Journal of Policy Research, 8(3), 289-302
https://jprpk.com
https://doi.org/10.5281/zenodo.7288155

Crimes Related to Cryptocurrency and Regulations to Combat Crypto Crimes

Naheeda Ali[1]

Abstract

In recent years, cryptocurrencies' economic application and speculative value have soared. Cryptocurrency is being used as a means of trade, even in Pakistan. The government does not legalize it, but it is traded like many other states. Globally it causes fraudulent investment schemes. Cryptocurrencies are speculative, as the dot-com boom of the 1990s. Even though these organizations lacked a product, business plan, and profit potential, the stock market was eager to invest heavily in internet-related companies. A few years later, a dot-com catastrophe ended an era of unjustified and speculative online firms. The gold rush occurred much earlier. In the 1800s, people worldwide sought their fortune in the U.S., Canada, and Australia. They rapidly understood that mining a significant gold stake was dangerous and unlikely to succeed. In 2021, cryptocurrencies will become the dominant form of money. 2021 was the landmark year. Bitcoin became the new gold rush and caused online fraud, known as cryptocurrency fraud. We will examine cryptocurrency, crimes, laws, and regulations to combat crypto crimes.

Keywords: Cryptocurrency, Stock market, Law and regulations, Crypto crime, Economy.

1. Introduction

The blockchain technology that underpins cryptocurrencies can completely revamp the payment system by providing accountability, secrecy, and irreversibility. Transactions cannot be changed or updated. The decentralized blockchain technology may potentially overcome the weaknesses and problems with the current payment processes. This would lead to the development of a more effective and efficient system. According to a recent study, as of May 2021, there were 377 exchanges and 9756 different cryptocurrencies, both of which are subject to change daily. Implementing blockchain payment systems and cryptocurrencies properly presents a large set of obstacles. They also make it more challenging to investigate issues when they arise. For instance, the lack of understanding among investors, marketing strategies, and inadequate lack of regulation, if any at all, make cryptocurrencies very susceptible to the enormous fluctuations that may occur in the stock market (Reddy, E. (2020). On social media, a significant amount of cryptocurrency is being sold through various forms of excitement. Language, as well as deceptive advertising using celebrity status that has nothing to do with working business plans and detailed product descriptions, but all of them making extravagant claims about the possible earnings. Recent research found that good attention to detail, product disclosure, or any other aspect did not assist in determining whether or not the initial coin offering (ICO) was a scam. The disclosure of information and details on the document issuance turns out to be a double-edged sword (Dyson, S et al., 2019).

On the other hand, there is a lack of specific information on the issuance, business strategy, and open markets. Code repositories will likely be included in the due diligence process carried out on behalf of the investors. To put things another way, it did not appear that this information assisted in determining whether or not the scheme was legal. It was not legitimate (Kreminskyi O. et al., 2021). While using cryptocurrencies like bitcoin in digital transactions has been forbidden, some nations, like China, are developing their national cryptocurrencies like the CNY4 and the Bit-coin to compete in the market. In addition, the value of a particular cryptocurrency may increase or decrease in response to statements made by well-known figures in the media or political arenas (Kethineni, S., & Cao, Y. (2020). Bitcoin's price fell precipitously after Elon Musk tweeted that Tesla would stop using the cryptocurrency, for example. After the excitement generated by social media drove up the stock price to an unbelievable level, the value of Dogecoin shares skyrocketed, and then they promptly crashed.

The cryptocurrency was called after the popular meme. Crash sometime later. Even though Dogecoin can be used as a cryptocurrency just like Bitcoin, it was initially conceived as a joke. Because of cryptocurrencies' speculative nature, we are reminded of the dot-com bubble, moving even in the past, and the rush for gold. Cryptocurrencies' speculative character is similar to the dot-com bubble of the 1990s when any company related to the internet attracted significant investment in the stock market even though these companies did not have a product, a business plan, or the ability to generate profits. During this time, any company related to the internet attracted significant investment in the stock market (Maurushat, A., & Halpin, D. (2022). The bubble was, of course, followed a few years later by a crisis in the dot-com sector, which ended an age of unjustifiable and exceedingly speculative businesses operating on the internet. In the 1800s, individuals from over the world travelled to Australia, Canada, and the U.S. to pursue their fortunes. Despite their confidence, they quickly learnt that finding and extracting a large gold deposit was risky and unlikely.

[1] Assistant professor, Department of Law, University of the Punjab, Gujranwala Campus, Gujranwala, Pakistan, email: naheeda.ali@pugc.edu.pk

Fraudulent ICOs are more significant than the typical sample, according to 2021 research. Fraudulent ICOs raise four times as much as reputable ones. If there is a positive association between the two, it may be because fraud incentives rise as more money is gathered. Corporate outsiders and insiders like founders may be motivated to commit fraud for financial advantage (Christiansen, N. B., & Jarrett, J. E. 2019).

1.1. Cryptocurrency Taxonomies

Suppose a person does not completely understand the critical language associated with the technologies and processes. In that case, it is impossible to understand the advantages and disadvantages of regulating cryptocurrencies and the complexities associated with crypto investigations. The author's interactions with the government, business, and, most importantly, victims of bitcoin fraud have shown a lack of a common understanding of these essential elements. As a result, key terminology is supplied below; nevertheless, some readers may want to go directly to the following parts (Sai A. et al., 2021).

1.2. Cryptocurrency Characteristics

It is anticipated that more than 4,000 distinct cryptocurrencies will be in use as of the beginning of the year 2021. On some other pages, the number is listed as 9756.22. However, only a few offer significant returns on investment, and the majority have a very restricted or nonexistent trading volume. Bitcoin, the cryptocurrency considered the "flagship" of the whole industry, along with Ripple, Ether, Monero, Litecoin, and Tether, are some of the cryptocurrencies performing exceptionally well. These cryptocurrencies were not initially designed to be investments; instead, they were built to enable various capabilities. Investment and value were added much later. This is essential since hundreds of cryptocurrencies have been created to cheat investors out of their money, run frauds, or engage in speculative speculation. This part of the guide will investigate the most widespread legal types of cryptocurrency. In the following table, you will find an outline of critical characteristics shared by the most popular cryptocurrencies (Caliskan, K. 2020).

1.3. Legitimate, Common Cryptocurrencies

The following is an analysis of the most widespread legal forms of cryptocurrency. When we say that these cryptocurrencies are authentic, they are not fraudulent. They were not created in the first place to engage in highly speculative investing. They are well-known brands, and their sales represent a sizeable portion of the market. The first cryptocurrency ever created, Bitcoin (BTC), runs on an open-source platform and a peer-to-peer network. Even though it is today the most popular and expensive cryptocurrency, vulnerabilities have been uncovered in the blockchain since it was first made accessible to investors in 2008. The year 2008 was the first time it was made available to investors. This featured a slow rate of transactions, a restricted number of users who could utilize the system in a row at once, a limited capacity, and the high processing needs that mining entailed. Because of this, there is significant energy expenditure, ultimately leading to higher costs associated with each transaction. Various items tied to bitcoin have emerged due to the cryptocurrency's growing popularity worldwide. According to a website that provides global business data, around 14,000 Bitcoin ATMs are located worldwide. The potential use of blockchain technology to create cutting-edge applications in several disciplines and industries, including healthcare, supply chains, fleet management, and agriculture, has been extensively promoted by academic institutions and commercial firms over the last few years. Since 2016, several nations, notably Japan, have acknowledged that the value of Bitcoin and other cryptocurrencies is similar to that of traditional currencies. This contributed to the cryptocurrency's existing legitimacy and expanded it in some countries, but it did so while simultaneously boosting the confidence of both consumers and investors (Caliskan, K. 2020).

