KrimOJ Kriminologie – Das Online-Journal
Criminology – The Online Journal

No. 4/2022

Alex McCord, Philip Birch & Alan Davison

Technology Enabled Crime: Examining the Role of Cryptocurrency

The illicit use of cryptocurrencies is an area in which a race exists between criminals seeking to exploit evolving technology, investigators trying to detect or disrupt activity, and legislators attempting to regulate its use. Law enforcement face multiple challenges, including the identification of offenders and the lack of a consistent regulatory framework to prosecute criminal activity as well as of tools and training to prevent or disrupt crime. To better understand the relationship between cryptocurrency offending and digital disruption* investigation and prevention methods, a review of the existing scientific evidence was conducted with the aim of supporting practitioners, such as the police, in their work of preventing, disrupting and reducing crime. Findings detail the categories and volume of criminal activity as well as the influence of cryptocurrency markets on crime and important aspects for law enforcement practitioners, while a selection of digital disruption investigation and prevention methods proposed by academic security researchers were also identified; these are discussed with recommendations for further research. The influence of criminal activity as a cryptocurrency market driver is additionally considered. It is suggested that criminal use of cryptocurrencies, while increasing in raw numbers, is decreasing by volume relative to the entire market. However, the state of knowledge of the scope, scale and rate of change is uneven between areas of criminal activity, with no consensus as yet on a consistent model of calculation. The paper concludes with a number of recommendations.

Keywords: crime, cryptocurrency, investigation, security, technology, policing

Technologiegestützte Kriminalität – Zur Rolle von Kryptowährungen

Bei der illegalen Nutzung von Kryptowährungen liefern sich Straftäter:innen, die versuchen, neue Technologie auszunutzen, Ermittler:innen, die versuchen, Straftaten aufzudecken oder zu unterbinden und Gesetzgeber, die versuchen, die Nutzung zu regulieren, ein Wettrennen. Den Strafverfolgungsbehörden stellen sich zahlreiche Herausforderungen, etwa die Ermittlung von Straftäter:innen, das Fehlen eines rechtlichen Rahmens für die Strafverfolgung sowie von Instrumenten und Ausbildung um Straftaten vorzubeugen oder sie zu unterbinden. Um die Beziehung zwischen Kryptowährungsdelikten und Ermittlungs- und Präventionsmethoden zur digitalen Disruption besser zu verstehen, wird der Forschungsstand analysiert. Ziel ist es, die Praxis, z. B. die Polizei, bei Prävention, Störung und Reduzierung von Delikten zu unterstützen. Die Ergebnisse informieren über Kategorien und Umfang illegaler Aktivitäten sowie den Einfluss von Kryptowährungsmärkten auf Kriminalität, beides wichtige Aspekte für Strafverfolgungsbehörden. Außerdem wurden Ermittlungs- und Präventionsmethoden für digitale Disruption aus der Sicherheitsforschung identifiziert; diese werden hinsichtlich Empfehlungen für weitere Forschung diskutiert. Ebenso wird der Einfluss illegaler Aktivitäten als Treiber des Kryptowährungsmarktes diskutiert. Es wird angenommen, dass die illegale Nutzung von Kryptowährungen zwar zahlenmäßig zunimmt, das Volumen im Verhältnis zum gesamten Markt jedoch abnimmt. Allerdings ist der

https://doi.org/10.18716/ojs/krimoj/2022.4.4

Kenntnisstand über Umfang, Ausmaß und Veränderungsrate in den verschiedenen Deliktsbereichen uneinheitlich, und es besteht noch kein Konsens über ein einheitliches Berechnungsmodell. Der Text schließt mit einer Reihe von Empfehlungen.

Schlagwörter: Ermittlung, Kryptowährung; Kriminalität, Technologie, Strafverfolgung, Sicherheit

1. Introduction

There has been a decline in traditional forms of crime and disorder in recent times, yet the rise of crime in the online space is on the rise, requiring innovative and alternative solutions in order to combat (CBS, 2021; Gladstone, 2019; McCord et al, 2022a; McCord, 2022b). Those working in the field, responsible for the prevention, disruption and reduction of crime, are arguably being left behind, both in terms of knowledge and response to this shift of crime in the online space (Cross et al, 2021; Horsman, 2017; Harkin et al, 2018). This paper, therefore, adopts a review of the scientific literature and evidence on an aspect of online crime, that of crime that is facilitated in the online space using cryptocurrency. As such the paper provides law enforcement agencies a knowledge bank for this increasing threat to public safety, with practice recommendations for application to their practice.

1.1 Understanding Cryptocurrency

The explosion of cryptocurrency markets has created a transnational, borderless and initially unregulated landscape with democratized entry, open to anyone with online access and the willingness to learn to navigate the system (Bailey et al., 2021; Mackenzie, 2022). Described as a digital Wild West, transacting in cryptocurrency is attractive to both legitimate investors and criminals (Collins, 2022; Morton & Curran, 2022). The global cryptocurrency market expanded exponentially between 2019 and 2021, beginning 2019 with a market-cap of USD $ 135 billion and peaking at $ 3 trillion in November 2021 (Jevans, 2022). Cryptocurrency transaction volume in 2021 totalled $ 15.8 trillion, within which the current total of payments to known illicit addresses was $ 14 billion, or 0.15 % of the market at the time of calculation, representing a 79 % increase in illicit activity from 2020 and adjusted as additional illicit addresses are identified (Grauer et al., 2022). Despite significant market devaluations in 2022, as of the end of the second quarter, the global market cap remained a substantial figure at USD $ 896.7 billion, with forecasts predicting eventual stability and growth (CoinMarketCap, 2022; Streissguth, 2022).

Cryptocurrencies are sometimes referred to interchangeably as virtual or digital currencies (Aquisdata, 2022; Sanz-Bas et al., 2021), which are usually, although not always, based on blockchain technology (Cooper, 2021). Virtual currencies have been categorised as belonging to open or closed-loop systems, where an open currency can be traded or converted between systems (Aquisdata, 2022), and a closed-loop currency can only be used within one system (Financial Action Task Force, 2021b). Some suggest further separation of virtual currencies, considering digital currency a superordinate term referring to any currency that is digital, within which three types of virtual currencies exist: closed, such as video game credits that can only be used within the issuing game; uni-directional such as points within a loyalty reward program used to purchase goods or services; and bi-directional (Scheidegger & Raghubir,

2022). A bi-directional digital currency, such as Bitcoin, Ethereum or Tether, is open and can be traded or converted in either direction to other digital currencies or government-backed legal tender, known as fiat currency (Kethineni & Cao, 2020). For clarity, the focus of this paper is on currencies which are open and able to be bi-directionally traded.

1.2 Calculating Cryptocurrency Crime and its Use

The blockchain data platform Chainalysis used the calculation method to arrive at their USD $14 billion figure for 2021, by which transactions to previously identified illicit addresses are totalled (Grauer et al., 2022; Grauer & Updegrave, 2021). Foley et al. (2019) utilised an alternate methodology, extrapolating illicit activity based on networks and behaviour patterns to suggest that as many as 25 % of bitcoin users engaged in illicit activity during the review period, with 46 % of reviewed transactions deemed illicit. There is as yet no consensus on one method of computing criminal activity. It has been argued that the calculation method may return a low estimate, as it does not take into account overall user behaviour and is limited to known illicit accounts, while the behaviour analysis method may capture innocent transactions and therefore be inflated (Schickler, 2022). The Financial Action Task Force (2021a), an intergovernmental body, advised that identifying illegal uses of cryptocurrency using the calculation method should be treated as a minimum or conservative estimate only of illegal or illicit activity. It therefore may arguably be suggested that the illicit cryptocurrency transaction volume in 2021 was at least 0.15 % ($ 14 billion) of the market total.

The use of cryptocurrency is attractive to criminals for a number of reasons; chiefly, the ease of use and perception of anonymity (Kethineni & Cao, 2020). While blockchain transactions are publicly available and increasingly traceable, the flow of currency can be obscured by mixers or tumblers, which break up transactions between sender and receiver and can facilitate money laundering (Dumchikov et al., 2022), or the use of privacy coins which utilise proprietary technology to further shield users' identities (Bele, 2021). In addition, Decentralized Finance (DeFi) has become popular since 2020, allowing users to trade currency, invest, and generate or receive loans without banks, credit checks or proof of identity (Grauer & Updegrave, 2021; Mackenzie, 2022). A key element of DeFi is its reliance on smart contracts, automatic execution of transactions once specified conditions have been met, using blockchain technology (Schär, 2021). DeFi has been identified as both a positive development by allowing users a higher level of control, and a risky one that can be exploited (Jin & Vinella, 2022).

As a consequence, the rapid rise of cryptocurrency, its use in criminal activity, as well as more broadly across society, a digital race has emerged in which IT developers and legal systems across the globe are playing catch up in their prevention and response to technology enable crime using cryptocurrency.

1.3 Digital Race between Criminals, IT Developers and the Legal System

With governments attempting to legislate criminal uses of cryptocurrency as both legitimate and criminal players explore what is possible within the system a digital race has emerged (Hammond & Ehret, 2022). Security specialists and engineers in both academic and commercial sectors are engaged in a similar race to develop solutions to protect legitimate users and

detect, prevent or disrupt illicit activity (Ahmed-Rengers et al., 2020; Grauer & Updegrave, 2021; Kolachala et al., 2021; Sapkota & Grobys, 2021). Within the development field, some argue that use of machine learning to develop tools to fight illicit cryptocurrency can also be used by criminals to identify targets (Wang et al., 2021), and that the best way forward may be a combination of regulation, enforcement and automatic prevention (Collins, 2022). In recognition of this digital race, this study seeks to understand how technology enabled crime is facilitated by cryptocurrency and what effective responses are emerging in order to address this criminality.

2. Study & Methodology

This study set out to better understand the relationship between cryptocurrency, crime and law enforcement, due to the increase recognition of the chasm being created between the rise and shift of crime to online space, coupled with the fact law enforcement agencies are being left behind in terms of knowledge and responding to such. The study was therefore guided by the following four questions:

1. How is cryptocurrency enabling digital or technology-enabled crime?
2. What are those crimes?
3. How is crime in the digital space affected or influenced by cryptocurrency?
4. What is the law enforcement response?

