projects, and Research*. 22.

Ajzen, I. (1991). The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes,50, 179–211.

Barratt, M. J., Lenton, S., Maddox, A. and Allen, M. (2016) What if You Live on Top of a Bakery and You Like Cakes: Drug Use and Harm Trajectories Before, During and After the Emergence of Silk Road. *International Journal of Drug Policy* [online]. 35, pp. 50-57.

BBC, 2023. Do Kwon: Fugitive 'cryptocrash' boss arrested in Montenegro. https://www.bbc.co.uk/news/technology-65058533 [Accessed 18 December 2023].

Black, D. B. (2022) Cryptocurrency Fuels Growth of Crime. *Forbes* [online].

Brewster, T. (2022) Global Drug Conspiracy Used Binance To Launder Millions In Crypto, DEA Investigation Finds. *Forbes* [online]. 19 December. Available from: https://www.forbes.com/sites/thomasbrewster/2022/12/19/mexican-drug-gang-money-laundering-over-binance-crypto-exchange/ [Accessed 18 August 2023].

Bolder (2023) Washing, cashing: the lost coins, treasure men and money laundering in cryptocurrency. *Bolder* [blog]. Available from: https://boldergroup.com/insights/money-laundering-in-cryptocurrency/ [Accessed 17 August 2023].

Brown, S.D. 2016. Cryptocurrency and criminality: The Bitcoin opportunity. The Police Journal, 89(4), pp.327-339.

Chainalysis (2022) DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate. *Chainalysis* [blog]. 26 January. Available from: https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/ [Accessed 18 August 2023].

Cohen, L. and Godoy, J. (2023) Sam Bankman-Fried convicted of multi-billion-dollar FTX fraud. *Reuters* [online]. 3 November.

Coinbase, 2021. An overview of the use of cryptocurrencies in terrorist financing. Available online: https://www.coinbase.com/en-gb/blog/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing (Last accessed 18 December 2023)

Coingraph (2023) 10 High-Profile Crypto Fraud Cases You Need to Know About. *Coingraph* [online]. 5 November. Available from: https://www.coingraph.news/10-high-profile-crypto-fraud-cases-you-need-to-know-about/ [Accessed 11 November 2023].

Collins, J. (2022) *Crypto, crime and control: Cryptocurrencies as an enabler of organised crime*. Global Initiative Against Transnational Organised Crime. Switzerland. June 2022.

Cong, L. W., Grauer, K., Rabetti, D. and Updegrave, H. (2023) Blockchain Forensics and Crypto-related Cybercrimes. *SSRN* [online]. Pp. 1-115.

Cryptowallet (2023) *Monero Use Case*. Available from: https://cryptowallet.com/academy/monero-use-case/ [Accessed 20 August 2023].

Davis, J. (2020) *New technologies but old methods in terrorism financing*. Royal United Services Institute for Defence and Security Studies. [Accessed 22 July 2023].

Dearden, T. E. and Tucker, S. E. (2023) Follow the Money: Analysing Darknet Activity Using Cryptocurrency and the Bitcoin Blockchain. *Journal of Contemporary Criminal Justice* [online]. 39(2), pp. 257-275.

Dudani, S., Baggili, I., Raymond D. and Marchany, R. (2023) The Current State of Cryptocurrency Forensics. *Forensic Science International: Digital Investigation* [online]. 46, pp. 1-11.

Dyntu, V. and Dykyi, O. (2018) Cryptocurrency in the System of Money Laundering. *Baltic Journal of Economic Studies* [online]. 4(5), pp. 75-81.

Elliptic, 2023. How Hamas has utilized crypto, and what may be coming https://www.elliptic.co/blog/how-hamas-has-utilized-crypto-and-what-may-be-coming

Europol (2021) *Cryptocurrencies – Tracing the evolution of criminal finances*. Luxemburg, Publications office of the European union.

Fabe A.P., Toledo J.A., and Laksmi S. (2022) The growth of financial technology in Indonesia: Implications for terrorism financing. *International Annals of Criminology* [online]. 60, pp. 162-181. [Accessed 8 July 2023].