Ether (ETH) 's decentralized cryptocurrency ecosystem is built on the blockchain technology initially developed for Bitcoin. On the other hand, the Ethereum Blockchain features what are known as smart contracts, which are pre-built automatic agreements. The term "smart contract" refers to an agreement that can carry out its terms automatically and is stored on a public blockchain. Intelligent contracts are algorithms with specified criteria that dictate whether an activity is approved or not and may auto-negotiate the functionality of the transactions. These conditions govern what determines whether an action is authorized or not. These conditions can dictate whether an activity is allowed or not. The user constructs the intelligent contracts according to their needs, and the contracts automatically carry out their terms when specific criteria are satisfied. Ether is widely recognized as the first cryptocurrency to include smart contracts. It has become one of the most popular coins among investors and regular users. It is noteworthy to note that Nick Szabo is credited with creating intelligent contracts around the year 2005. This was three years before Bitcoin was launched into circulation. The following information about intelligent contracts can be found in the white paper for Ethereum:

Building the ultimate abstract foundational layer for cryptocurrency crimes. Built-in Turing-complete programming language. This allows anybody to design smart contracts and decentralized apps with arbitrary ownership, transaction, and state transition rules. This investigation will take place by building the blockchain. The blockchain that underpins Ether is an altered version of the one used by Bitcoin, and the peer-to-peer network it employs is open source. It is interesting to note that the price of Ether is said to have increased by more than 13,000 per cent between 2014 and 2017.

Ripple (XRP) launched its business in 2012 and, at the time, was operating under the name OpenCoin. Since then, Ripple has been the topic of many discussions and criticism; despite Ripple's critics, control over cash volume and release is the primary source, investors initially saw it as a solid investment owing to the structure of the firm and the presence of many heavyweight investors. This was the case, although the criticism was levied against it. Even though the Initial Coin Offering (ICO) for Ripple took place in 2013, the cryptocurrency did not start making substantial inroads in the open market until 2017. Ripple's primary objective was to develop a blockchain network that, similar to conventional banking, would make it possible to implement more effective methods of making cross-border payments ((Dargahi, T et al., 2019).

Since then, Ripple has worked with many organizations in the business sector, improving international payment networks and simplifying academic blockchain research. Ripple controls or selects the nodes connecting to it, limiting the number of people that may monitor its network. Due to the creation of authority inside the blockchain, many believe that node selection leads to the blockchain's centralization (Nijsse, J., & Litchfield, A. (2020).

Ripple, on the other hand, maintains that its network is decentralized and that this is because it has deliberately selected trustworthy nodes to link to its blockchain. Most other cryptocurrencies enable anybody to mine, so youngsters may work together to make more money. This is a concern since it makes it easier for adults to steal cryptocurrency from minors. Because of this conspiracy, control would be obtained over the network, and the parties engaged would, in effect, serve as a centralized regulatory body. The XRP Ledger has always been intrinsically decentralized since users may adjust their "Unique Node Lists" and the validators they trust. Always so. This must be explored to determine whether it convinces potential customers that Ripple is not centralized. Ripple appears more efficient and cost-effective since it is centralized. Proof-of-work algorithms are crucial to decentralized blockchains. Monero is a decentralized, anonymous Bitcoin-like cryptocurrency. It distributes its cash using the same Proof of Work (PoW) mining mechanism as Bitcoin. Satoshi Nakamoto invented Monero. Shen Noether's arguments, on the other hand, imply that the first version of the Monero protocol was modelled after Crypto Note, which conceals both the destination and the origin of financial transactions via ring signatures and one-time keys.

Monero is distinguished from other cryptocurrencies in that it conceals the amounts of transactions by employing ring signatures, enhancing the level of privacy associated with those transactions. According to the official website, Monero will randomly reorder its users' public keys to prevent anyone from being able to single out a specific user. In addition, the Monero blockchain uses a one-of-a-kind mechanism that generates a one-time wallet address that the recipient of the payment can only link. Because of this, tracking transactions using blockchain analysis is challenging, even with cutting-edge tracing technologies like CipherTrace and Chainalysis. Since of this feature, criminals prefer Monero over other cryptocurrencies because it eliminates the possibility of scrutiny from law enforcement, which is present in most other cryptocurrencies (Dika, A. 2017).

The digital currency known as Litecoin was given its name because its creators envisioned it functioning as a "lighter" or "less robust" alternative to Bitcoin; Charles Lee, the founder of Litecoin and a former software engineer at Google, views Litecoin to be the silver coin that complements Bitcoin's gold coin. The initial launch of the cryptocurrency took place in October of 2011. The Litecoin Blockchain utilizes code similar to that of the Bitcoin Blockchain; nevertheless, there are some fundamental changes. The Litecoin block was developed to facilitate faster transactions, resulting in Litecoin's transactions. Stablecoins, such as Tether (USDT), are partially decentralized tokens that operate on the Bitcoin Blockchain. Tether is also known as the United States Dollar. It was established in 2014 and had a tight relationship with Bitfinex, a cryptocurrency exchange based in Hong Kong.

Even though there are several competing stablecoins, the market share held by Tether is the largest. Tether is 'tethered' to an equal quantity of fiat money (USD) on a 1:1 ratio, as the name indicates. Tether is centralized, unlike other decentralized cryptocurrencies. This is why Tether is not generally regarded as a cryptocurrency in its own right. Tether Limited is keeping a reserve quantity of fiat cash similar to Hong Kong's. Because the Tether will only be vulnerable to the volatility of the US Dollar, the goal of tethering is to ensure that customers and investors continue to have faith in the cryptocurrency (USD). All decentralized cryptocurrencies are susceptible to the volatility of their decentralized markets, and there are no underpinning protections for these coins. Many people's primary concern is the volatile market conditions and the easy manipulability of cryptocurrency exchanges. Unregulated currencies will continue to have high-risk elements (Pernice, I. G. et al., 2019). D Tether Limited is required to perform the role of a centralized asset custodian for reserve assets. As a result, our chosen system is not entirely decentralized. (There is, however, a decentralized kind of digital money known as tethers that are now in circulation) because it is pegged to the US dollar, Tether can benefit from inflation to maintain a value equivalent to that of the USD, which is an additional advantage (Nijsse, J., & Litchfield, A. 2020).

1.4. Fraudulent or Less Trustworthy Cryptocurrencies

Coins with a lower authentication level are more likely to be counterfeit and have several traits in common. These features include celebrities who utilize social media to promote the currency, fraudulent websites, bogus exchange locations, fake mobile applications, and celebrities who create fake websites. Ponzi schemes and pump-and-dump operations are regularly used in fraudulent transactions using bitcoins. Moreover, investments in cryptocurrencies are often highly high in terms of their speculative potential. In the part that follows, Section 3, we will go into depth on the pump, dump, and Ponzi schemes. The next section of this chapter will discuss fraudulent cryptocurrencies as well as the usage of cryptocurrencies in fraudulent activities. This discussion will include case studies, investigative challenges, regulatory techniques, and cryptocurrency crimes (Wątorek, M. et al., 2021).

1.5. Cryptocurrency-Related Crime

Since its inception, bitcoin has been used illegally. Some experts believe cryptocurrencies were developed to aid unlawful activity. Bitcoin's creator made great efforts to protect consumers from fraud and hackers. No evidence suggests Nakamoto wanted Bitcoin to enable criminal conduct rather than safeguard users (Sharma, D. K. et al., 2020). Every day bitcoin crimes include ransomware, affiliate marketing, fraudulent traders and exchanges, and bogus trading platforms. 50 Crypto crimes, however, frequently include both crypto-enabled and crypto-dependent elements. Bitcoin fraud often involves money laundering. HM Treasury and Home Office gave the following information. Cryptocurrencies help launder cybercriminal gains and simplify the movement of cash (Liu, Y. et al., 2022). Action Fraud, the UK's fraud reporting bureau, received 5,581 cryptocurrency-related complaints in 2020. This 57 per cent gain cost UK investors £113 million. 52 Fraud made up 54% of cryptocurrency-related crimes in 2019, according to Chainalysis. This reduced worldwide revenue by $2.6 billion. Ainsworth and Hu (2020, p. Using forensic analysis to prevent cryptocurrency crime is overhyped. Most cryptocurrency thieves are arrogant and defy police to arrest them, stating, "Catch me if you can." Based on available evidence, cryptocurrency-enabled crime is expected to rise over time. However, this forecast depends on law enforcement's ability to reduce criminals' usage of cryptocurrencies. Ainsworth notes, however, that this may not change the perpetrators' mindset (Kyriazis, N. A. 2021).

