IMSISS
International Master
Security, Intelligence
& Strategic Studies

Erasmus
Mundus

CRYPTOCRIME, BLOCKCHAIN, AND BEYOND: INVESTIGATING CRIMINALS' ILLICIT USE OF CRYPTOCURRENCY AND EXPLORING LAW ENFORCEMENT OPPORTUNITIES

July 2022

Glasgow Student Number: 2481810
DCU Student Number: 20109369
Charles Student Number: 28976638

Presented in partial fulfilment of the requirements for the degree
of

International Master in Security, Intelligence and Strategic Studies

Word Count: 22050

Supervisor: Dr James Gallen

Date of Submission: 26th July2022

University of Glasgow

DCU

UNIVERSITY OF TRENTO

CHARLES UNIVERSITY

Abstract

In recent years, cryptocurrencies have evolved and become widespread. The anonymity and decentralisation of these technologies have attracted criminals who use them to buy and sell illegal products on the black market while hiding their identities and avoiding punishment. Cryptocurrencies, a new technological development, have their own positive and negative consequences as they can be used by criminals to perform illegal activities. At the same time, cryptocurrencies are being used by law enforcement bodies for investigations. Also viewed as a concern is the illicit use of cryptocurrencies for money laundering, terrorism financing and sanctions evasion on the global levels. The introduction and advancement of analytical tools enable law enforcement to track suspect addresses using the blockchain's records of bitcoin transactions. Concurrently, anti-money laundering (AML) rules and financial authorities have played a crucial role in the battle against money laundering and collecting vital role in the fight against money laundering and the collection of intelligence on suspicious activity conducted via financial institutions. This dissertation's study aims to evaluate the illegal and legal usage of cryptocurrencies to understand better whether they should be considered a danger to global or national security or a chance for technical progress. At the same time demonstrates other use cases, such as effective governance using blockchain technologies.

Keywords: Cryptocurrencies, Bitcoin, Blockchain, Money, Money Laundering, Darknet Market, Blockchain Forensics

Acknowledgement

I am grateful to Dr James Gallen, my research supervisor, for his sage advice, support, and keen observations, which helped me manage the complexities of writing a thesis. I also want to thank the IMSISS personnel for giving me clear and concise direction and aiding me with project-related administrative responsibilities. I also appreciate Mr Aditya Khurana's assistance in proofreading the work.

I want to express my gratitude to my therapist, Hiba, who helped me overcome months of depression and sadness and inspired me to focus on my studies. Lastly, I want to thank my friends and family for their unwavering support and encouragement during my studies.

Table of Contents

List of Abbreviations

BTC	Bitcoin
DeFi	Decentralized Finance
NFT	Non-Fungible Token
ICO	Initial Coin Offering
UN	United Nations
P2P	Peer-to-Peer
DLT	Distributed Ledger Technology
CBDC	Central Bank Digital Currency
PoW	Proof of Work
PoS	Proof of Stake
BoE	Bank of England
ECB	European Central Bank
IMF	International Monetary Fund
FATF	Financial Action Task Force
IOU	I Owe You
P2P	Peer to Peer
KYC	Know Your Customer
AML	Anti-Money Laundering
SHA256	Secure Hash Algorithm – 256 Bits
5AMLD	5th Anti-Money Laundering Directive
6AMLD	6th Anti-Money Laundering Directive
CFTC	US Commodity Futures Trading Commission

1 Introduction

1.1 Rise of Cryptocurrencies and the Associated Threats

The technology boom in recent decades has led to many innovations, and new technological inventions in different sectors and one notable sector are the financial sector. First, the modern financial companies powered by technology, often known as 'FinTech', digitalised money from its paper form and pushed the whole financial eco-system towards a paperless system. Then the people who had trust issues with the traditional monetary system started working towards peer-to-peer electronic currency, which led to the birth of Bitcoin and several other cryptocurrencies. The idea of Bitcoin came into existence from a whitepaper published by pseudonymous author "Satoshi Nakamoto" on a random internet forum. The white paper by Satoshi outlined the principles of a virtual cash system that would allow users to send virtual funds anonymously and securely without the involvement of central financial institutions (Nakamoto, 2008). Several works were done on digital cash before Bitcoin, but none had the promising feature of *decentralisation, pseudo-anonymity, and transparency* in Bitcoin architecture. The decentralisation and transparency were possible in Bitcoin due to Blockchain, the underlying technology, a digital public ledger where all transactions are recorded using cryptography and shared in the distributed network. The blockchain registers the Bitcoin transactions, and the parties involved are identified using Bitcoin addresses created using cryptographical methods, enabling pseudo-anonymity. Since the inception of Bitcoin, several other virtual currencies have emerged, and since most of them use cryptography for security, they are termed cryptocurrencies. As of June 2022, there are more than a thousand cryptocurrencies, as shown by a popular cryptocurrency tracker CoinMarketCap.