2.1 Method

In order to address the four questions a review of the academic and grey literature was conducted using a search, appraisal, synthesis and analysis framework (Grant & Booth, 2009). Databases searched included EBSCO Host, Informit, Lexis Nexis, ProQuest Central, SAGE, Science Direct, SCOPUS, Taylor and Francis and Web of Science. Reference searches within articles and reviews of the publication sections of decentralized finance (DeFi) and blockchain analysis firms, commercial technology developers, cybersecurity firms and government criminology agencies were also conducted. Search terms were divided into two categories including criminal nature and use of digital currency, separated internally by "OR" Boolean operators and externally by the "AND" operator, with use of the "*" wild card character to capture alternate spellings.

Accepted terms and definitions within this field of research are emerging, making the choice of search terms potentially subject to bias. A broad list of search terms was compiled from an initial SCOPUS background search using the keywords crime AND crypto*, with two independent reviewers evaluating each subsequent keyword individually. Given the aim to focus on open, bidirectional currencies, the term "virtual currency" was eliminated from the search string. Additionally, search terms related to cybercrime were eliminated as this term was evaluated as potentially capturing sources outside the scope of this article. A complete list of search terms is provided in table 1 below.

Table 1. Keywords and Search Terms

Criminal Nature	*AND*	**Digital Currency**
Crime OR		Cryptocurrenc* OR
Blackmail OR		Crypto OR
Technology-enabled crime OR		Digital currenc* OR
Digital crime OR		Bitcoin OR
Digitally-assisted crime OR		Ethereum OR
Online offending OR		Litecoin OR
Crypto-crime OR		Binance OR
Blockchain hacking OR		USD Coin OR
Blockchain fraud OR		XRP OR
Illegal crypto* OR		Solana OR
NFT fraud		Cardano OR
		Dogecoin OR
		Monero

Note. The Science Direct database search was abridged to comply with limitations on Boolean operators and wildcards as follows: (crime OR fraud OR illegal OR hacking) AND (crypto OR cryptocurrency OR cryptocurrencies OR "digital currency" OR "digital currencies").

Academic articles were peer-reviewed and written in English with full-text accessibility. Grey literature included whitepapers, company reports, conference proceedings, media publications and industry-specific online articles. The search period was limited to publications following the first Bitcoin whitepaper (Nakamoto, 2008), to 2022. Sources were required to contain identified keywords in each of the two categories for initial consideration; this process yielded 2,281 sources. A staged review eliminated duplicates and then evaluated the remaining articles by title or abstract, yielding 510 potential sources. These sources were read initially by abstract and analysed, then marked for full text review, narrowing the sources to 148. While the date range was intentionally broad in order to capture the evolution of criminal cryptocurrency activity, 80 % of the resources included were dated between 2020-2022.

3. Findings

Below the four questions that guided the study are addressed.

3.1 How Does Cryptocurrency Enable Crime?

Cryptocurrencies can be either a target for criminals by theft or exploitation, or a means of payment for illegal goods and services (Bele, 2021). The use of cryptocurrencies can enable or support criminal activity from the individual to the governmental level by removing traditional obstacles such as visibility and traceability (Patel & Bharat, 2012). At an individual level this might involve fraud or darknet market payments (Cortez, 2021), or at a governmental level might involve the evasion of international sanctions (Carlisle & Izenman, 2019). The decentralisation and pseudo-anonymity of cryptocurrency transactions provides a layer of identity protection to those using funds for illicit means (Dyntu & Dykyj, 2021). There is no bank to function as an intermediary or central point of contact, and accounts are not tied to an identity or user (Kuzuno & Tziakouris, 2018). As the currencies traded are not government-backed and do not originate from a central point, trade can be truly transnational (Fletcher et al., 2021).

Further, as the currencies are digital, there is no need for physical storage of financial assets (Sanz-Bas et al., 2021). This does not mean that cryptocurrency transactions are invisible; rather, that a certain level of technological ability is required to track and interpret them (Kaushik & Dahiya, 2021). An inherent level of transparency exists in that all blockchain transactions are publicly available (Trozze, Kamps, et al., 2022). This has given rise to a race between criminals seeking to remain anonymous, IT developers creating techniques or products to track activity, and governments seeking to regulate the arena.

The use of mixers, also known as tumblers, is one way to hide a trail of blockchain transactions. Mixing or tumbling services pool cryptocurrency resources with users sending funds in random amounts to a number of new addresses, which are then sent on to the destination address minus a service fee (van Wegberg et al., 2018). Privacy coins such as Monero, Dash or ZCash operate with less transparency than currencies such as Bitcoin or Ethereum, hiding the sending and receiving addresses, and/or the amount of the transaction from their blockchain (Sapkota & Grobys, 2021).

As with any activity, the use of cryptocurrency for criminal activities requires a certain level of skill and familiarity with technology, which can be an obstacle to some individuals or organisations (Silfversten et al., 2020). It has been argued that the knowledge and confidence required to enter the digital currency system may be a factor in the low percentage of criminal activity within the market, and analysis of known illicit crypto accounts reveals that a large share of known criminal balances is held by a small number of accounts described as "criminal whales" (Grauer et al., 2022; Kaushik & Dahiya, 2021).

3.2 What Types of Cryptocurrency Crime Exist?

The review of literature revealed several major areas of criminal activities either influenced by or enabled by use of cryptocurrency. Some sources have attempted to monitor and calculate the magnitude at which these activities take place. The areas of crime are listed and will be discussed in detail below: fraud, money laundering, ransomware, malware, theft, financing of terrorism, acts driving geo-political instability, evasion of sanctions and payments made for illegal services or within darknet markets. According to statistics compiled by industry data watchers including CipherTrace, a subsidiary of MasterCard, and Chainalysis, a blockchain data platform, approximately 0.10 % to 0.15 % of all cryptocurrency traffic in 2021 was related to criminal activity, which represents a drop from 2020 figures at 0.62-0.65 % (Grauer et al., 2022; Grauer & Updegrave, 2021; Jevans, 2022). This data is subject to continual revision; Chainalysis updates their annual data retrospectively as addresses or wallets known to be used for illicit cryptocurrency activity are identified, with the 2020 data growing from 0.34 % to 0.62 % during the 2021 reporting period (Grauer et al., 2022).

3.2.1 Fraud and Scams

Fraud was the largest crypto crime area by transaction volume, with USD $ 7.8 billion sent to known scam addresses in 2021 (Grauer et al., 2022). Within this category, investment scams are the most common with Ponzi schemes, initial coin offerings and pump and dump schemes dominating the field (Trozze, Kamps, et al., 2022). The US Federal Trade Commission (2022) reported consumer cryptocurrency investment scam losses of USD $ 680 million in 2021, and

$ 329 million in Q1 2022, suggesting nearly a four-fold increase. The Australian Competition and Consumer Commission (ACCC) reported that in Q1 and Q2 2022, cryptocurrency investment scams made up over 50 % of all scams reported, with AUD $ 113 million lost as of June 2022 (ACCC, 2022). Romance schemes, within which the pig-butchering scheme arose out of China and spread globally (Wang & Zhou, 2022), and business or government-impersonation schemes were the most popular after investment scamming, accounting for 19 % and 13 % of reported crypto fraud cases in the United States in 2021, respectively (US Federal Trade Commission, 2022). See Trozze, Kamps, et al. (2022) for a description of over forty types of cryptocurrency fraud tactics identified to date.

3.2.2 Money Laundering

There are several ways in which cryptocurrency can be used to launder illicit funds. Currency exchanges can be used to trade illicit currency for other digital or traditional fiat currencies (Sanz-Bas et al., 2021). Gambling websites can be used by a player to intentionally lose money to a confederate, or by single players who deposit illicit currency in multiple transactions, then cash out in other digital or fiat currencies (Wronka, 2022). Person to person (P2P) transactions may involve illicit currency, retail websites which sell legal goods as a front, or the purchase of gift, credit or debit cards preloaded with untainted currencies (Dumchikov et al., 2022; Dupuis & Gleason, 2021). Bitcoin ATMs allow users to deposit cash in person and receive Bitcoin credit sent to a wallet address known only by account number and email, with no further identity checks, and the reverse ability to withdraw cash from a Bitcoin account (Hyman, 2015; Sanz-Bas et al., 2021).

Tumblers support laundering by breaking up currency trails on visible blockchain currencies such as Bitcoin by mixing multiple transactions from both legitimate and illicit users into transactions sent to new addresses, minus a service fee, which then send the funds to the customer (Dupuis & Gleason, 2021). Another method of laundering currency is through mainstream video gaming, exploiting a closed-loop system to launder bi-directional currency (Wronka, 2022). Launderers create a new account for a closed currency video game such as Fortnite, Grand Theft Auto or Worlds of Warcraft, fund it using illicit cryptocurrency and offer it for sale in a mainstream marketplace such as eBay for either digital or fiat currency (Sanz-Bas et al., 2021; Scheidegger & Raghubir, 2022).

According to Grauer et al. (2022), approximately $ 8.6 billion in cryptocurrency was laundered in 2021, up $ 2 billion from 2020. Nevertheless, laundering via cryptocurrency is arguably less prevalent than in traditional fiat currency. The amount of crypto laundered in 2020 represented 0.5 % of the market, while the amount of fiat currency laundered in same year made up 5 % of the global GDP (Grauer et al., 2022).

3.2.3 Ransomware

Ransomware is a type of malware which targets an individual computer, a network or a system and takes control of the data, encrypting and blocking the owner's access until they meet a ransom demand, often via cryptocurrency payment (Turner et al., 2019). Double extortion attacks additionally threaten to make data public or available for auction if the ransom demand is not met (Europol, 2021). As of January 2022, Chainalysis had identified USD $ 692 million in funds sent to known ransomware addresses in 2020, a figure which doubled during 2021 as

new ransomware addresses were identified. Estimates for 2021 ransomware activity were $ 602 million, a figure forecast to double if past patterns prove consistent (Grauer et al., 2022). The exponential growth in ransomware attacks in 2021 was also reported by US Financial Crimes Enforcement Network (FinCEN) with a forecast that 2021 ransomware attacks would outpace the previous 10 years combined (US Department of Treasury, 2021). Both FinCen and the analytic firm CipherTrace noted a trend in requests for payment in the privacy coin Monero, with some attackers charging a supplement for payment in Bitcoin. However, Bitcoin remains the primary method of ransomware payment (Jevans et al., 2022; US Department of Treasury, 2021).