This section examines prevalent crypto crimes, provides case studies, and discusses investigating and dealing with this crime category. All information has been changed so the industry, perpetrators, jurisdiction, and others cannot be identified. Sections 4 and 5 examine criminal factors, investigator challenges, and regulatory methods.

1.6. Initial Coin Offerings (ICOs)

Someone developed a website and extensively marketed investment possibilities in the new SoMEMoney cryptocurrency on social media sites such as Twitter and Facebook. In exchange for their monetary contributions, investors could acquire coin tokens in the cryptocurrency. Even though there were valid initial coin offers, many were fraudulent. The initial coin offering (ICO) that was part of the SoMEMoney hoax promoted the cryptocurrency as being on par with Bitcoin. In this situation, the company lacked industry or computer science skills, but it did not have genuine technology or business plans to support its operations. Their sole significant background was in business administration and marketing. Facebook and Linkedin, two popular social media platforms, had links to advertisements for the chance (Chohan, U. W. 2019).

2. Literature Review

2.1. Affiliate-Marketing Ponzi Scheme

One warned him it sounded like frauds on the ACCC website. One cautioned him that it sounded like online scams (ACCC). The Australian Competition and Consumer Commission (ACCC) protects consumers against fraudulent and dishonest enterprises employing fresh investment capital. This type of fraud is known as paying old investors with new money (Castonguay, J. J., & Stein Smith, S. (2020). A pyramid scheme is another name for this type of investment scam.

Nevertheless, the investment opportunity is a hoax, and very little in the way of actual rewards is produced. The scam organizers take a portion of the monies contributed by subsequent investors and utilize that money to pay hefty "dividends" to previous participants. Investors are led to believe that they are obtaining a return on their investments through payments such as these, as a result of which they are encouraged to invest additional money in the plan. Con artists regularly convince investors to engage the assistance of their loved ones and friends in the investing process. This is similar to the scenario with so-called pyramid schemes (Nadlifatin R. et al., 2022).

Banner Ad Ponzi Scheme

This case study focused on a significant international fraud ring that, since 2016, has been operating several fraudulent websites associated with internet advertising. The websites sought new clients either directly or indirectly via affiliate ads, who subsequently sold the client data to fraudulent actors. This might have been done either directly or indirectly. Affiliate marketing is a kind of marketing in which one business offers another business financial compensation in return for the latter advertising the former business's wares in exchange for a commission. SQL injections are a standard tool used by criminals to replace legitimate sponsored advertisements with fake ones (and appear higher in Google rankings (Rognone et al., 2020).

In many cases, illegal information is disseminated to millions of users via technically illegal botnets. Affiliate marketing is a well-known and successful distribution method for cybercriminals since cybercriminals commonly utilize various injections to move themselves up higher in the Google results. SQL injection is a typical cyber attack that manipulates backend databases by inserting malicious code. This type of attack is known as a "spear-phishing" assault. In this scenario, the injection successfully replaced the sponsored advertisement on the website, and the legitimate advertisement ranked higher in the Google search rankings (Maurushat, A., & Halpin, D. (2022).

The con artists employed high-pressure sales strategies to offer customers access to their proprietary platform, which, according to the fraudsters, enabled them to produce their web adverts. It was explained to the customers that they anticipated generating a profit proportional to the total number of clicks they obtained, another name for the pay-per-click model. The con artists tampered with the profit numbers, prompting the customers to invest more money and look for a better return on their investment. The author's private investigative business became aware of this scam, and in response, it recruited other informants from inside the organization to aid in carrying out the con. Along with the profit data, the customers' advertising was shown to be phoney in the informants' information. Most of the money customers paid were deposited into the fraudster's bank account, and only a small portion was kept to make "profit" payments to earlier customers. As with previous Ponzi schemes, the distribution of this profit payment made the investors see they were obtaining a return on their money, which encouraged them to put even more money into the plan. This is similar to other Ponzi schemes (Maurushat, A., & Halpin, D. 2022).

Even though this fraudulent plan was modelled like a traditional Ponzi scheme, the con artists created bitcoin exchange wallets so their victims could send payments using cryptocurrency. After that, the bitcoin was cleansed through a series of complex transactions, many of which involved the utilization of mixers to conceal the source and ultimate destination of the cash. The investigation is still underway and has been turned over to a law enforcement body in a different country so that the client's funds can be recovered and prosecuted. In this illustration, the typical type of offence was fraudulent banner advertising, and the offender's payment was made possible by using cryptocurrencies. The same laws might apply to this situation as they did to the SoMEMoney scandal. Among them are potential outcomes involving significant organized crime, fraud in general, and the laundering of money or the profits of illegal activities. Because SQL injection includes malicious code, it would fall within the purview of cybersecurity hacking rules. These provisions include unauthorized access to data or systems and modifying or interfering with data or systems. Other regulators may also prosecute the individuals responsible for fraudulent investment schemes outside of law enforcement, such as consumer agencies, consumer protection commissions, and tax authorities (Sunarti S. et al., 2020).

2.2. Boiler Room Pump-and-Dump Cryptocurrency Traders

The strategies implemented by fraudulent traders have been around for a significant amount of time. Hollywood presented these tactics in the film "Boiler Room," released in 2000, and "Wolf of Wall Street," released in 2013. The term "boiler room scheme" is widely used to refer to this fraudulent operation. Typically, boiler room syndicates will make unsolicited phone calls to potential investors and employ aggressive sales tactics to promote various items, such as renewable energy, foreign money, gold, and banner advertisements. In most cases, the offenders do not hold valid business licenses. They rarely own the items they sell, which means that the customers are investing in something that is either phoney or worthless (Austin, J. 2021). Fake bitcoin traders use conceptually similar strategies to those of actual traders.

On the other hand, the digital money that they claim to trade and invest on behalf of their victims does not exist. After a client's transactions have been carried out, it is common to set up sophisticated online portals that the customer can log into to examine the outcomes of the trades. However, the cryptocurrency does not exist, and the trading options, account balance, and profit and loss figures displayed on the webpage are fictitious representations (Mackenzie, S. 2022).

2.3. Fake Forex Trade

This case study focuses on a fictitious website belonging to a foreign exchange (FX) broker. The website's proprietors asserted that they were based in the United Kingdom (UK) and provided a license number issued by the Financial Conduct Authority (FCA). In addition, a phone number for the United Kingdom was provided on the website. Because of the low-interest rates offered by his bank, Jack White intended to invest in foreign exchange equities. After contacting the broker website, Jack was assigned a broker who provided investment guidance concerning cryptocurrencies offering guaranteed high rates of return. After that, Jack invested 50,000 USD, which was later converted to Bitcoin and transmitted to the wallet address supplied by the broker. Jack is now the proud owner of 50,000 Bitcoin. Jack found this unusual, but since he was starting in the investment world, he did not question the validity of using cryptocurrencies to pay for shares because he thought it was perfectly acceptable (Dupuis, D. et al., 2021).

During the next week, Jack carefully checked his account and noted that the returns on his investment were rather large. This led him to conclude that his investment was a wise one. Jack attempted to take his money out of his account, but the withdrawal attempt was unsuccessful. Jack's earnings remained in his account. When Jack called his broker to report the issue, the broker advised him that before he could take the money, he would need to pay the income tax due on the amount of money he was withdrawing. Jack acted by the instructions and paid the tax, but he could not contact his broker over the phone once he had paid the tax. His account was closed, and he did not get a response to any of the emails he sent (Maurushat, A., & Halpin, D. 2022).