The cryptocurrency market first peaked in 2017 as the market saw a dramatic increase, with the price of Bitcoin reaching from $1,000 to $20,000. This led to much public interest in the crypto sphere, but this did not last long as the market crashed and lost momentum. However, the pandemic brought dramatic turmoil to the crypto market, with the overall market value reaching a trillion dollars, with BTC leading the value with prices as high as $60,000. The total market capitalisation of cryptocurrencies reached almost $3 trillion in 2022 (refer to Figure 1 in the Appendix). This led to the increased public interest and various innovations in the crypto sphere and gave rise to a new financial market, Decentralized Finance. The whole concept of DeFi is based on removing central authority from any financial services. The innovation in crypto also led to the introduction of Non-Fungible Tokens (NFTs)[1], Metaverse and Web3[2], which have been making headlines with digital arts and virtual reality companies valued at millions of dollars.

While the innovations in the field of crypto and blockchain have been phenomenal, most of them operated in unregulated spaces. Their core features, such as decentralisation, make it harder to enforce regulations without an overseeing authority. The growing market, innovations and lack of rules make the crypto space more susceptible to criminals. Briefly, the core features of cryptocurrencies today imply that they satisfy many of the demands of terrorists, money launderers, and other criminals who rely on the capacity to move cash globally (Keene, 2014). As cryptocurrency usage grows, the illegal use of cryptocurrency is increasing. A new report shows that cryptocurrency-based crime was at an all-time high in 2021, with transactions amounting to $14 billion over the year compared to $7.8 billion in 2020 (Chainalysis, 2022b). Chainalysis, the private blockchain forensic company, identifies criminal usage of various cryptocurrencies for illicit activities such as terrorism financing, sanction bypass, ransomware [3]and darknet [4]usage by tracking addresses related to illegal activities (refer to Figure 2 in Appendix). While the amount used for illicit activities is

[1] **NFTs** are digital tokens which help to represent ownership of unique items which involves art, real estate, and any collectables.

[2] **Web3** is a term used to describe the future of the internet built on decentralized blockchains.

[3] **Ransomware** attacks are a type of cyberattack which restricts the system or file access to the user by encrypting it. The user (victim) will be shown a message on the screen to pay a ransom to get the decryption code and gain access to their system. Most ransomware has a timer and failure to make the payment within that time causes the computer to crash and delete all the files from the system. Ransomware attacks are hot topics, and recently cryptocurrencies are being used as a mode of payment for ransom, a growing concern.

[4] **Darknet** refers to a private network only accessible by specific software or configuration or authorisation and is often used to host dark web pages for illegal purposes.

staggering, it is still relatively low compared to the amount linked to legitimate usage of cryptocurrencies. Critics argue that cryptocurrencies and blockchain present more opportunities for law enforcement than criminals as blockchain is transparent and allows for more advanced forensic tools. Using the Ethereum blockchain for distributing aid to Syrian refugees by the World Food Programme (WFP) proved successful. It helped the UN to distribute more than $1 million in 2017 (Starkie, 2017). This pilot program run by the UN was far more efficient and helped improved UN operations and cash-based transfers in the aid process. Estonia, known to be the world's most advanced digital society, uses blockchain in its e-government system. So far, it has proven to be efficient in delivering public services while increasing the security and resilience of the available government systems (Parol, 2018).

This research will investigate how criminals misuse cryptocurrencies and to what extent they have been misused with the current technologies. Further exploring blockchain use cases, this research tries to identify how law enforcement, regulatory bodies, and the public sector can utilise this new technology to contribute literature on the field.