Fanusie, Y. J. and Robinson, T. (2018) *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*. Centre On Sanction & Illicit Finance.

FATF (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

Foley, S., Karlsen, J. R. and Putnins, T. J. (2018) Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies? *The Review of Financial Studies* [online]. 32(5), pp. 1798-1853.

Greenberg, A. (2021) Feds Arrest an Alleged $336M Bitcoin-Laundering Kingpin. *Wired* [blog]. 27 April. Available from: https://www.wired.com/story/bitcoin-fog-dark-web-cryptocurrency-arrest/ [Accessed 5 November 2023].

Hasbi A. H., and Mahzam, R. (2018) Cryptocurrencies: Potential for terror financing? *RSIS Commentary* [online]. 75, pp. 1-3. [Accessed 20 July 2023].

Joo, M. H., Nishikawa, Y. and Dandapani, K. (2020) Cryptocurrency, A Successful Application of Blockchain Technology. *Managerial Finance* [online]. 46(6), pp. 715-733.

Kethineni, S. and Cao, Y. (2020) The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review* [online]. 30(3), pp. 325-344.

Kozhipatt, J. (2023) 5 Social Media Crypto Scams to Avoid. *CoinDesk* [online]. 18 January. Available from: https://www.coindesk.com/learn/5-social-media-crypto-scams-to-avoid/ [Accessed 11 November 2023].

Kutera, M. 2022. Cryptocurrencies as a subject of financial fraud. *Journal of Entrepreneurship, Management and Innovation*, *18*(4), pp.45-77.

Leuprecht, C., Jenkins, C. and Hamilton, R. (2023) Virtual Money Laundering: Policy Implications of the Proliferation in the Illicit Use of Cryptocurrency. *Journal of Financial Crime* [online]. 30(4), pp. 1036-1054.

Malik, N. (2018) How Criminals And Terrorists Use Cryptocurrency: And How To Stop It. *Forbes* [online]. 31 August. Available from: https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/ [Accessed 5 November 2023].

Manea, G. C. and Paun C. V. (2019) Terrorist Threats on the Economic System and Combating Financing Terrorist Organisations. *Sciendo* [online]. 13(1), pp. 920-932.

Maruf, R. (2023) Tornado Cash crypto firm founders indicted for allegedly laundering money for North Korean hackers. *CNN Business* [online]. 23 August.

Matakovic, I. C. (2022) Crypto-assets Illicit Activities: Theoretical Approach with Empirical Review. *International E-journal of Criminal Sciences* [online]. 5(17), pp. 1-30.

McCord, A., Birch, P. and Davison, A. (2022) Technology Enabled Crime: Examining the Role of Cryptocurrency. *Criminology – The Online Journal* [online]. 4(4), pp. 428-451.

Ndiaye, M. and Konate, P.K. 2021, October. Cryptocurrency crime: Behaviors of malicious smart contracts in blockchain. In *2021 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-8). IEEE.

Nolasco Braaten, C. and Vaughn, M.S., 2021. Convenience theory of cryptocurrency crime: A content analysis of US federal court decisions. *Deviant Behavior*, *42*(8), pp.958-978.

Richard M. (2021) Mounting Cases of Money Laundering through Digital Currencies in 2021. *ShuftiPro* [blog]. 15 November. Available from: https://shuftipro.com/blog/mounting-cases-of-money-laundering-through-digital-currencies-in-2021/ [Accessed 18 August 2023].

Nave, P. (2021) 4 Cryptocurrency Money-Laundering Cases. *Axiom Alpha* [online]. Available from: https://axiomalpha.com/cryptocurrency-money-laundering-cases/ [Accessed 20 August 2023].

Office of Public Affairs (2021) *Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer"*. 28 April. Available from: https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer [Accessed 18 August 2023].

Office of Public Affairs (2023) *Founder and Majority Owner of Cryptocurrency Exchange Charged with Processing Over $700 Million of Illicit Funds*. 18 January. Available from: https://www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange-charged-processing-over-700-million [Accessed 20 August 2023].

Outlook Money Team (2022) 7 Cases Of Cryptocurrency Money Laundering Under Investigation; Rs 135 Crore Attached, Says Government. *Outlook* [online].