After getting to this understanding, Jack did not waste any time reporting that he had been the target of a con job to the appropriate authorities. The police advised the victim that the individuals responsible for the crime were located outside of their jurisdiction. As a result, they were unable to investigate them. After that, Jack made contact with private detectives so that they could monitor the cryptocurrency transactions and do forensic research on the website and the persons involved in the fraud. At this point, the investigation is still being carried out. This case study focuses on a fictitious website belonging to a foreign exchange (FX) broker. The website's proprietors asserted that they were based in the United Kingdom (UK) and provided a license number issued by the Financial Conduct Authority (FCA). In addition, a phone number for the United Kingdom was provided on the website (Mackenzie, S. 2022).

Because of the low-interest rates offered by his bank, Jack White intended to invest in foreign exchange equities. After contacting the broker website, Jack was assigned a broker who provided investment guidance concerning cryptocurrencies offering guaranteed high rates of return. After that, Jack invested 50,000 USD, which was later converted to Bitcoin and transmitted to the wallet address supplied by the broker. Jack is now the proud owner of 50,000 Bitcoin. Jack found this unusual, but since he was starting in the investment world, he did not question the validity of using cryptocurrencies to pay for shares because he thought it was perfectly acceptable (Austin, J. 2021).

During the next week, Jack carefully checked his account and noted that the returns on his investment were rather large. This led him to conclude that his investment was a wise one. Jack attempted to take his money out of his account, but the withdrawal attempt was unsuccessful. Jack's earnings remained in his account. When Jack called his broker to report the issue, the broker advised him that before he could take the money, he would need to pay the income tax due on the amount of money he was withdrawing. Jack acted by the instructions and paid the tax, but he could not contact his broker over the phone once he had paid the tax. His account was closed, and he did not get a response to any of the emails he sent (Maurushat, A., & Halpin, D. 2022).

After getting to this understanding, Jack did not waste any time reporting that he had been the target of a con job to the appropriate authorities. The police advised the victim that the individuals responsible for the crime were located outside of their jurisdiction. As a result, they were unable to investigate them. After that, Jack made contact with private detectives so that they could monitor the cryptocurrency transactions and do forensic research on the website and the persons involved in the fraud. At this point, the investigation is still being carried out.

2.4. Ransomware/ Crypto Locker

Ransomware encrypts local data and distributes it to coerce victims into paying a ransom. Ransomware affects PCs and networks. This is sometimes called "cyber extortion." Today's ransomware source code may encrypt data with excellent accuracy. Using public-key encryption techniques such as RSA 2048-bit or RSA 4096-bit makes it difficult, if not impossible, to break the encryption with current computing power. RSA 2048-bit or 4096-bit keys are used (Bansal, U. 2021).

The ransomware may typically show instructions on retrieving the private key for file decryption on the principal victim's computer and in mapped file-share folders. Users are typically told to pay a ransom anonymously. Bitcoin is anonymous and difficult to track. After the ransom has been paid, the victim could be provided with the victim's private key and instructions on how the victim's data might be decrypted. 63 It is conceivable that even after paying a ransom, one would not be able to get a decryption key that works. Since the beginning of ransomware dissemination, there has been a discernible rise in the level of complexity found in assaults. Multiple organized crime syndicates operating on a global scale have simultaneously carried out many coordinated attacks worldwide (Reshmi, T. R. 2021).

Ransomware attacks have become more sophisticated due to the introduction of blockchain technology and its subsequent rise in popularity. The blockchain is used in these ransomware attacks to enable the attack itself and the payment. This specific ransomware assault is still in its infant stages; nonetheless, it is a novel and complicated attack method that, at the time, only had a limited number of technological countermeasures available to defend against it. 64 Crypto Locker and Dox ware are the two types of ransomware that are seen the most often. The malicious software known as Crypto Locker encrypts data stored on computers and other devices that run the Windows operating system. Windows is the operating system that is targeted by ransomware attacks the most often. Microsoft does not support many older Windows versions. This means that the company does not produce patches or distribute security updates for these versions, leaving these systems vulnerable to attack. Microsoft has discontinued the production and distribution of security updates for these older versions of Windows. The culprits behind a Crypto Locker attack would typically demand a ransom in the form of bitcoin, which must be paid by a specific deadline to receive the decryption key. Since 2013, this specific kind of ransomware has been spreading like wildfire, and it still causes problems. The company may decide not to pay the ransom if the data in question is not particularly sensitive and if it has backups of the material in question. Dox ware deviates marginally from other kinds in that the typical danger posed is the disclosure of private information to the general public. The crooks involved prey on individuals as well as businesses and other organizations. Photographs of family members, internet search histories, medical records, and intellectual property are examples of sensitive data. In this scenario, the victim must pay a certain amount of bitcoin within a certain length to prevent the sensitive information from being disclosed (Gómez-Hernández J. et al., 2022).

For example, a wealthy CEO was held hostage and demanded $1 million to release photos of his children and grandkids. The CEO felt compelled to pay the ransom, despite the cyber incident response organization's advice. The customer said they would not have paid the ransom if the information had come from the firm since they had backups, cyber insurance, and an elaborate cyber incident response policy. Their response plan did not include any personally sensitive information, and their cyber insurance did not cover this area of their business. As the cybersecurity sector advanced with new decryption tools and increased readiness, criminals focused on doing ware or personal cyber extortion (Thakur, S. et al., 2022).

Paying a ransom is illegal in many countries and poses other legal issues. Accepting terrorist-linked cryptocurrencies is illegal. If a firm is taken hostage by ransomware and the payment is to a bitcoin wallet used to support terrorism, the company cannot pay. This includes ransom insurance reimbursement. There is no official list of bitcoin wallet addresses linked to terrorist funding. Wallets and cryptocurrencies tagged "removed from trading due to internal and external standards" may help identify bitcoin abuse. Australian cryptocurrency exchange CoinSpot has a list of wallets that might cause problems in the future (Bansal, U. 2021).

It is not difficult for criminals to establish a new wallet once an existing wallet has been flagged as hazardous and banned. Because of this, it is difficult to put a halt to illegal conduct. Typically, tracking software for cryptocurrencies like Ciphertrace will use verified intelligence as an essential component of their service. Wallets known to have ties to terrorist groups prohibited from entering the nation are included in this category. A more in-depth discussion of tracing may be found in Section 4, which can be accessed via this link (Reshmi, T. R. 2021).

3. Crypto Crime Investigations

As with any specialized crime or investigation, there are exceptional standards for investigating bitcoin crimes. Cryptocurrency is in its early phases as a direct or indirect component of criminal activity. Because of the decentralized and uncontrolled nature of cryptocurrencies, there is little doubt that crimes that are facilitated or dependent on cryptocurrency will increase in frequency and severity in the years to come. The anonymity afforded by cryptocurrencies acts as a stimulant, leading to an increase in the number of illegal operations carried out. There are currently 67 comments (Ogunyolu, O. A., & Adebayo, A. O. 2022).

3.1. Methodology of Investigation

The fundamental objective of any inquiry is to discover who or what is responsible for the criminal activity and, if feasible, retrieve the stolen property. However, this is sometimes a wishful thinking aspect only. However, this seemingly straightforward investigative concept takes on an entirely new significance when investigating bitcoin. Cryptocurrencies' exponential expansion and complex nature are the critical challenges law enforcement agencies must overcome. Interviewing potential eyewitnesses, canvassing the area, and searching for fingerprints are no longer options for the police officers investigating the murder. In addition, the conventional ways, either following the money trail or the communication route, are made even more difficult by cryptography in criminal activity. Because this is a new kind of crime that occurs online rather than in the real world, the only way to solve it is through technological means and specialized training. Both bitcoin transactions and wallets (also known as accounts) are designed to be completely anonymous. Investigating crimes committed using cryptocurrencies or crimes made possible by cryptocurrencies immediately creates additional challenges for investigators (Maurushat, A., & Halpin, D. 2022).