1.2 Research Question

The increasing usage of blockchain technologies, growing public interest in cryptocurrencies and rapid development in the field combined with most of the academic literature associated with financial or non-governmental sectors provide an opportunity to research public sector use cases of blockchain and its impact on national or global security. This research can be divided into two parts - the first part aims to analyse the current illicit usages of blockchain technologies, such as criminals using cryptocurrencies to fund their crime, and the second part of the research aims to explore the legitimate use cases and potential opportunities for the public sector and law enforcement bodies. Most states see Bitcoin and other cryptocurrencies as a threat to the government due to their core feature of decentralisation and anonymity. Countries like China have banned cryptocurrencies but embraced blockchain technologies to create centralised digital currency (*USC U.S.-China Institute*, 2021). At the same time, countries like the US and the UK have treated them as assets and brought taxation laws and developed regulatory frameworks to bring them under the legislation. There is no standard agreement on how to regulate cryptocurrencies and whether to perceive them as a threat or opportunity for technological advancement. While much focus is given to cryptocurrencies, other concepts, such as the NFTs and Decentralized Finance (DeFi), are rapidly developing in the crypto space. These areas need more research to understand their potential threat to global or national security. This presents us with an opportunity to dive deeper into the subject matter. This research aims to analyse the illegal use cases of cryptocurrencies and explore legitimate use cases. As a result, the study evaluates the illegal and legal usage of cryptocurrencies to understand better whether they should be considered a danger to global or national security or a chance for technical progress. Different states and public organisations have been working on regulatory frameworks and policies for cryptocurrencies and overall blockchain technologies. This research also aims to analyse such regulatory frameworks or legislation, which will help better understand how different states perceive the rapidly developing field of cryptocurrency and blockchain technologies.

1.3 Research Methodology

As mentioned in the previous part, this research is divided into two parts – the first is associated with the investigation of illegal usage of cryptocurrencies, and the second is dedicated to exploring potential use cases and opportunities for the public sector, including law enforcement bodies. For this purpose, the research employs mixed methods combining both quantitative and qualitative research methods to provide a holistic view of the subject matter. Various case studies will be done to understand the illegitimate use cases of cryptocurrencies, performing document analysis of different reports published by well-known institutions around the subject matter. Due to limited resources for data collection and the non-availability of blockchain forensic tools for academics, the primary statistical data of blockchain transactions are omitted; instead, statistical data and graphs from the published reports will be referenced for describing cryptocurrency-related data and establishing money flow in different case studies. As blockchain technologies are rapidly developing and new use cases are being explored, there is considerably limited resources and published literature; however, in the recent two years, research in the field has been increasing with the government in the countries like the US and EU exploring regulatory frameworks for cryptocurrencies and blockchain technologies. This research cites some significant events and cases around the subject domain along with empirical data, presents them as proof of the arguments mentioned and helps the reader get more clarity on the subject matter.

1.4 Scope and Limitation

This thesis aims to investigate different crimes done using cryptocurrency through case studies exploring reports and articles published in recent years. The study will focus on two major areas: first, the types of crimes committed using the cryptocurrency – cyberattacks and ransomware to steal cryptocurrency and crypto laundering for supporting crimes beyond blockchain, such as terrorism financing and nuclear missile funding, and second, investigate legitimate use cases along with potential use cases while exploring regulatory frameworks and legislation.

This research acknowledges its limitation as most of the analysis is referenced from third parties' reports and while lacking own data samples for analysis. This is due to the massive volume of data in the blockchain and the lack of academic blockchain forensic tools readily available for student researchers.

1.5 General Structure of Thesis

The structure of this dissertation can be broken down into six major chapters. Each chapter is further sub-divided into different sub-topics for clarity. Chapter 1, the introduction part of the thesis, briefly touches on the concept of blockchain, cryptocurrencies and their impact on global or national security while outlining the thesis's research questions, methodologies, and overall structure.

In Chapter 2, the thesis looks deeper into the technology associated with cryptocurrencies and its brief history giving an overview of the working of blockchain technologies and cryptocurrencies along with the overall market structure. At the end of Chapter 2, the thesis provided legal and compliance issues with cryptocurrencies and how different countries are dealing with cryptocurrencies discussing their regulatory framework around cryptocurrencies. In Chapter 3, the quantitative and qualitative analysis of cryptocurrencies and blockchain technology is done along with some case studies to investigate how criminals use cryptocurrencies and the mechanism of illicit activities on the blockchain. In Chapter 4, the thesis investigates legitimate use cases through qualitative analysis of successful projects implemented using blockchain technologies in the public sector and governance and discusses opportunities presented to law enforcement bodies. Chapter 5 explores the new regulations proposed by states such as the United Kingdom and the European Union, and the United States to embrace the rapidly developing crypto and blockchain technologies and highlights some of the primary law enforcement activities that occurred in the crypto space in the last year. Combining these, the future of cryptocurrencies is discussed in contrast to such regulatory actions. Then, the final chapter provides the conclusion with the results drawn from the analysis of the case studies in the earlier chapters and tries to answer the research questions.