Pieroni, C. (2018) La Crypto Nostra: How Organised Crime Thrives in the Era of Cryptocurrency. *North Carolina Journal of Law & Technology* [online]. 20(5), pp. 111-147.

Prendi, L., Borakaj, D. and Prendi, K. (2023) The New Money Laundering Machine Through Cryptocurrency: Current and Future Public Governance Challenges. *Corporate Law & Governance Review* [online]. 5(2), pp. 84-91.

Raza, H. and Raza, M. R. (2021) A Study of Blockchain Technology, Bitcoin and Other Cryptocurrencies as Means of Money Laundering, Frauds and Scams. *Global Media and Social Sciences Research Journal (Quarterly)* [online]. 2(1), pp. 73-84.

Sanction Scanner (2023) Cryptocurrency Scandals and Anti Money Laundering. *Sanction Scanner* [blog]. Available from: https://sanctionscanner.com/blog/cryptocurrency-scandals-and-anti-money-laundering-398 [Accessed 17 August 2023].

Sàndor, B. and Fehèr, D. J. (2019) *Examining the relationship between the Bitcoin and cybercrime*. The 13th international symposium on applied computational intelligence and informatics. Timisoara, Romania. 29-31 May.

Shaheen, H. (2023) OneCoin's Legal Head pleads guilty in landmark case for cryptocurrency fraud. *Cryptopolitan* [blog]. 9 November. Available from: https://www.msn.com/en-us/news/crime/onecoins-legal-head-pleads-guilty-in-landmark-case-for-cryptocurrency-fraud/ar-AA1jFv3R [Accessed 11 November 2023].

Sigalos, M. (2022) Crypto criminals laundered $540 million by using a service called RenBridge, new report shows. *CNBC* [online]. 10 August. Available from: https://www.cnbc.com/2022/08/10/crypto-criminals-laundered-540-million-using-renbridge-elliptic-says.html [Accessed 17 August 2023].

Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J. And Salas, A. (2020) Exploring the use of Zcash cryptocurrency for illicit or criminal purposes. Cambridge, RAND corporation.

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.

Teichmann, F.M.J. and Falker, M.C., 2021. Cryptocurrencies and financial crime: solutions from Liechtenstein. Journal of Money Laundering Control, 24(4), pp.775-788.

The Police Foundation (2021) *Crypto-currency enabled future crime*. 8 March.

Thowseaf, S. 2023. Cryptocurrency May Prove Financial Crime: A Conceptual Analysis. In *Emerging Insights on the Relationship Between Cryptocurrencies and Decentralized Economic Models* (pp. 110-121). IGI Global.

Tredinnick, L. (2019) Cryptocurrencies and the Blockchain. *Business Information Review* [online]. 36(1), pp. 39-44.

Trozze, A., Kamps, J., Akartuna, E.A. 2022. Cryptocurrencies and future financial crime. Crime Sci 11, 1.

Trozze, A., Davies, T. and Kleinberg, B. 2023. Explaining prosecution outcomes for cryptocurrency-based financial crimes. Journal of Money Laundering Control, 26(1), pp.172-188.

Tsuchiya, Y. and Hiramoto, N. (2021) How cryptocurrency is laundered: Case study of Coincheck hacking incident. *Forensic Science International: Reports* [online]. 4, pp. 1-7.

United States v. Francisley da Silva, et al., S1 22 Cr. 622 (AT)

US Department of Justice, 2017. Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox

U.S. Attorney’s Office (2022) Two Indicted in East Texas Cryptocurrency Money Laundering Scheme. *United States Secret Service* [online]. 10 March.

Wiwoho, J., Pratama, A. M., Pati, U. K. and Tejomurti, K. (2023) Examining cryptocurrency use among muslim affiliated terrorists: Case typology and regulatory challenges in Southeast Asian Countries. *Jurnal Hukum dan Praanta Sosial* [online]. 18(1), pp. 102-124. [Accessed 20 July 2023].

Wronka, C. (2023) Financial Crime in the Decentralised Finance Ecosystem: New Challenges for Compliance. *Journal of Financial Crime* [online]. 30(1), pp. 97-113.