3.1.1. Tracking Cryptocurrencies for Money Laundering and Illicit Profit

The most challenging obstacle in cybercrime is undoubtedly identifying the individual or organization behind an attack. Several issues might emerge concerning attribution, including the following: Who exactly are the individuals to blame for what happened? What equipment is involved in the event, and where exactly are they situated? Who may be claiming responsibility for the assault, and is it possible to verify this allegation? Tracking capabilities may determine IP addresses, the location of the device, or the location of the exchange; nevertheless, they cannot identify the exact person using the technology. The only thing that can be attributed to a gadget, exchange, account, or cryptocurrency wallet is the possibility that it was utilized (Maurushat, A., & Halpin, D. (2022). Rival criminal organizations or state-sponsored groups sometimes falsely accuse each other of creating ransomware. Cybercrime and cybersecurity are politically sensitive sectors full of purposefully propagated misinformation. It may be challenging to establish who was responsible for an attack, whether a group, a person, or connected devices, accounts, or code. This verification can rarely be performed by tracking the money or the communication trail. Instead, extra information (such as informants) is often necessary for the vicinity of the events. Several challenges exist when working with virtual currencies before successfully identifying persons engaged in fraudulent behaviour (Wright, C. S. 2021).

Additionally, it can be challenging to determine whether or not a transaction is being utilized for illegal activity instead of a lawful reason. One can recognize a wallet that is connected to a transaction. Using public ledgers, however, it is impossible to determine whether the transaction was conducted for a legal cause or an illegal purpose such as money laundering. There are further issues, some of which will be discussed here, followed by more in Section (Villányi, B. 2021).

Two of the most prominent firms globally have created software that utilizes the public ledger records of the blockchain to track transactions. This was done as a direct response to the simplicity with which criminal proceeds may be cleaned up using cryptocurrencies. CipherTrace and Chainalysis are top-tier, privately-held businesses that are leaders in their field and specialize in monitoring bitcoin transactions. It is becoming an increasingly frequent practice for law enforcement agencies and private investigative organizations to employ their software and other technological tools to trace bitcoin transactions and eventually discover the persons responsible for the unlawful conduct (Desmond, D. et al., 2021).

Tracing bitcoin transactions has two purposes: one is to identify the persons responsible for illegal conduct, and the other is to identify the profits of illegal activity. Ciphertrace and Chainalysis68 have created visual graphs to clarify blockchain data. Visual graphs help investigators evaluate transactional data and find money launderers (AFRIKAN, N.. 2021).

Only a few currencies provide visual graphs, which is a bit of a bummer. In order to improve productivity while simultaneously cutting down on the number of false positives, more development of visualization products is required. Using the program does not in any way ensure that there will be no errors. Monitoring Bitcoin transactions is notoriously tricky, requiring significant time invested in practice and studies to get the necessary expertise.

3.1.2. The Value of Cryptocurrency Exchanges

In April 2021, the website cryptimi.com, which provides information and recommendations about cryptocurrencies, estimated a total of 504 exchanges across the globe. It is anticipated that there are 504 different exchanges, but CoinMarketCap.com is monitoring only 259. The remaining exchanges are thought to be in the process of getting started. It is believed that the absolute number of active exchanges varies consistently. Further, according to Cipher Trace, 58 per cent of Bitcoin transmitted from an American exchange to another exchange was done so across international borders. All transactions were sent to overseas exchanges with inadequate KYC standards. 58% of all transactions. This makes fighting crypto crime difficult. Many governments have been pressed to control cryptocurrency exchange points (Section 5) and other technology used to launder money and buy unlawful things (Bellavitis, C. et al., 2021).

3.1.3. Crypto-Fraud Policing: Private Vs Public

However, organizations that investigate internet fraud. Globally do not conduct many productive investigations. International organizations such as Interpol supply information on internet fraud schemes, keep an eye on instances and provide intelligence and assistance to national law enforcement agencies. No resources are available to investigate international fraud in many nations since those resources are being spent and utilized elsewhere. This is because those resources are being used elsewhere. Naturally, there are substantial differences in resources from one nation to the next, but in general, the problem of prioritizing resources is a problem in all jurisdictions (Corbet S. et al., 2019).

Legislators and scholars generally believe that the legal system will be able to tackle the issue of combatting cybercrime provided the necessary legislation is implemented and adequate resources are dedicated to the work at hand. If these prerequisites are satisfied, then the idea that this outcome is possible is founded on the presumption that the law will be able to overcome a broad range of obstacles. On the other hand, this is not the case regarding illegal activities associated with cryptocurrencies. Regardless of whether or not a computer was used to assist with the fraudulent activity, Existing criminal regulations for fraud, money laundering, and other crimes make prosecuting fraudsters conceivable in most countries. These regulations would enable fraudulent prosecution. Due to the difficulty of cryptography, convictions are uncommon. Law enforcement and intelligence organizations have concentrated on disrupting crime (Issac, A. C., & Baral, R. 2020).

Investigating cybercrime is challenging. The problems include harmonization of laws, jurisdictional concerns, resource implications, lack of training, uncertainty in how a criminal provision will be construed alongside human-rights provisions, and technological impediments that make it difficult to track back to the perpetrator. These obstacles make it hard to find the criminal. Online fraud does not affect people's health or safety. Therefore law enforcement organizations do not prioritize it. Despite advances in machine learning, data techniques, and AI, attribution is still a challenging problem (as the tracking section showed) (Hornuf, L. et al., 2021).

Law enforcement agencies and many private investigative businesses have an additional challenge in the form of an additional impediment in the form of a desire and competence to adapt to this new kind of crime or crime facilitator. They are going to have to overcome this obstacle. As Dyson73 comments, Understanding the technological process that takes place throughout the transaction processes of each cryptocurrency algorithm is a fresh challenge for investigators (Corbet, S. et al., 2019).

Many law enforcement agencies worldwide are trying to adapt to the problems posed by cryptocurrencies. Many are slow to respond, hurting victims. The business sector is adapting to this new crime by creating tools to help victims and personal capacities to aid law enforcement. These technologies and talents are being created to combat emerging crimes. Private investigation services can investigate, but it is challenging to acquire exchanging documents. Because of privacy regulations, most exchanges will not let private investigators access their information. They will support law enforcement if they obtain a formal letter of request from the relevant agency; in the author's experience, a subpoena is only needed in highly uncommon instances. Private detectives tasked with tracing crypto criminals have a difficult task. Private investigators often find that law enforcement agencies move slowly or cannot assist them in getting documents (Tredinnick, L. 2019).

Our research has shown that when paired with the information and intelligence held by law enforcement and regulatory agencies, the intelligence and technology held by private companies can produce successful solutions. However, there has been a worldwide shortage of law enforcement authorities willing to collaborate with private organizations. Thankfully, this is starting to shift. We notice that the United States Federal Bureau of Investigative and Europol are starting to engage more freely with private investigation businesses when they can do so within their own organizational and regulatory frameworks. Even though the writers cannot discuss new capabilities and agreements, we feel compelled to make this point. The question "why?" must be asked while considering the potential that law enforcement is not interested in this matter. The solution requires far more investigation and thought, but there is little question that the problem lies in a lack of knowledge and flexibility on the part of management (Cheung, J. 2019).

Police require more training to do initial case evaluations, understand investigative needs, and refer cases to specialists. Many crypto-crime victims believe they were duped. Misled citizens include individuals who avoid police stations or whose early complaints take too long to reach the appropriate expert due to distance. Investigators. Regulatory constraints that prevent law enforcement from sharing case information, a lack of resources, or other factors may also be to blame. The issue may be this. Our findings indicate a lack of curiosity, a culture that avoids sharing data with private enterprises, and a belief that fraud is not as pervasive as it formerly was. This is a complicated problem since it is not as harmful as other cyber crimes (Li Z. et al., 2022).