3.2.4 Malware

Malware outside the scope of ransomware can include tools to access a user or organization's wallet credentials in order to facilitate theft, to create botnets, defined as multiple private computers networked together and remotely controlled by malicious scripts (Dion-Schwarz et al., 2019), which can support illegal crypto mining (Europol, 2021; Zimba et al., 2021). Illegal crypto mining, also known as cryptojacking, initially attacked computer and smartphone systems to mine Bitcoin (Ali et al., 2018; Sigler, 2018). However, the power required to successfully mine Bitcoin has exponentially increased, with application-specific integrated circuits (ASIC) the system of choice (de Vries & Stoll, 2021). Bitcoin miners are turning to mining farms, where the illegal component of the activity is stealing electricity rather than accessing systems (Dindar & Gül, 2021). Mining via cryptojacking has been more recently used for Monero, with a takedown in late 2021 of the Russia-based botnet Glupteba, which had surreptitiously networked over 1 million machines for Monero mining (Grauer et al., 2022). Monero uses algorithm changes to decrease the computational power required for mining, designed to facilitate mining through standard web browsers (de Vries & Stoll, 2021). A whitepaper released by cybersecurity firm SonicWall detailed use of organization systems for cryptojacking, reported a 709 % increase in attacks on government organizations in 2021, and a 218 % in attacks on healthcare companies (Conner, 2022).

3.2.5 Theft of Cryptocurrency

Cryptocurrency theft can occur at the individual or exchange level, with hacking the primary method of access (Goldsmith et al., 2020). At the individual end, users can be targeted by botnets delivering malware to intercept login details (Europol, 2021). Hackers can alternatively monitor a user's system to identify cryptocurrency transactions in progress, and employ a "clipper" to replace the copied wallet address with their own to divert the funds (Gomez et al., 2022). Bitcoin exchange hacks represent the larger thefts, with the hacks of MtGox in 2014 yielding over USD $ 1 billion in Bitcoin value (Ali et al., 2015), and the Coincheck hack in 2018, which yielded USD $ 530 million (Tsuchiya & Hiramoto, 2021).

Decentralized finance (DeFi) platforms are quickly becoming an area of rapid growth in cryptocurrency theft (Jevans, 2022). Robinson and DePow (2022) estimate stolen cryptocurrency from DeFi platforms at USD $ 10.5 billion for January to November 2021, an increase from $ 1.5 billion the previous year. In 2020, 33 % of total stolen cryptocurrency originated from DeFi platforms, with over half coming from individual users (Grauer & Updegrave, 2021;

Wronka, 2021). An area of DeFi vulnerability is the exploitation of smart contracts, with hackers altering codes within contracts to divert funds (Ndiaye & Konate, 2021). A reversed variation on smart contract theft is a honeypot contract, a seemingly flawed smart contract which freezes funds if a hacker attempts to exploit it by fulfilling the contract (Trozze, Kamps, et al., 2022).

3.2.6 Financing of Terrorism

Terrorist organisations use cryptocurrency funds in three categories: receipt of funds, the transfer or management of funds, and spending (Dion-Schwarz et al., 2019). A study of crypto accounts linked to terrorist organizations between 2017-2021 showed al-Qaeda and the Al-Qassam brigade, the military wing of Hamas, to be the most visibly active crypto users (Grauer et al., 2022). Seizures by the US and Israeli governments were announced (Teichmann & Falker, 2021; US Department of Justice, 2021); however, despite government interruptions it is estimated that Al-Qassam had raised USD $ 7.7 million in multiple cryptocurrencies (Carlisle, 2022). The US DOJ (2021) also announced the interruption of a scheme selling phony personal protective equipment during the COVID-19 pandemic, with the proceeds funnelled to ISIS operations.

It has been argued that some terrorist organizations are deterred from using cryptocurrencies due to lack of understanding of blockchain technology, the question of whether trading in digital assets is permissible under religious law, and lack of confidence in cryptocurrency value stability due to market volatility (Kethineni & Cao, 2020; Kfir, 2020). Others argue that the minimal evidence of terrorist activity using cryptocurrencies reflects a lack of detection, or that given what is known about methods of terrorist financing, that a rise in use of cryptos should be expected (Andrianova, 2020; Dyntu & Dykyj, 2021; Paul, 2018; Şen & Akarslan, 2018).

3.2.7 Geo-Political Acts and Evasion of Sanctions

While commanding a smaller share of the illicit crypto market, cryptocurrency can be used within acts of war, such as a cyber-attack perpetrated by Russia against Ukraine concurrently with the January 2022 invasion, which was disguised as a ransomware attack demanding cryptocurrency payment (Lewis, 2022; Microsoft Security, 2022). Cryptocurrencies can be used by government-backed organizations either to avoid international sanctions, or to facilitate arms dealing (US Department of Justice, 2021). The decentralized nature of cryptocurrency trade offers a workaround for sanctioned governments to transact internationally and also raise funds via theft or hacking (Turner et al., 2019). Examples include North Korea's Lazarus Group hack of the online game Axie Infinity, which netted USD $ 540 million (Vigna, 2022), and their previous WannaCry 2.0 ransomware heist generated approximately USD $4 billion (Schaake, 2020). Venezuela and Iran have both operated cryptomining operations to raise funds, which also allows them to exploit the availability of inexpensive electricity (Carlisle, 2022). Mining has been particularly lucrative in Iran, where it is estimated that approximately USD $ 186 million in Bitcoin has been mined, with the bulk of the funds moving since 2021 (Grauer et al., 2022).

3.2.8 Darknet Markets and Payment for Illegal Services

In 2021, darknet markets transacted USD $ 2.1 billion in cryptocurrencies, with the bulk of payments ($ 1.8b) made in markets for illegal drugs and the balance in fraud markets, which support crime-as-a-service tools such as ransomware kits or stolen credentials for crypto or fiat currency (Grauer et al., 2022). These figures are adjusted as additional illicit accounts are identified, and represent a steady increase from an estimated USD $ 1 billion in 2019, and $ 1.7 billion in 2020 (Bahamazava & Nanda, 2022; Grauer & Updegrave, 2021). Additionally, in 2021 approximately USD $112 million was spent in P2P transactions associated with darknet market activity, indicating buyers and sellers may have initially transacted within markets and then moved to direct sales (Grauer et al., 2022).

In this category, cryptocurrency is a method of payment for illegal products or services, rather than a direct target or vehicle. Darknet markets may flourish, come to the attention of authorities and be shut down, with new markets popping up in their wake. Examples include Silk Road from 2011-2013 (Robertson, 2018), Agora 2013-2015 (Baravalle et al., 2016) and Hydra 2015-2022 (US Department of Justice, 2022). Cryptocurrencies are attractive to illicit vendors due to anonymity and global reach, with a clear progression away from Bitcoin to privacy coins such as Monero (Bahamazava & Nanda, 2022). Some darknet markets in 2021 including Archetyp and the now-closed White House began to require payment in Monero (Grauer et al., 2022).

While illicit substances and illegally obtained prescription drugs make up a large part of darknet market traffic (Robertson, 2018), other services are offered with payment in cryptocurrency. The South Korean sex trafficking ring Nth Room involved the exploitation of women and children with payment in cryptocurrency and content distributed via the encrypted messaging app Telegram (Ewen, 2020). Further examples include payments for counterfeit documents (Baravalle et al., 2016), illicit trafficking in protected goods such as the antiquities market (Paul, 2018), or paying for illegal services such as murder-for-hire (Cortez, 2021; Europol Spotlight, 2021).

3.3 How Does the Cryptocurrency Market Influence Digital Crime?

A primary way in which cryptocurrency markets can influence digital crime is ease of access and removal of typical obstacles faced when transacting in fiat currencies (Teichmann & Falker, 2021). It has been argued that use of cryptocurrency allows criminal activity to be timeless, borderless and unregulated (Prytula et al., 2021). A shift in criminal activity from centralized to decentralized markets may also be occurring as a reaction to increasing regulatory oversight in centralized markets (Robinson & DePow, 2022). Decentralized finance exchanges (DEX) can allow criminals to bypass anti-money-laundering and know-your-customer requirements by facilitating P2P trades which do not pass through a third-party central exchange such as Binance or Coinbase (Aspris et al., 2021; Carlisle, 2022; Klimek, 2020). 97 % of the USD $ 1.3 billion in stolen cryptocurrency in Q1 of 2022 was taken from DeFi platforms, according to a report by Chainalysis (2022). The rise of privacy coins such as Monero, Dash, ZCash employ additional security elements, either embedded or as opt-in features, making it more difficult to link accounts to users (Bele, 2021; Jevans et al., 2022; Silfversten et al., 2020). Some central cryptocurrency exchanges such as Coinbase, Bittrex and Kraken have delisted

privacy coins, further marginalizing their use (Jha, 2022). The Financial Action Task Force (2020) cites the pattern of trading traditional cryptocurrencies such as Bitcoin to privacy coins, and the movement between centralized and decentralized exchanges as red flags for money laundering or the financing of terrorism.

Financial influencers, known as finfluencers, offer financial advice aimed at Gen Z and millennial investors on platforms such as TikTok, Instagram and YouTube, a practice beginning to be regulated (ASIC, 2022; Battin, 2022). While some finfluencer advice is legitimate, the opportunity for misleading or fraudulent investment scams is known (Mackenzie, 2022). The US Federal Trade Commission (2022) reported that nearly half the reported cases of crypto fraud in 2021 originated on social media platforms, the largest of which was Instagram at 32 %. Messaging services such as Telegram and Discord have been used as vehicles for crypto "pump and dump" investment schemes on central exchanges such as Binance or Bittrex (Hamrick et al., 2021; Kamps & Kleinberg, 2018).