Additionally, since certain law enforcement agencies separate cybercrime investigation from fraud, such agencies have more expertise in the former. The cybercrime unit may have custody of this material, but the fraud unit does not have access. Before it can become a priority for law enforcement agencies, education of investigators in cryptography and cybercrime has to take place first; this will need substantial managerial support and commitment. (Twomey, D., & Mann, A. (2020). They are not very interested in furthering their education by participating in technical training at the executive level. Regrettably, chief executive officers (CEOs) must have undergone at least some technical training to satisfy the requirements of cryptocurrency investigations and understand the seriousness of the crime surrounding cryptocurrencies. It is pretty unlikely that sufficient finances will be available at this time. The issue will not be fully understood by those in charge of law enforcement, even though resources have been allocated to finding a solution. We are committed to entering the digital era as a law enforcement agency and are now working on this issue. One inherently more human perspective is that the amount of funding and resources available to train law enforcement officers in certain jurisdictions is insufficient. There is a shortage of specialists to lead the training, even though such resources might become available (Tredinnick, L. 2019).

4. Regulations to Combat Cryptocurrency Crime

It is common practice to believe that regulation is legal, consisting of clearly defined rules and regulations. However, the regulation of cryptocurrencies can take many different forms, mainly classified as either technological or legal measures below.

4.1. Technical Regulatory Approaches

The most effective approach to accomplish something is almost always through applying technically based solutions. This is especially true in the realm of cybercrime. For instance, making it illegal to conduct fraud using cryptocurrencies is not a practical approach to decreasing cryptocurrency fraud. There are other ways to reduce cryptocurrency fraud. Customers are unable to differentiate between types of cryptocurrencies that are authentic and those that are either false or highly speculative and, as a result, exploitative of their lack of information about cryptocurrencies. In a similar vein, awareness campaigns are an excellent place to start, but owing to the complexity of the methods used by criminals, they will not be enough; the vast majority of customers cannot differentiate between a real and fake cryptocurrency (Nghiem, H et al., 2021).

4.2. Fraudulent Content Is Blocked

New technological and business-oriented methods are constantly being developed to combat crypto fraud. Internet Service Providers and social media businesses may check for fraudulent behaviour and prohibit access to a false website or social media link. A blocklist is a list of local websites and media links that may be erased from the internet. This organization might be government-related or non-profit. Even if a client employs a VPN or TOR, most customers, particularly those with less digital knowledge, won't (Kamps, J. et al., 2022).

Despite internet warning flags indicating the product they are investing in may be a fraud, many consumers nonetheless invest in it. Despite warnings and education, many fall for these frauds. According to 2017 Ponzi research in China, even after being misled, investors continued to participate in similar Ponzi schemes (Fei et al., 2020). 74 Sociocultural factors and advertising tactics are essential in attracting investment, according to the study. High living costs, inflation, false advertising, weak banking systems, and complicated legal systems (Maurushat, A., & Halpin, D. 2022).

Our investigations discovered that many of the fraud victims were seasoned investors, including those who were wealthy. In our experience, these investment frauds target middle-aged to older men, ages 35 to 65. Victims respond like gamblers who keep putting money in slot machines for a 1 in 1 million chance, even though they are unaware of the likelihood that their money will be returned to them (Ahn, B. 2022).

4.3. Extensions for Web Browsers/ Add-ons

Another concept gaining traction is the idea of an official browser plugin that can identify possible instances of fraud and scams and notifies users of the possibility that the link they are about to click on is fraudulent. The browser add-on may come equipped with its URL checking. This URL checker might provide a comprehensive list of validated websites that are safe for use. It could also notify users when navigating a website that has been reported or marked for engaging in suspicious conduct. In addition, the URL checker could provide a list of websites that have been reported for engaging in questionable activities. Our add-on for browsers could undertake HTML scanning and individual web pages, looking for dubious websites cloaked across several websites as false pictures or fraudulent download buttons (Aziz, R. M et al., 2022).

It is feasible to build the extension with cooperation from commercial businesses, police enforcement, and regulatory agencies such as security commissions to give it a veneer of legitimacy. This possibility exists because it is desirable to create the extension. The issue with extension browsers is, once again, one of fraud: Cybercriminals will acquire knowledge from their past errors and start selling extensions that give the impression of being honest. Because of this, the strategy has the potential to be abused in order to make it easier to defraud investors. Consequently, this possibility exists (Panda, S. K. et al., 2021).

4.4. Stable-Coins

Stablecoins are cryptocurrencies whose value is related to an external asset, commonly the U.S. dollar or gold. This theoretically stabilizes the cryptocurrency's price, reducing market volatility. Recent advancements have raised the potential that blockchain technology might be used to improve international payment networks, primarily by developing a worldwide stable coin (GSC). The GSC's dangers and concerns have not been adequately handled. 2019 G7 research discussed GSCs. The research indicated that risks and problems outweigh benefits. Regulation and scale are the main GSC dangers and concerns (Jadye S. et al., 2021).

A GSC will aim to address regulatory issues related to privacy (as opposed to secrecy or anonymity), cyber security, consumer protection, and AML/CTF, to mention a few. Lack of internet access is the biggest concern overall. According to Staista.com, 40.6% of the world's population will not have internet access by 2021. 2021 forecasts. This makes blockchain access more difficult. Bitcoin ATMs and other cash-based conversion services present a hurdle. As of June 2021, Coinatmradar.com estimated 21,465 bitcoin ATMs across 71 countries. Despite 63.5% of countries without ATMs, there is one for every 357.5 million people globally. (Sanz-Bas, D. et al., 2021).

5. Approaches to Regulation from a Legal Perspective

Numerous jurisdictions like Pakistan are in the process of enacting a plethora of new regulations that, among other things, legalize cryptocurrencies, prohibit cryptocurrencies or initial coin offerings (ICOs), mandate the mandatory registration of exchange points, enact mechanisms for mandatory identification, the provision of trust certificates, and the imposition of limits on the selling of cryptocurrency. It does not include a comprehensive legal analysis of the many different kinds of rules; instead, it discusses the broad categories of tactics and the possible advantages and downsides of the approach (Sanz-Bas, D. et al., 2021).

5.1. Cryptocurrency and Blockchain Legalization

First, the notion that cryptocurrencies and blockchain should be legal may appear counterintuitive. One could assume that most recently developed technology is by definition lawful. The decision of some nations to legalize virtual currencies can be seen as more of a statement about the market than anything else. The Malta Digital Innovation Authority is a governing organization established by the Maltese government. Its mission is to develop and practice the act's guiding principles. However, the law provides the developer with a certification that certifies the innovation, which helps generate trust in the market. Designing or deploying a blockchain or smart contract does not need a license. One must apply for certification that they have met the law's standards (Madadi M. et al., 2021).

In 2020, 70% of the enterprises that were part of Malta's pioneering concept had opted not to get regulated under government rules. These firms have not filed for a trusted service license. Businesses that deal in cryptocurrency have decided not to become certified, raising the potential that they wish to hire criminals. Such firms may decide that the standard is too onerous or that market analysis shows certification is not necessary to win customer trust. However, these are all just speculations. Therefore, nothing can be proven (Shestak, V., & Mefedenko, A. 2021).

5.2. Ban Crypto Exchanges

It has been chosen by the governments of several nations, including Egypt, Iraq, Nepal, Pakistan, and Vietnam, to criminalize blockchain technology and cryptocurrencies. Making a conduct a criminal offence and prohibiting it are two entirely different concepts to consider. Because bitcoin transactions are secret, individuals may hide their online identities by using TOR, TAILS, or a VPN (VPN). The restriction is unlikely to curb cryptocurrency-related crime (Xi, C. 2022) successfully.