An interesting hypothesis has been floated that the public perception of criminal activity in cryptocurrency markets seems to be a market driver. When government seizures, new policies, or enhanced security measures are announced, values have historically gone up (Abramova & Bohme, 2021; Caporale et al., 2020; Klimek, 2020). In the opposite direction, natural language processing was used to study the effects of negative news within the crypto-crime discourse on Bitcoin values in online forums. Findings include correlation between price dips and the Quadriga bankruptcy, the Coincheck hack and the shutdown of illicit cryptomining facilities in Iran (Coulter, 2022). It remains to be seen whether this pattern will continue following 2022 value crashes. Mid-year analysis of the criminal cryptocurrency market by Atlas VPN seems to indicate that crypto theft is increasing, despite market volatility which may be influenced by public perception (Ruth, 2022). The report detailed that in the first half of 2022, crypto hacks resulted in USD $ 1.97 billion in losses, the largest of which was the Ethereum Axie Infinity hack.

Study of an early dark net market, Silk Road, led researchers to question whether increasing uptake of cryptocurrencies would influence the growth of larger, transnational drug markets (Aldridge & Décary-Hétu, 2016). A further study identified that many smaller cryptomarkets have arisen within the countries of product consumption, suggesting this pattern may be influenced by the perception that product shipping across international borders remains risky (Demant et al., 2018). Bahamazava and Nanda (2022) note the local market trend as well as a gradual shift in dark net drug payments from Bitcoin to privacy coins.

Within the criminological study of cryptocurrency, it is relevant to consider the evidence of what has happened, the forecasters predicting what may happen, and the sceptics who argue what may not happen. Despite numerous warnings of the use of cryptocurrency markets for terrorism financing, some suggest that the perception of market volatility is potentially a deterrent to wider uptake (Kfir, 2020). Blockchain analytic firms such as Chainalysis and CipherTrace continue to show that not only is the percentage of illicit crypto trade low relative to the entire market cap, but also that illicit activity is growing at a slower rate than the total market, and further, that large portions of illicit funds are held by a relatively low number of criminal whale accounts (Grauer et al., 2022; Jevans et al., 2022). Others argue that criminal activity related to cryptocurrency is a niche issue which will be increasingly regulated with evolving technology (Butler, 2020; Litan, 2022; Sexton, 2021).

3.4 What is the Law Enforcement Response?

Hurdles encountered by law enforcement from the local to the international level include formalising consistent definitions of cryptocurrencies, cooperation with other jurisdictions at a transnational level, and the ability to detect illicit activity and identify the perpetrators. Given the speed of developing technology, a cat-and-mouse game of evasive techniques appears to be in perpetual motion. Nevertheless, a growing number of market shutdowns, seizures, arrests and successful prosecutions are occurring.

Fletcher et al. (2021) highlighted the difference across jurisdictions with the naming and classification of cryptocurrencies, noting that some countries define crypto as a form of currency, a digital asset or a technological tool. Jurisdictions also have varying approaches to the legislation of crypto trade, with some countries such as China, Turkey and Egypt banning the use of cryptocurrencies altogether, others such as Iran banning trade but licensing mining, or prohibition without enforcement, such as Mexico or Bolivia (Hammond & Ehret, 2022). Russia's position on cryptocurrency is evolving, with a previously implemented ban on the use of crypto as a payment method extended in July 2022 to include non-fungible tokens (NFT; Liu, 2022). When attempting to prosecute cryptocurrency-related crimes, jurisdictions have used financial crime, cybercrime or organized crime statutes with varying degrees of success (Klimek, 2020; Reddy, 2020; Soana, 2022). As an example, arguments within the Florida case of State v. Espinoza hinged on whether a seller of Bitcoin fell within the existing statute's definition of a "money transmitter" (Whiteman, 2020). An analysis of 31 cryptocurrency-related cases decided in the US federal district and circuit courts revealed a common defence that the defendants' actions were not illegal as they were not covered by existing legislation (Nolasco Braaten & Vaughn, 2021). An analysis of 58 criminal cases in various regions of the Russian Federation revealed some convictions, in particular where sufficient evidence of fraud was submitted or theft of electricity for crypto mining could be proven, or suspension of investigations due to lack of ability to detect transactions or inability to utilise subject matter experts (Pushkarev et al., 2020). An example of successful use of a long-standing statute in a cryptocurrency case is the US Racketeer Influenced and Corrupt Organizations Act (RICO). Conspiracy charges against the owner and an employee led to multiple indictments and a conviction following the closure of AlphaBay, a darknet drug market (UNODOC, 2020; US Department of Justice, 2020). Further analysis of the potential application of RICO to other cryptocurrency cases, however, noted obstacles including the transnational nature of crypto as well as the RICO condition requiring that organized crime infiltrate a legitimate crypto business, suggesting the success of cases like AlphaBay may be the exception rather than the rule (Klimek, 2020).

It has been acknowledged that cryptocurrency technology is evolving faster than the law (Bokovnya et al., 2020), with court outcomes often hinging on details such as whether cryptocurrency is money, or whether blockchain evidence is admissible (Trozze, Davies, et al., 2022; Whiteman, 2020). The US has introduced a Cryptocurrency Enforcement Framework with a dedicated investigation team focused on crypto laundering, uses of mixers and tumblers, and crimes related to cryptocurrency exchanges (Meyerowitz, 2022). Jurisdictions are scrambling to update their legislation to effectively prosecute cryptocurrency crimes, from how cryptocurrencies are classified to whether they can be seized and how seized funds can be used (Dumchikov et al., 2022; Houben & Snyers, 2018; Voskobitova et al., 2021; Yanchao, 2021). A

unique move by the government of Lichtenstein introduced regulation on blockchain technology as a method of regulating cryptocurrency trade (Teichmann & Falker, 2021), which has been noted by other legal analysts as a potentially promising basis for international legislative standards (Voskobitova et al., 2021).

Some jurisdictions have partnered with private enterprise in order to obtain investigative and defensive tools to identify criminals and protect consumers. Examples include Ukraine's collaboration with Cisco to investigate phishing attacks (Holub et al., 2018) or the US Internal Revenue Service offering financial incentives to multiple blockchain security firms for any successful subversion of the anonymizing features of the privacy coin Monero (Culafi, 2022), effectively creating a system of digital bounty hunting. Malaysia adopted a process model of digital forensics in collaboration with commercial enterprise; however, a survey of investigators found the current system lacking, in that not all officers had sufficient training to use the tools and gaps exist between what data can be detected and what is admissible in court proceedings (Taylor et al., 2021b).

Seizure of illicit cryptocurrency is a motivator for law enforcement to develop the technological skills needed for successful detection and identification (Collins, 2022; Li et al., 2021). The UK's National Crime Agency seized an estimated GBP £ 322 million in cryptocurrency between 2018-2022 based on the Proceeds of Crime Act 2002; however, as cryptocurrency is considered non-cash property, a conviction is required for seizure under the act (Sparkes, 2022). In Australia, Victorian police seized AUD $ 8.5 million in crypto linked to dark net drug markets in 2021, the largest seizure to date in Australia (Smith, 2021). The US completed the first known seizure of illicit cryptocurrency in 2013 when the dark net market Silk Road was shuttered (Voskobitova et al., 2021), and continues to lead the world in illicit crypto seizure with USD $ 3.2 billion seized in 2021 (Collins, 2022). Both the US and Israeli governments have successfully seized cryptocurrencies raised to fund terrorism by al-Qaeda and Hamas, using blockchain analysis (Grauer et al., 2022). It has been suggested in an article focused on Bitcoin seizures in Canada that opportunities exist for provision of tools and training to law enforcement for confiscation, as well as education to law enforcement on best practices related to the secure holding of seized cryptocurrency (King & Warrack, 2018).

4. Discussion & Conclusion

It has been argued by academic security researchers, industry experts and governments that consistent global regulation and inter-jurisdictional cooperation is necessary to combat crypto-related crime (Europol, 2021; Jevans, 2022; Kfir, 2020; Reddy, 2020; Teichmann & Falker, 2021; Voskobitova et al., 2021). Irwin and Dawson (2019) recommended a combination of the approaches of Europe, the Americas and Australia to develop a consistent global framework for addressing illicit cryptocurrency activity. The Financial Action Task Force (2021a), formed as a global watchdog for financial crimes, could potentially hold this function and offer templates for global regulation.

A further common recommendation is that law enforcement investigators should improve their technological and analytic skills (Kuzuno & Tziakouris, 2018), and also partner with engineers and developers in the private and academic sectors in order to develop effective and user-friendly investigative tools (Soana, 2022; Taylor, Omar, et al., 2021). At a local level, officers in Pune, India engaged in self-directed blockchain learning which led to the detection of

cryptocurrency fraud and an arrest; however, without the necessary legal statues in place, they were unable to hold the perpetrators or prevent them moving funds (Qureshi, 2022). At a national level, the UK's National Crime Agency and the US Department of Justice have successfully seized illicit crypto assets related to the Silk Road closure and shut down the darknet child sexual abuse market Welcome to Video with intelligence gained by the use of private sector tools (Chainalysis, 2020; Grauer & Updegrave, 2021).

Academic security engineers have proposed and continue to develop numerous solutions for corporations, law enforcement and individual users. Methodology papers returned in the current literature review search results are detailed in Table 2 below. Additionally, recommendations are made for further development of solutions. It is argued that a vital investigative tool is de-anonymization of transactions (Dyntu & Dykyj, 2021; Han et al., 2020). The ability to detect and interrupt malicious smart contract execution has also been highlighted (Kamidoi et al., 2021; Ndiaye & Konate, 2021). It was additionally recommended that developers of tech solutions integrate legislation as part of their systems-building; for example, anti-money laundering tools could be developed with consideration of current statues and frameworks (Kolachala et al., 2021). The search terms of the current review did not target disruptive solutions; however, the number of potential solutions organically returned suggests further academic research targeted to digital disruption would contribute to the emerging body of literature. Ongoing review of emerging solution-focused literature could support and inform the work of legislators and agencies as well as blockchain security firms.