5.3. Cryptocurrency, ICO Regulation & Restrictions

As seen before, initial coin offerings (ICOs) are hazardous investments frequently associated with fraud. The initial coin offering (ICO) market has, up until very recently, been exempt from the regulation that applies to the security industry and initial public offers of equities. There have been reports of initial coin offerings (ICOs) raising billions of dollars; as a result, governments worldwide have developed legislation for investing in cryptography. Countries such as the United States of America, China, Australia, and the European Union are examples of these. Since 2017, coin offerings (ICOs) have been prohibited in China. According to a report published by the Library of Congress in 2018 and titled Regulation of Cryptocurrencies around the World79, it was mentioned that certain governments are working on creating their own nationalized or regional cryptocurrencies. Only the national governments of countries like China, Thailand, Indonesia, and others are authorized to nationalize cryptocurrencies. These many kinds of cryptocurrencies are now being generated to control the market in terms of profits and illegal activities. It is impossible to determine from the available data whether or not this method is effective (Brown VII, S. H. 2022).

Initial coin offerings (ICOs) in other jurisdictions, such as Australia and the United States, are governed by the securities and investing statutes relevant to those countries. However, they have not been outright banned. For instance, if you live in Australia and want to launch an initial coin offering (ICO), you must have a license to operate in the country's financial services industry. This license comes with a slew of laws and regulations that must be followed. It is the same in the United States, where initial coin offers (ICOs) or digital asset security offerings (DASOs), more commonly known under the law, are subject to mandatory licensing (Srivastava, A. 2021).

5.4. Exchange Point Regulation & AML

Exchange points continue to be an essential tool for determining whether or not money is being laundered, criminal profits are being laundered, and, ultimately, whether or not criminals are utilizing cryptocurrencies. Exchange points are regulated under anti-money laundering and anti-terrorism laws. A company must have a local presence to operate a cryptocurrency exchange or platform in Australia. Australia must comply. These guidelines help clients discover lawful bitcoin exchanges and should help law enforcement identify criminals and illegal profits. These standards help customers find legitimate crypto exchanges.

Thefts may easily circumvent such measures, however. They are fast. Cryptocurrency transactions do not need a central authority or third-party go-between. This is not always the case with exchange points, even if it works roundaboutly. This requires clarification (Hsu, Y., & Liu, C. 2021).

If you used an exchange point to launder money or obtain criminal earnings, you might undertake one of the following to escape law enforcement. Start by using a well-known exchange location that criminal groups promote and that is either unregulated or unlikely to comply with rules. These organizations may not comply with rules. Second, using a bitcoin mixer makes it hard to track transactions back to their originator (Madadi M. et al., 2021). One must confine their victims to countries beyond the exchange point to avoid Australia's complex investment fraud rules. These regulations safeguard Aussies against investment fraud. This finishes the job. Written rules seldom achieve their writers' goals. The following example illustrates this principle. Consequently, the danger of a traceback has been lowered, and you may now withdraw cash (or equivalent) from the exchange (Shestak, V., & MEFEDENKO, A. 2021).

You could pay a sophisticated terrorist outfit, or a criminal organization might hire the services of a crypto middleman or broker. Both of these options are viable options. This broker protects your cryptocurrency holdings and allows you to exchange them for fiat cash or precious commodities such as gold. Your cryptocurrency holdings may also be converted into fiat currency. Why would a group participating in illegal conduct utilize a location like this? It is the same as when criminal groups utilize precious artwork as collateral for large drug transactions or weapon sales. Those are also examples of illegal activity. This rule is only broken when a person or entity that sits amid the transaction backs the cryptocurrency. Despite all of the enthusiasm around bitcoin, it is not yet extensively utilized in actual transactions, and using it may not be easy. For instance, I would not be able to buy a Ferrari by just stepping into a car dealership and paying for it with gold or cryptocurrency. The method of extracting value via the broker is more streamlined and less vulnerable to inspection when compared to other methods, such as withdrawing money from a Bitcoin exchange. Despite the significance of these brokers, there is a dearth of information that the general public can access on them (Madadi M. et al., 2021).

The writers have taken part in investigations where the victims were situated in various jurisdictions inside Australia and internationally. In one instance, the person responsible for the scam was tracked down and apprehended in one of Australia's states (where there were no victims). However, since he took cryptocurrencies from a recognized exchange, he was prosecuted in a different state than where the exchange was located. Law enforcement in the Bitcoin exchange's jurisdiction told the victims they lacked jurisdiction since the exchange lacked a sufficient link to criminal profits (Arianna, T. et al., 2022). Law enforcement in the Bitcoin exchange's jurisdiction informed the victims. In addition, they specified that both the victims and the arrests must occur inside the same judicial district. The author believes that this interpretation of the law is wrong. Criminals receive the message from this type of official response that Australia is open for business regarding cybercrime, including the use of regulated cryptocurrency exchanges. To increase Australia's procedures to protect against investment fraud, confine their victims to far-off places. This is the only thing necessary to avoid compliance with the requirements. When put into practice, rules virtually never function as their authors intended them to when the regulations were written down. This specific example demonstrates the principle that was made in more detail (Shih, D. H. et al., 2021).

6. Recommendations and Conclusions

There is still hope for combating fraud enabled by cryptocurrencies, which depend on cryptocurrencies. When billions of dollars in taxable revenue are stolen, law enforcement and regulatory authorities will eventually catch up and stop the most despicable actions. In order to effectively combat crypto crime, a combination of regulatory and technical strategies, as well as public-private collaboration, is necessary. In addition, the levels of digital literacy required of regulators, law enforcement agencies, and private investigators must be significantly increased. The following is a suggestion for immediate consideration from our team. The first step is to enhance law enforcement's training regarding digital crimes. Second, private groups and regulatory and law enforcement authorities must cooperate more to reduce fraud and disrupt the economic model. This disrupts the economic model. When the legislative frameworks of agencies do not support collaboration, the frameworks themselves need to be revised. Access to and use of law enforcement data should ideally be provided, under suitable control measures, for private agents screened and certified. Because one of the authors is now working on his or her graduate thesis on the subject, the details of such a proposal will not be laid out in this chapter. In conclusion, there is a need for additional studies to be conducted in order to improve the tracking and monitoring of cryptocurrencies.

References

Ahn, B. (2022). Implementation and Early Adoption of an Ethereum-Based Electronic Voting System for the Prevention of Fraudulent Voting. *Sustainability*, 14(5), 2917.

Arianna, T., Kamps, J., Akartuna, E. A., Hetzel, F. J., Bennett, K., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. Crime Science, 11(1).

ARIKAN, N. İ. (2021). Identification of the Variables Effecting the Value of the Cryptocurrency. The Journal of International Scientific Researches, 6(1), 27-34.

Austin, J. (2021). Stock markets play ‘whack a mole’with Pump and Dump schemes. Available at SSRN 3972431.

Aziz, R. M., Baluch, M. F., Patel, S., & Ganie, A. H. (2022). LGBM: a machine learning approach for Ethereum fraud detection. International Journal of Information Technology, 1-11.

Bansal, U. (2021, May). A review on ransomware attack. In 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC) (pp. 221-226). IEEE.

Bellavitis, C., Fisch, C., & Wiklund, J. (2021). A comprehensive review of the global development of initial coin offerings (ICOs) and their regulation. Journal of Business Venturing Insights, 15, e00213.

Brown VII, S. H. (2022). Gambling on the Blockchain: How the Unlawful Internet Gambling Enforcement Act Has Opened the Door for Offshore Crypto Casinos. Vanderbilt Journal of Entertainment & Technology Law, 24(3), 535.

Caliskan, K. (2020). Data money: The socio-technical infrastructure of cryptocurrency blockchains. Economy and Society, 49(4), 540-561.

Castonguay, J. J., & Stein Smith, S. (2020). Digital Assets and Blockchain: Hackable, Fraudulent, or Just Misunderstood?. Accounting Perspectives, 19(4), 363-387.

Cheung, J. (2019). The Case for Crypto: Why Cryptocurrencies Should Be Universally Adopted. Int'l Fin. L. Rev., 65.