Table 2: Digital Investigative Methods

Author(s)	**Solution**
Akcora et al. (2020); Mantri et al. (2022)	Ransomware attack prediction
Hairil et al. (2021)	Ransomware detection
Dindar & Gül (2021); Rahimi et al. (2021)	Detection of illicit cryptomining facilities
Kaushik and Dahiya (2021)	Automatic investigation of Bitcoin balances and addresses
Li et al. (2022)	Detection of Ethereum phishing scams
Liu et al. (2022); Sun et al. (2019); Xia et al. (2021)	Classification or flagging of accounts based on behaviour
Lv et al. (2020); Wallace & Scott-Hayward (2020); Zheng et al. (2018)	Transaction de-anonymization
Phetsouvanh et al. (2019)	Identification of extortion transaction patterns
Singh et al. (2021); Tan et al. (2021)	Fraud detection
Taylor, Ariffin, et al. (2021)	Method of freezing cryptowallets
Wecksten et al. (2017)	Recovery method post-ransomware attack
Zhang et al. (2020)	Identification of gambling or mining communities

Note. These results are not exhaustive, as the search terms within the current review did not explicitly target technological solutions.

The need to identify, disrupt or prosecute criminals must be balanced with citizens' rights to privacy and autonomy; this is true in both the traditional fiat currency and the cryptocurrency landscapes (Dyson et al., 2018). Keller et al. (2021) proposed a method of collaborative de-anonymization, where law enforcement might publicly request information related to specific cryptocurrency offenses, allowing users to decide whether to share pertinent information, a digital version of a global neighbourhood watch or crime tips line. It has been argued that the

elements of pseudo-anonymity and decentralization not only facilitate criminal activities, but also promote financial inclusion, allowing low-income or otherwise marginalized individuals greater access to financial systems (Bailey et al., 2021). While some countries have attempted to ban cryptocurrencies (Hammond & Ehret, 2022), it has been argued that widespread bans might simply lead to development of other alternative financial systems (Hendrickson & Luther, 2021). The move from centralized to decentralized exchanges is also expected to grow, with the need for specific DeFi regulation (Robinson & DePow, 2022; Wronka, 2021). Kreminskyi et al. (2021) proposed that a solution to controlling criminal activity in a decentralized, transnational system could be to utilise the same qualities through international cooperation to implement a decentralized management system.

In the wake of the significant cryptocurrency devaluation in 2022, some have questioned whether the entire market will dwindle to an end (Arti, 2022). Others argue that cryptocurrency is merely experiencing growing pains as it moves from an unregulated and speculative marketplace to one which is more regulated, with both short-term volatility and long-term growth to be expected (Coppola, 2022; Gailey & Haar, 2022). The digital research firm Gartner has forecast that criminal cryptocurrency activity may drop as much as 30 % in the next two years, basing this prediction on the increasing use of emerging blockchain intelligence tools by law enforcement, increasing government regulation, and buy-in from virtual asset service providers such as cryptocurrency exchanges, who may see increased security as a driver of mainstream adoption of cryptocurrencies (Litan, 2022). Whether or not Gartner's basis for future drops in criminal activity proves correct, it has already been identified that the rate of criminal activity is decreasing by volume as a percentage of the entire market (Grauer et al., 2022; Grauer & Updegrave, 2021).

4.1 Conclusion

Whilst this paper has drawn on a secondary data approach to research through the utilisation of existing scientific literature and evidence which engenders several limitations such as limited evaluation of selected literature used, this does not detract from the value of the work. It is clear that the illicit cryptocurrency landscape is evolving at a speed difficult for traditional law enforcement to match without support and collaboration from other industries. To effectively address criminal use of cryptocurrencies, officers must be supported to develop the skills and technical tools required to investigate activity. Additionally, sufficient legal and judicial infrastructure must be in place to prosecute and convict those apprehended, including consistent definitions or classifications of digital assets, legislation to allow surveillance, apprehension, seizure of evidence and prosecution. International cooperation to identify consistent standards and thresholds of legal and illegal activities and products should be prioritised. The emerging blockchain intelligence industry could include consideration of regulatory frameworks from the ground-up when designing their investigative products. Academic researchers can provide a bridge of knowledge sharing between commerce and government by providing ongoing targeted research, to aggregate and review the evolving nature of cryptocurrency offending and emerging disruptive digital solutions. The decentralized, collaborative format of cryptocurrency and blockchain technology allows global inclusion and democracy, moving the traditional locus of control away from traditional financial gatekeepers. Stronger partnerships

between technological innovators in private or academic settings, legislators, and law enforcement could apply and utilise these same principles of decentralization to collaborate on solutions to effectively address criminal activity.

Literaturverzeichnis

Abramova, S., & Bohme, R. (2021). Out of the dark: The effect of law enforcement actions on cryptocurrency market prices. *2021 APWG Symposium on Electronic Crime Research* (eCrime), 1-11. https://doi.org/10.1109/eCrime54498.2021.9738787

ACCC. (2022, June 6th). *Australians are losing more money to investment scams*. Scamwatch. https://www.scamwatch.gov.au/news-alerts/australians-are-losing-more-money-to-investment-scams

Ahmed-Rengers, M., Shumailov, I. & Anderson, R. (2020). Tendrils of crime: Visualizing the diffusion of stolen bitcoins. In G. Cybenko, D. Pym, & B. Fila (Eds.), *Graphical Models for Security. GraMSec 2018. Lecture Notes in Computer Science*. Cornell University Library. https://doi.org/10.1007/978-3-030-15465-3_1

Akcora, C. G., Li, Y., Gel, Y. R. & Kantarcioglu, M. (2020, July 11th-17th). Bitcoin heist: Topological data analysis for ransomware prediction on the bitcoin blockchain IJCAI. *International Joint Conference on Artificial Intelligence*, https://www.scopus.com/inward/record.uri?eid=2-s2.0-85095529010&partnerID=40&md5=f3013c86ba859a0f97fcb07ce37ee76d

Aldridge, J. & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy, 35*, 7-15. https://doi.org/https://doi.org/10.1016/j.drugpo.2016.04.020

Ali, S. T., Clarke, D. & McCorry, P. (2015). *Bitcoin: Perils of an unregulated global p2p currency Lecture Notes in Computer Science 23rd International Workshop on Security Protocols*, Sidney Sussex College.

Ali, S. T., McCorry, P., Lee, P. H. J. & Hao, F. (2018). ZombieCoin 2.0: Managing next-generation botnets using Bitcoin. *International Journal of Information Security, 17*(4), 411-422. https://doi.org/10.1007/s10207-017-0379-8

Andrianova, A. (2020). Countering the financing of terrorism in the conditions of digital economy. In M. Vochozka, S. Ashmarina, & A. Mesquita (Eds.), *Digital transformation of the economy: Challenges, trends and new opportunities* (Vol. 908, pp. 20-31). Springer Verlag. https://doi.org/10.1007/978-3-030-11367-4_2

Aquisdata (2022). *Global cryptocurrency and exchanges. Global Industry SnapShots*. http://ezproxy.lib.uts.edu.au/login?url=https://www.proquest.com/trade-journals/global-cryptocurrency-exchanges-updated-10/docview/2619336114/se-2?accountid=17095

Arti (2022, June 28th). *Bitcoin is dead in 2022! Analysts spell the unreasonable demise*. Analytics Insight. https://www.analyticsinsight.net/bitcoin-is-dead-in-2022-analysts-spell-the-unreasonable-demise/

ASIC (2022, March 21st). Discussing financial products and services online. (INFO 269). Canberra: Australian Securities and Investments Commission. https://asic.gov.au/regulatory-resources/financial-services/giving-financial-product-advice/discussing-financial-products-and-services-online/

Aspris, A., Foley, S., Svec, J. & Wang, L. (2021). Decentralized exchanges: The "wild west" of cryptocurrency trading. *International Review of Financial Analysis, 77*, 101845. https://doi.org/10.1016/j.irfa.2021.101845

Bahamazava, K. & Nanda, R. (2022). The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence. *Forensic Science International: Digital Investigation, 40*, 1-9. 301377. https://doi.org/https://doi.org/10.1016/j.fsidi.2022.301377

Bailey, A. M., Rettler, B. & Warmke, C. (2021). Philosophy, politics, and economics of cryptocurrency II: The moral landscape of monetary design. *Philosophy Compass, 16*(11), e12784. https://doi.org/https://doi.org/10.1111/phc3.12784

Baravalle, A., Lopez, M.S., & Lee, S.W. (2016). Mining the Dark Web: Drugs and Fake Ids. *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, 350-356.

Battin, D. (2022, May 7th). Finfluencers, meme stocks, and regulatory response. *Review of Banking & Financial Law*. https://www.bu.edu/rbfl/2022/03/28/finfluencers-meme-stocks-and-regulatory-response/

Bele, J. L. (2021). *Cryptocurrencies as facilitators of cybercrime The 3rd Eastern European Conference of Management and Economics (EECME 2021) – Sustainable Development in Modern Knowledge Society*, Les Ulis. https://doi.org/10.1051/shsconf/202111101005

Bokovnya, A. Y., Shutova, A. A., Zhukova, T. G. & Ryabova, L. V. (2020). Legal measures for crimes in the field of cryptocurrency billing. *Utopia y Praxis Latinoamericana, 25(*Extra 7), 270-275. https://doi.org/10.5281/zenodo.4009713

Butler, S. (2020). *Cyber 9/11 will not take place: A user perspective of bitcoin and cryptocurrencies from underground and dark net forums 10th International Workshop on Socio-Technical Aspects in Security and Trust* (STAST), https://doi.org/10.1007/978-3-030-79318-0_8

Caporale, G. M., Woo-Young, K., Spagnolo, F. & Spagnolo, N. (2020). *Cyber-attacks, cryptocurrencies, and cyber security*. https://www.cesifo.org/DocDL/cesifo1_wp8124_2.pdf

Carlisle, D. (2022, March 20th). *Preventing financial crime in cryptoassets*. Elliptic. https://www.elliptic.co/resources/typologies-report-2022

Carlisle, D. & Izenman, K. (2019, April 14th). *Closing the crypto gap: Guidance for countering North Korean cryptocurrency activity in southeast Asia*. https://static.rusi.org/20190412_closing_the_crypto_gap_web.pdf

CBS (2021, March 1st). *Sharp drop in traditional crime*. https://www.cbs.nl/en-gb/news/2021/09/sharp-drop-in-traditional-crime

Chainalysis (2020). Chainalysis in action: US government agencies seize more than $1 billion in cryptocurrency connected to infamous darknet market silk road. *Chainalysis*. https://blog.chainalysis.com/reports/silk-road-doj-seizure-november-2020/

Chainalysis (2022, April 14th). Defi hacks are on the rise. *Chainalysis*. https://blog.chainalysis.com/reports/2022-defi-hacks/

CoinMarketCap (2022). *Glocal cryptocurrency market cap*. https://coinmarketcap.com/charts/

Collins, J. (2022, June 16th). *Crypto, crime and control: Cryptocurrencies as an enabler of organized crime. Global Initiative Against Transnational Organized Crime*. https://globalinitiative.net/wp-content/uploads/2022/06/GITOC-Crypto-crime-and-control-Cryptocurrencies-as-an-enabler-of-organized-crime.pdf

Conner, B. (2022, February 17th). 2022 Sonicwall cyber threat report. *Sonic Wall*. https://www.sonicwall.com/resources/white-papers/2022-sonicwall-cyber-threat-report/

Cooper, G. (2021). Virtual property: Trusts of cryptocurrencies and other digital assets. *Trusts and Trustees, 27*(7), 622-631. https://doi.org/10.1093/tandt/ttab027

Coppola, F. (2022, June 29th). Why this crypto crash is different. *CoinDesk*. https://www.coindesk.com/layer2/futureofmoney/2022/06/29/why-this-crypto-crash-is-different/

Cortez, C. A. (2021). Bitcoin searches and preserving the third-party doctrine. *St. Mary's Law Journal, 52*(1), 153-186. https://commons.stmarytx.edu/thestmaryslawjournal/vol52/iss1/5

Coulter, K. A. (2022). The impact of news media on Bitcoin prices: modelling data driven discourses in the crypto-economy with natural language processing. *Royal Society Open Science, 9*(4), Article 220276. https://doi.org/10.1098/rsos.220276

Culafi, A. (2022, January 24th). Monero and the complicated world of privacy coins. *Tech Target*. https://www.techtarget.com/searchsecurity/news/252512394/Monero-and-the-complicated-world-of-privacy-coins

De Vries, A., & Stoll, C. (2021). Bitcoin's growing e-waste problem. *Resources, Conservation and Recycling*, *175*, 105901.

Demant, J., Munksgaard, R., Décary-Hétu, D. & Aldridge, J. (2018). Going local on a global platform: A critical analysis of the transformative potential of cryptomarkets for organized illicit drug crime. *International Criminal Justice Review, 28*(3), 255-274. https://doi.org/10.1177/1057567718769719

Dindar, B., & Gül, Ö. (2022). The detection of illicit cryptocurrency mining farms with innovative approaches for the prevention of electricity theft. *Energy & Environment*, *33*(8), 1663–1678. https://doi.org/10.1177/0958305X211045066

Dion-Schwarz, C., Manheim, D. & Johnston, P.B. (2019). *Terrorist use of cryptocurrencies: Technical and organizational barriers and future threats*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf

Dumchikov, M., Reznik, O. and Bondarenko, O. (2022), "Peculiarities of countering legalization of criminal income with the help of virtual assets: legislative regulation and practical implementation", *Journal of Money Laundering Control*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JMLC-12-2021-0135

Dupuis, D. & Gleason, K. (2021). Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime, 28*(1), 60-74. https://doi.org/10.1108/JFC-06-2020-0113

Dyntu, V. & Dykyj, O. (2021). Cryptocurrency as an instrument of terrorist financing. *Baltic Journal of Economic Studies, 7*(5), 67-72. https://doi.org/10.30525/2256-0742/2021-7-5-67-72

Dyson, S., Buchanan, W. J. & Bell, L. (2018). The challenges of investigating cryptocurrencies and blockchain related crime. *The Journal of The British Blockchain Association, 1*(2), 1-6. https://doi.org/https://doi.org/10.31585/jbba-1-2-(8)2018

Europol (2021, November 11th). Internet organised crime threat assessment. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Europol (2021), Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.

Ewen, P. (2021). The Finance of Sex Trafficking and Impact of COVID-19. *Journal of Modern Slavery: A Multidisciplinary Exploration of Human Trafficking Solutions*, *6*(2). 1-11.

Financial Action Task Force (2020, September 14th). *Virtual assets red flag indicators of money laundering and terrorist financing*. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf

Financial Action Task Force (2021a). *Second 12-month review virtual assets and VASPs*. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

Financial Action Task Force (2021b, October 28th). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

Fletcher, E., Larkin, C. & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance, 56*, Article 101387. https://doi.org/10.1016/j.ribaf.2021.101387

Foley, S., Karlsen, J. R. & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies, 32*(5), 1798-1853. https://doi.org/10.1093/rfs/hhz015

Gailey, A. & Haar, R. (2022, October 31st). The future of cryptocurrency: 8 experts share predictions for the second half of 2022. *Time*. https://time.com/nextadvisor/investing/cryptocurrency/future-of-cryptocurrency/

Gladstone, N. (2019, January 21st). *Crime in NSW has been dropping for more than a decade. This is why*. https://www.smh.com.au/national/nsw/crime-in-nsw-has-been-dropping-for-more-than-a-decade-this-is-why-20181108-p50eq4.html

Goldsmith, D., Grauer, K. & Shmalo, Y. (2020). Analyzing hack subnetworks in the bitcoin transaction graph. *Applied Network Science, 5*(1), Article 22. https://doi.org/10.1007/s41109-020-00261-7

Gomez, G., Moreno-Sanchez, P. A. & Caballero, J. (2022). Detecting cybercriminal bitcoin relationships through backwards exploration. *ArXiv, abs/* 2206.00375. https://doi.org/10.48550/arXiv.2206.00375

Grant, M. J. & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal, 26*(2), 91-108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Grauer, K., Kueshner, W., & Updegrave, H. (2022, February 9th). Crypto crime report. *Chainalysis*. https://go.chainalysis.com/2022-crypto-crime-report.html

Grauer, K., & Updegrave, H. (2021, February 16th). Crypto crime report. *Chainalysis*. https://go.chainalysis.com/2021-Crypto-Crime-Report.html

Hairil, Cahyani, N. D. W. & Nuha, H. H. (2021). *Ransomware detection on bitcoin transactions using artificial neural network methods* [Conference Paper]. 2021 9th International Conference on Information and Communication Technology (ICoICT), https://doi.org/10.1109/ICoICT52021.2021.9527414

Hammond, S. & Ehret, T. (2022, April 1st). Cryptocurrency regulations by country. Thomson Reuters. https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf

Hamrick, J. T., Rouhi, F., Mukherjee, A., Feder, A., Gandal, N., Moore, T. & Vasek, M. (2021). An examination of the cryptocurrency pump-and-dump ecosystem. *Information Processing & Management, 58*(4), 102506. https://doi.org/10.1016/j.ipm.2021.102506

Han, W. L., Duong, V., Nguyen, L., Mier, C. & Ieee. (2020, May 26-27). *Darknet and bitcoin de-anonymization: Emerging development Zooming Innovation in Consumer Technologies Conference (ZINC)*. https://doi.org/10.1109/ZINC50678.2020.9161431

Harkin, D., Whelan, C. & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. Police Practice and Research, 19(6), 519-536. https://doi.org/10.1080/15614263.2018.1507889

Hendrickson, J. R., & Luther, W. J. (2022). Cash, crime, and cryptocurrencies. *The Quarterly Review of Economics and Finance*, *85*, 200-207.

Holub, A., O'Connor, J. & Ieee. (2018). *Coinhoarder: Tracking a Ukrainian bitcoin phishing ring dns style APWG Symposium on Electronic Crime Research (eCrime),* San Diego, CA. https://doi.org/10.1109/ECRIME.2018.8376207

Horsman, G. (2017). Can we continue to effectively police digital crime? *Science & Justice, 57*(6), 448-454. https://doi.org/10.1016/j.scijus.2017.06.001

Houben, R. & Snyers, A. (2018, September 6th). Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

Hyman, M. (2015). Bitcoin atm: A criminal's laundromat for cleaning money. *St. Thomas Law Review, 27*(2), 287-308.