Chohan, U. W. (2019). Initial coin offerings (ICOs): Risks, regulation, and accountability. In Cryptofinance and mechanisms of exchange (pp. 165-177). Springer, Cham.

Christiansen, N. B., & Jarrett, J. E. (2019). Forfeiting cryptocurrency: decrypting the challenges of a modern asset. Dep't of Just. J. Fed. L. & Prac., 67, 155.

Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (2019). Cryptocurrencies as a financial asset: A systematic analysis. International Review of Financial Analysis, 62, 182-199.

Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (2019). Cryptocurrencies as a financial asset: A systematic analysis. International Review of Financial Analysis, 62, 182-199.

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A cyber-kill-chain based taxonomy of crypto-ransomware features. Journal of Computer Virology and Hacking Techniques, 15(4), 277-305.

Desmond, D., Salmon, P., & Lacey, D. (2021). Functional systems within cryptolaundering processes: a work domain analysis model of cryptolaundering activities. Journal of Cyber Policy, 6(2), 155-176.

Dimpfl, T., & Peter, F. J. (2021). Nothing but noise? Price discovery across cryptocurrency exchanges. Journal of Financial Markets, 54, 100584.

Dupuis, D., Smith, D., & Gleason, K. (2021). Old frauds with a new sauce: digital assets and space transition. Journal of Financial Crime.

Dyson, S., Buchanan, W. J., & Bell, L. (2019). The challenges of investigating cryptocurrencies and blockchain related crime. arXiv preprint arXiv:1907.12221.

Felix, T. H., & von Eije, H. (2019). Underpricing in the cryptocurrency world: evidence from initial coin offerings. Managerial Finance.

Gómez-Hernández, J. A., Sánchez-Fernández, R., & García-Teodoro, P. (2022). Inhibiting crypto-ransomware on windows platforms through a honeyfile-based approach with R-Locker. IET Information Security, 16(1), 64-74.

Hornuf, L., Kück, T., & Schwienbacher, A. (2021). Initial coin offerings, information disclosure, and fraud. Small Business Economics, 1-19.

Hsu, Y., & Liu, C. (2021). Legalization of Central Bank Digital Currency under Blockchain Industry. CONVERTER, 450-458.

Issac, A. C., & Baral, R. (2020). A trustworthy network or a technologically disguised scam: A biblio-morphological analysis of bitcoin and blockchain literature. Global Knowledge, Memory and Communication.

Jadye, S., Chattopadhyay, S., Khodankar, Y., & Patil, N. (2021). Decentralized Crowdfunding Platform Using Ethereum Blockchain Technology.

Kamps, J., Trozze, A., & Kleinberg, B. (2022). Cryptocurrencies: Boons and curses for fraud prevention. In A Fresh Look at Fraud (pp. 192-219). Routledge.

Kethineni, S., & Cao, Y. (2020). The rise in popularity of cryptocurrency and associated criminal activity. International Criminal Justice Review, 30(3), 325-344.

Kreminskyi, O., Kuzmenko, O., Antoniuk, A., & Smahlo, O. (2021). International cooperation in the investigation of economic crimes related to cryptocurrency circulation. Studies of Applied Economics, 39(6).

Kyriazis, N. A. (2021). A survey on volatility fluctuations in the decentralized cryptocurrency financial assets. Journal of Risk and Financial Management, 14(7), 293.

Li, Z., Liu, W., Chen, H., Wang, X., Liao, X., Xing, L., & Zou, D. (2022, May). Robbery on DevOps: Understanding and Mitigating Illicit Cryptomining on Continuous Integration Service Platforms. In 2022 2022 IEEE Symposium on Security and Privacy (SP)(SP). IEEE Computer Society, Los Alamitos, CA, USA (pp. 363-378).

Liu, Y., Tsyvinski, A., & Wu, X. (2022). Common risk factors in cryptocurrency. *The Journal of Finance*, 77(2), 1133-1177.

Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. The British Journal of Criminology.

Maurushat, A., & Halpin, D. (2022). Investigation of Cryptocurrency Enabled and Dependent Crimes. In Financial Technology and the Law (pp. 235-267). Springer, Cham.

Nadlifatin, R., Persada, S. F., Clarinda, M., Handiwibowo, G. A., Laksitowati, R. R., Prasetyo, Y. T., & Redi, A. A. N. P. (2022). Social media-based online entrepreneurship approach on millennials: A measurement of job pursuit intention on multi-level marketing. Procedia Computer Science, 197, 110-117.

Nghiem, H., Muric, G., Morstatter, F., & Ferrara, E. (2021). Detecting cryptocurrency pump-and-dump frauds using market and social signals. Expert Systems with Applications, 182, 115284.

Nijsse, J., & Litchfield, A. (2020). A taxonomy of blockchain consensus methods. Cryptography, 4(4), 32.

Ogunyolu, O. A., & Adebayo, A. O. (2022). An appraisal of ethical issues and the effect of artificial intelligence on the cryptocurrency market. Global Journal of Engineering and Technology Advances, 11(02), 063-070.

Panda, S. K., Mohammad, G. B., Nandan Mohanty, S., & Sahoo, S. (2021). Smart contract-based land registry system to reduce frauds and time delay. Security and Privacy, 4(5), e172.

Pernice, I. G., Henningsen, S., Proskalovich, R., Florian, M., Elendner, H., & Scheuermann, B. (2019, June). Monetary stabilization in cryptocurrencies–design approaches and open questions. In 2019 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 47-59). IEEE.

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.

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. International Journal of Information Management Data Insights, 1(2), 100013.

Rognone, L., Hyde, S., & Zhang, S. S. (2020). News sentiment in the cryptocurrency market: An empirical comparison with Forex. *International Review of Financial Analysis*, 69, 101462.

Sai, A. R., Buckley, J., Fitzgerald, B., & Le Gear, A. (2021). Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management*, 58(4), 102584.

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.

Sharma, D. K., Pant, S., Sharma, M., & Brahmachari, S. (2020). Cryptocurrency mechanisms for blockchains: models, characteristics, challenges, and applications. Handbook of research on blockchain technology, 323-348.

Shestak, V., & MEFEDENKO, A. (2021, April). Countering to Legalization of Funds, Obtained With the Help of Using Digital Financial Assets. In For citations: Shestak, VA & Mefedenko, AM (2021). Countering to legalization of funds, obtained with the help of using digital financial assets. Regulation of legal relations: problems theory and practice. XX annual international student scientific and practical conference (1-2 April 2021). Mos.

Shih, D. H., Huang, F. C., Chieh, C. Y., Shih, M. H., & Wu, T. W. (2021). Preventing return fraud in reverse logistics—A case study of ESPRES solution by Ethereum. Journal of Theoretical and Applied Electronic Commerce Research, 16(6), 2170-2191.

Thakur, S., Chaudhari, S., & Joshi, B. (2022). Ransomware: Threats, Identification and Prevention. Cyber Security and Digital Forensics, 361-387.

Tredinnick, L. (2019). Cryptocurrencies and the blockchain. Business Information Review, 36(1), 39-44.

Twomey, D., & Mann, A. (2020). Fraud and manipulation within cryptocurrency markets. Corruption and fraud in financial markets: malpractice, misconduct and manipulation, 624.

Villányi, B. (2021). Money Laundering: History, Regulations, and Techniques. In Oxford Research Encyclopedia of Criminology and Criminal Justice.

Wątorek, M., Drożdż, S., Kwapień, J., Minati, L., Oświęcimka, P., & Stanuszek, M. (2021). Multiscale characteristics of the emerging global cryptocurrency market. Physics Reports, 901, 1-82.

Wright, C. S. (2021). Bitcoin: The Most Law-Abiding System Ever Created. Available at SSRN 3942115.

Xi, C. (2022). The End of the War or the Commencement of Battle? Cryptocurrency Regulation in China. Cryptocurrency Regulation in China (April 19, 2022).