Irwin, A. S. M. & Dawson, C. (2019). Following the cyber money trail. *Journal of Money Laundering Control, 22*(1), 110-131. https://doi.org/https://doi.org/10.1108/JMLC-08-2017-0041

Jevans, A., Still, J. & Barragan, J. (2022, April 18th). Current trends in ransomware with special notes on Monero usage. *CipherTrace*. https://ciphertrace.com/current-trends-ransomware-monero/

Jevans, D. (2022, October 22nd). Cryptocurrency crime and anti-money laundering report. *CipherTrace*. https://ciphertrace.com/crime-and-anti-money-laundering-report/

Jha, P. (2022, June 16th). Regulations and exchange delistings put future of private cryptocurrencies in doubt. *Coin Telegraph: The Future of Money*: News. https://cointelegraph.com/news/regulations-and-exchange-delistings-put-future-of-private-cryptocurrencies-in-doubt

Jin, J. & Vinella, P. (2022). *Some of the challenges facing DeFi for mass adoption*. Preprint. https://www.researchgate.net/profile/Peter-Vinella/publication/361477227_Some_of_the_Challenges_Facing_DeFi_for_Mass_Adoption_Working_Paper_1/links/62b3c7e4d49f803365b2b513/Some-of-the-Challenges-Facing-DeFi-for-Mass-Adoption-Working-Paper-1.pdf

Kamidoi, Y., Yamauchi, R. & Wakabayashi, S. (2021). A protocol for preventing transaction commitment without recipient's authorization on blockchain and its implementation. *IEEE Access*, 9, 24390-24405. https://doi.org/10.1109/access.2021.3056623

Kamps, J. & Kleinberg, B. (2018). To the moon: Defining and detecting cryptocurrency pump-and-dumps. *Crime Science, 7*(1), Article 18. https://doi.org/10.1186/s40163-018-0093-5

Kaushik, K. & Dahiya, S. (2021). An automated abstract approach for investigating bitcoin balances and wallet addresses Proceedings of the 2021 10th International Conference on System Modeling and Advancement in Research Trends, *SMART*, 444-448. https://doi.org/10.1109/SMART52563.2021.9676254

Keller, P., Florian, M. & Bohme, R. (2021). Collaborative deanonymization Conference on Financial Cryptography and Data Security (FC), https://doi.org/10.1007/978-3-662-63958-0_3

Kethineni, S. & Cao, Y. (2020). The rise in popularity of cryptocurrency and associated criminal activity. International *Criminal Justice Review, 30*(3), 325-344. https://doi.org/10.1177/1057567719827051

Kfir, I. (2020). Cryptocurrencies, national security, crime and terrorism. *Comparative Strategy, 39*(2), 113-127. https://doi.org/10.1080/01495933.2020.1718983

King, D. & Warrack, P. (2018, June 26th). *Real considerations for law enforcement in seizing virtual currency. ACAMS Today: The Magazine for Career-minded Professionals in the Anti-Money Laundering Field.* https://www.acamstoday.org/real-considerations-for-law-enforcement-in-seizing-virtual-currency/

Klimek, A. R. (2020). Reinvesting in RICO with cryptocurrencies: Using cryptocurrency networks to prove RICO's enterprise requirement. *Washington and Lee Law Review, 77*(1), 509-550. https://scholarlycommons.law.wlu.edu/wlulr/vol77/iss1/9/

Kolachala, K., Simsek, E., Ababneh, M., Vishwanathan, R. & Assoc Comp, M. (2021, August 17th). *SoK: Money laundering in cryptocurrencies 16th International Conference on Availability, Reliability and Security (ARES)*, https://doi.org/10.1145/3465481.3465774

Kreminskyi, O., Kuzmenko, O., Antoniuk, A. & Smahlo, O. (2021). International cooperation in the investigation of economic crimes related to cryptocurrency circulation. *Estudios de Economia Aplicada, 39*(6), 1-13. https://doi.org/10.25115/eea.v39i6.5247

Kuzuno, H., & Tziakouris, G. (2018). Ad-hoc analytical framework of bitcoin investigations for law enforcement. IEICE *Transactions on Information and Systems, E101D*(11), 2644-2657. https://doi.org/10.1587/transinf.2017ICP0007

Lewis, J. (2022, June 16th). *Cyber war and Ukraine. Center for Strategic and Global Studies.* https://www.csis.org/analysis/cyber-war-and-ukraine

Li, J., Baldimtsi, F., Brandao, J. P., Kugler, M., Hulays, R., Showers, E., Ali, Z. & Chang, J. (2021). Measuring illicit activity in DeFi: The case of Ethereum. In M. Bernhard, A. Bracciali, L. Gudgeon, T. Haines, A. Klages-Mundt, S. Matsuo, D. Perez, M. Sala, & S. Werner (Eds.), *Financial Cryptography and Data Security (pp. 197-203)*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-63958-0_18

Li, S., Gou, G., Liu, C., Hou, C., Li, Z. & Xiong, G. (2022). TTAGN: Temporal transaction aggregation graph network for ethereum phishing scams detection WWW 2022 – *Proceedings of the ACM Web Conference 2022*. https://doi.org/10.1145/3485447.3512226

Litan, A. (2022, January 14th). Gartner predicts criminal cryptocurrency transactions will drop by 30% by 2024. Garnter Information Technology. https://www.gartner.com/en/articles/gartner-predicts-criminal-cryptocurrency-transactions-will-drop-by-30-by-2024

Liu, B. (2022, July 15th). Putin amends law to broaden Russia's crypto payments ban. *Blockworks*. https://blockworks.co/putin-amends-law-to-broaden-russias-crypto-payments-ban/

Liu, J., Zheng, J., Wu, J. & Zheng, Z. (2022). FA-GNN: Filter and augment graph neural networks for account classification in Ethereum. *IEEE Transactions on Network Science and Engineering*. *9*(4), 2579-2588. https://doi.org/10.1109/TNSE.2022.3166655

Lv, X., Zhong, Y. & Tan, Q. (2020). A study of bitcoin de-anonymization: Graph and multidimensional data analysis Proceedings – *2020 IEEE 5th International Conference on Data Science in Cyberspace, DSC 2020*. https://doi.org/10.1109/DSC50466.2020.00059

Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *The British Journal of Criminology*, *62*(6) 1537–1552, https://doi.org/10.1093/bjc/azab118

Mantri, A., Singh, N., Kumar, K., & Dahiya, S. (2022). Pre-Encryption and Identification (PEI): An Anti-crypto Ransomware Technique. *IETE Journal of Research*, 1-9.

McCord, A., Birch, P. & Bizo, L.A. (2022a). Digital displacement of youth offending: scoping and understanding the issue. *Journal of Criminological Research, Policy and Practice, 8*(4), 243-259. https://doi.org/10.1108/JCRPP-03-2022-0014

McCord, A., Birch, P. & Bizo, L.A. (2022b). Digital displacement of youth offending: addressing the issue, *Journal of Forensic Practice, 24*(3), 298-311. https://doi.org/10.1108/JFP-03-2022-0012

Meyerowitz, S. A. (2022). Justice department announces national cryptocurrency enforcement team. *Computer and Internet Lawyer, 39*(1), 16-17.

Microsoft Security (2022, June 28th). Destructive malware targeting Ukrainian organizations. Microsoft. https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

Morton, E. & Curran, M. (2022). Technical and legal aspects of tax debt collection and cryptocurrencies. *Australian Tax Forum, 37*(1), 1–26. https://doi.org/10.3316/informit.20220526067654

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Ndiaye, M. & Konate, P. K. (2021). Cryptocurrency crime: Behaviors of malicious smart contracts in blockchain. *2021 International Symposium on Networks, Computers and Communications, ISNCC 2021*. https://doi.org/10.1109/ISNCC52172.2021.9615702

Nolasco Braaten, C. & Vaughn, M. S. (2021). Convenience theory of cryptocurrency crime: A content analysis of U.S. federal court decisions. *Deviant Behavior, 42*(8), 958-978. https://doi.org/10.1080/01639625.2019.1706706

Patel, H. & Bharat, S. (2012). Money laundering among globalized world. In H. Cuadra-Montiel (Ed.), *Globalization (pp. 163-181)*. InTech. https://doi.org/10.5772/49946

Paul, K. A. (2018). Ancient artifacts vs. digital artifacts: New tools for unmasking the sale of illicit antiquities on the dark web. *Arts, 7*(2), Article 12. https://doi.org/10.3390/arts7020012

Phetsouvanh, S., Oggier, F., & Datta, A. (2018, November). Egret: Extortion graph exploration techniques in the bitcoin network. In *2018 IEEE International conference on data mining workshops (ICDMW)* (pp. 244-251). IEEE. https://doi.org/10.1109/ICDMW.2018.00043

Prytula, A., Lutsyk, V., Sviatoshniuk, A., Tkalia, O. & Kalachenkova, K. (2021). Cryptocurrency in transnational offenses: Criminal and civil legal aspects. *Amazonia Investiga, 10*(46), 209-216. https://doi.org/10.34069/ai/2021

Pushkarev, V. V., Artemova, V. V., Ermakov, S. V., Alimamedov, E. N., & Popenkov, A. V. (2020). Criminal prosecution of persons, who committed criminal, acts using the cryptocurrency in the Russian Federation. *Revista San Gregorio*, (42), 330-335. https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1566

Qureshi, M. (2022). How Pune police personnel reskilled themselves to tackle crypto crimes. *Indian Express*. https://indianexpress.com/article/technology/crypto/how-pune-police-personnel-reskilled-themselves-to-tackle-crypto-crimes-7948301/

Rahimi, A., Shahrestani, A., Ramezani, S., Zamani, P., Tehrani, S. O. & Moghaddam, M. H. Y. (2021). Filter Based Time-Series Anomaly Detection in AMI using AI Approaches. 2021 *5th International*

Conference on Internet of Things and Applications (IoT). https://doi.org/10.1109/iot52625.2021.9469717

Reddy, E. (2020). Analysing the investigation and prosecution of cryptocurrency crime as provided for by the South African cybercrimes bill. *Statute Law Review, 41*(2), 226-239. https://doi.org/10.1093/slr/hmz001

Robertson, C. (2018). When Bitcoins buy opioids: Why amending the federal money laundering statutes is necessary to combat the opioid crisis. Jurimetrics: *The Journal of Law, Science & Technology, 59*(1), 121-140.

Robinson, T. & DePow, C. (2022, January 7th) DeFi: Risk, regulation, and the rise of DeCrime. *Elliptic*. https://www.elliptic.co/resources/defi-risk-regulation-and-the-rise-of-decrime

Ruth, C. (2022, July 5th). Crypto hackers stole almost $2 billion in H1 2022. *Atlas VPN*. https://atlas-vpn.com/blog/crypto-hackers-stole-almost-2-billion-in-h1-2022

Sanz-Bas, D., Del Rosal, C., Náñez Alonso, S. L. & Echarte Fernández, M. Á. (2021). Cryptocurrencies and fraudulent transactions: Risks, practices, and legislation for their prevention in Europe and Spain. *Laws, 10*(3), 57. https://doi.org/10.3390/laws10030057

Sapkota, N. & Grobys, K. (2021, September). Asset market equilibria in cryptocurrency markets: Evidence from a study of privacy and non-privacy coins. *Journal of International Financial Markets, Institutions and Money*, 74, 101402. https://doi.org/https://doi.org/10.1016/j.intfin.2021.101402

Schaake, M. (2020). The lawless realm. *Foreign Affairs, 99*(6), 27-33.

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Review, 103*(2). https://doi.org/10.20955/r.103.153-74

Scheidegger, G. & Raghubir, P. (2022). Virtual currencies: Different schemes and research opportunities. *Marketing Letters, 33*(2), 351-360. https://doi.org/10.1007/s11002-022-09620-z

Schickler, J. (2022, May 22nd). How big is crypto crime, really? *CoinDesk*. https://www.coindesk.com/policy/2022/05/09/how-big-is-crypto-crime-really/

Şen, O. & Akarslan, H. (2018). Use of blockchain technology in the financing of DEASH. International *Journal of Information Security Science, 7*(4), 185-197.

Sexton, P. (2021). Honey pot – or not? Patricia Sexton explores the link between trans-national crime in the Pacific and crypto-currency. *New Zealand International Review, 46*(4), 10-13. doi/10.3316/informit.894922994720879

Sigler, K. (2018). Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom. *Computer Fraud & Security, 2018*(9), 12–14. https://doi.org/10.1016/s1361-3723(18)30086-1

Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J. & Salas, A. (2020). *Exploring the use of Zcash cryptocurrency for illicit or criminal purposes. RAND Europe*. https://www.rand.org/content/dam/rand/pubs/research_reports/RR4400/RR4418/RAND_RR4418.pdf

Singh, A., Gupta, A., Wadhwa, H., Asthana, S. & Arora, A. (2021). Temporal Debiasing using Adversarial Loss based GNN architecture for Crypto Fraud Detection. *2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA)*. https://doi.org/10.1109/icmla52953.2021.00067

Smith, J. (2021, August, 20). Victoria police seize record $8.5m in cryptocurrency linked to dark web drug deals. *The Market Herald*. https://themarketherald.com.au/victoria-police-seize-record-8-5m-in-cryptocurrency-linked-to-dark-web-drug-deals-2021-08-20/

Soana, G. (2022). Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry? *Economic Notes, 51*(1), Article e12195. https://doi.org/10.1111/ecno.12195

Sparkes, M. (2022). Follow the money. *New Scientist, 253*(3368), 18-19. https://doi.org/10.1016/s0262-4079(22)00008-2

Streissguth, T. (2022 October 27th). Bitcoin price prediction 2022. *NASDAQ*. https://www.nasdaq.com/articles/bitcoin-price-prediction-2022

Sun, Y., Xiong, H., Yiu, S. M. & Lam, K. Y. (2019). BitVis: An Interactive Visualization System for Bitcoin Accounts Analysis. *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*. https://doi.org/10.1109/cvcbt.2019.000-3

Tan, R., Tan, Q., Zhang, P. & Li, Z. (2021). Graph Neural Network for Ethereum Fraud Detection. *2021 IEEE International Conference on Big Knowledge (ICBK).* https://doi.org/10.1109/ickg52313.2021.00020

Taylor, S. K., Ariffin, A., Zainol Ariffin, K. A. & Sheikh Abdullah, S. N. H. (2021). Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets. *2021 3rd International Cyber Resilience Conference (CRC).* https://doi.org/10.1109/crc50527.2021.9392446

Taylor, S. K., M. Omar, M. S., Noorashid, N., Ariffin, A., Ariffin, K. A. Z. & Abdullah, S. N. H. S. (2021b). People, Process and Technology for Cryptocurrencies Forensics: A Malaysia Case Study. *Communications in Computer and Information Science,* 297–312. https://doi.org/10.1007/978-981-33-6835-4_20

Teichmann, F. M. J. & Falker, M. C. (2021b). Cryptocurrencies and financial crime: Solutions from Liechtenstein. *Journal of Money Laundering Control, 24*(4), 775-788. https://doi.org/10.1108/jmlc-05-2020-0060

Trozze, A., Davies, T. & Kleinberg, B. (2022). Explaining prosecution outcomes for cryptocurrency-based financial crimes. *Journal of Money Laundering Control.* https://doi.org/10.1108/jmlc-10-2021-0119

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

Tsuchiya, Y. & Hiramoto, N. (2021). How cryptocurrency is laundered: Case study of Coincheck hacking incident. *Forensic Science International: Reports,* 4, 100241. https://doi.org/10.1016/j.fsir.2021.100241

Tucci, L. (2019, July, 31). digital disruption. CIO. https://www.techtarget.com/searchcio/definition/digital-disruption

Turner, A. B., McCombie, S. & Uhlmann, A. J. (2019). A target-centric intelligence approach to WannaCry 2.0. *Journal of Money Laundering Control, 22*(4), 646-665. https://doi.org/10.1108/JMLC-01-2019-0005

UNODOC. (2020). United States of America v. Bryan Connor Herrell, No. 1:17-CR-00301-DAD-BAM (E.D. Cal. Sept. 2, 2020). https://sherloc.unodc.org/cld/case-law-doc/criminalgroupcrimetype/usa/2020/united_states_of_america_v._bryan_connor_herrell_no._117-cr-00301-dad-bam_e.d._cal._sept._2_2020.html

US Department of Justice. (2020). Colorado man pleads guilty to racketeering charges related to darknet marketplace alphabay. US Department of Justice. https://www.justice.gov/usao-edca/pr/colorado-man-pleads-guilty-racketeering-charges-related-darknet-marketplace-alphabay

US Department of Justice. (2021). Report of the attorney general's cybertaskforce: Cryptocurrency enforcement framework. https://www.justice.gov/archives/ag/page/file/1326061/download

US Department of Justice. (2022). Justice department investigation leads to shutdown of largest online darknet marketplace (U. D. o. Justice, Ed.). https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

US Department of Treasury. (2021). Ransomware trends in Bank Secrecy Act data between January 2021 and June 2021 (Treasury, Ed.) https://www.fincen.gov/sites/default/files/shared/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf

US Federal Trade Commission. (2022). Reports show scammers cashing in on crypto craze. Consumer Protection Data Spotlight. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

van Wegberg, R., Oerlemans, J. J. & van Deventer, O. (2018). Bitcoin money laundering: Mixed results? *Journal of Financial Crime, 25*(2), 419-435. https://doi.org/https://doi.org/10.1108/JFC-11-2016-0067

Vigna, P. (2022, April 14th). U.S. Agency links North Korea crime ring to $540 million axie infinity crypto hack; Lazarus group has allegedly stolen nearly $2 billion of crypto since 2017. *Wall Street Journal.*

https://www.wsj.com/articles/u-s-agency-links-north-korea-crime-ring-to-540-million-axie-infinity-crypto-hack-11649966631

Voskobitova, L., Vilkova, T., Nasonov, S., Khokhryakov, M. & Reshetnikov, Y. (2021). Illegal circulation of digital currencies: Features of criminal investigation. *Amazonia Investiga, 10*(45), 252-264. https://doi.org/10.34069/ai/2021.45.09.25

Wallace, V., & Scott-Hayward, S. (2020, June). Can SDN deanonymize Bitcoin users?. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE. https://ieeexplore.ieee.org/document/9148936/

Wang, F. & Zhou, X. (2022). Persuasive Schemes for Financial Exploitation in Online Romance Scam: An Anatomy on Sha Zhu Pan (杀猪盘) in China. *Victims & Offenders*, 1–28. https://doi.org/10.1080/15564886.2022.2051109

Wang, Z., Guo, J., Zhang, Y., Liu, M., Yan, L., Wang, Y., Liu, H. & Li, Y. (2021). BSMRL: Bribery Selfish Mining with Reinforcement Learning. *Data Mining and Big Data*, 1–10. https://doi.org/10.1007/978-981-16-7476-1_1

Wecksten, M., Frick, J., Sjostrom, A. & Jarpe, E. (2016). A novel method for recovery from Crypto Ransomware infections. *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*. https://doi.org/10.1109/compcomm.2016.7924925

Whiteman, M. (2020). Upskirting, bitcoin, and crime, oh my: Judicial resistance to applying old laws to new crimes – what is a legislature to do? *Indiana Law Journal, 95*(2019), 66-78.

Wronka, C. (2021). Financial crime in the decentralized finance ecosystem: new challenges for compliance. *Journal of Financial Crime*. https://doi.org/10.1108/jfc-09-2021-0218

Wronka, C. (2022). "Cyber-laundering": the change of money laundering in the digital age. *Journal of Money Laundering Control, 25*(2), 330-344. https://doi.org/10.1108/JMLC-04-2021-0035

Xia, Y., Liu, J., Zheng, J., Wu, J. & Su, X. (2021). Portraits of Typical Accounts in Ethereum Transaction Network. *Communications in Computer and Information Science*, 44–56. https://doi.org/10.1007/978-981-16-7993-3_4

Yanchao, Y. (2021). On the legal attributes of digital currency. *Social Sciences in China, 42*(2), 123-141. https://doi.org/10.1080/02529203.2021.1924463

Zhang, Y., Wang, J. & Zhao, F. (2020). Transaction Community Identification in Bitcoin. *2020 13th International Symposium on Computational Intelligence and Design (ISCID)*. https://doi.org/10.1109/iscid51228.2020.00038

Zheng, B., Zhu, L., Shen, M., Du, X., Yang, J., Gao, F., Li, Y., Zhang, C., Liu, S. & Yin, S. (2018). Malicious Bitcoin Transaction Tracing Using Incidence Relation Clustering. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 313–323. https://doi.org/10.1007/978-3-319-90775-8_25

Zimba, A., Chishimba, M., Ngongola-Reinke, C. & Mbale, T. F. (2021). Demystifying cryptocurrency mining attacks: A semi-supervised learning approach based on digital forensics and dynamic network characteristics. https://doi.org/10.48550/arXiv.2102.10634

Kontakt | Contact

Alex McCord | Faculty of Arts & Social Sciences | University of Technology Sydney | Sara.McCord@uts.edu.au

Philip Birch, PhD | Faculty of Arts & Social Sciences | University of Technology Sydney | Philip.Birch@uts.edu.au

Alan Davison, PhD | Faculty of Arts & Social Sciences |University of Technology Sydney | Alan.Davison@uts.edu.au