2 Blockchain and Cryptocurrencies – A Primer

2.1 Issues with Centralized Financial Systems

Before explaining the concept of blockchain and cryptocurrencies, it is essential to understand the flaws within the current centralised financial systems, specifically related to the fiat [5]currency system. As Satoshi wrote in his paper:

> "*The root problem with conventional currency is all the trust required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. (Nakamoto, 2008)*"

While there are several fundamental macroeconomic issues with fiat money, Satoshi highlights the issue of trust, which is provided via third parties in the conventional monetary system. The trust has been violated on several occasions, and the unethical practices by the third party have even contributed to the global financial crisis in history. This trust issue led to the existence of Bitcoin and blockchain technology, which aims

[5] **Fiat** currency is the currency issued by the government that is not backed by any physical commodity such as gold and silver. It derives its value from supply and demand and the stability of the government that issues them.

to remove the third party with algorithmic trust backed by cryptography. Nakamoto envisioned a decentralised digital payment system that eliminates the need for third-party intermediaries and prevents double spending via a secure, reliable, and unchangeable public database known as a blockchain with limitless scalability. Satoshi Nakamoto is the pseudonym used by the creator(s) of the Bitcoin cryptocurrency. Although the moniker Satoshi Nakamoto is often associated with Bitcoin, the identity of the person represented by the name has never been confirmed.

2.2 Blockchain – The Technology Empowering Cryptos

"Bitcoin: A Peer-to-Peer Electronic Cash System" was published by an anonymous author under the pseudonym Satoshi Nakamoto in 2008, proposing a novel method for transferring "funds" in the form of "Bitcoin" in a peer-to-peer (P2P) manner. In Nakamoto's paper, the underlying technology for Bitcoin was referred to as Blockchain, which refers to a specific method of organising and storing data and transactions. Subsequently, other forms of collecting data and transactions for P2P asset transfers were developed, resulting in the term "Distributed Ledger Technology" (DLT) being used to refer to the broader category of technologies (Natarajan, Krause and Gradstein, 2017).

Blockchain thus can be defined as a particular type of DLT which is capable of recording and sharing data across multiple ledgers (data stores), and each ledger has exact duplicate data records and is collectively maintained and controlled by a distributed network of computers, often referred to as nodes (Houben and Snyers, 2018). Blockchain employs an encryption technique known as cryptography. It utilises specific mathematical algorithms to create and verify a continuously growing data structure to which data can only be added. Existing data cannot be removed – in the form of a chain of "transaction blocks" that functions as a distributed ledger, making it immutable (Natarajan, Krause and Gradstein, 2017). It can exhibit other functions as well, such as there are permissionless blockchain and permissioned blockchain.

- **Permissionless Blockchain:** The permissionless blockchain is an open blockchain where anyone can join or leave without needing to have approval from a central entity. To join the permissionless blockchain, one can download relevant software and keep a copy of the ledger, which makes them part of the network. Most cryptocurrencies (Bitcoin, Ethereum, Solana, etc.) operate on the permissionless blockchain. This type of blockchain is also called public blockchain, as anyone can participate in the consensus and validate the data. Permissionless blockchain provides complete transparency of the users and transactions.

- **Permissioned Blockchain**: The permissioned blockchain is a closed blockchain where the entities must be pre-approved by a central authority (or the network administrator) to join the network. This type of blockchain can further be subdivided into *open permissioned* and *enterprise blockchain*. Anyone can view the open permissioned blockchain, but only approved network participants can update the transactions. On the other hand, the enterprise blockchain is closed and only accessible to network administrators for transaction generation or ledger updates. Some cryptocurrencies, such as Ripple and Neo, operate on an open permissioned blockchain. Hyperledger Fabric and R3's Corda are other examples of enterprise blockchain used by businesses or governments for their blockchain projects. One widespread use case of enterprise blockchain is the creation of *Central Bank Digital Currency (CBDC)*, a cryptocurrency issued and regulated by the nation's monetary authority.

2.2.1 How does Blockchain Work?

The working mechanism of blockchain is simple. However, a few key terminologies should be explained before explaining the operating mechanism.

- **Block** – a block in a blockchain is a collection of data (transactions).
- **Miner** – each node of the network that is responsible for validating transactions and creating a new block
- **Mining** – the process of validating and creating new blocks using computational power

- **Public and Private Key** – every user on a blockchain has two sets of keys, a public key known to everyone and used as walled addresses and a private key used for a digital signature for a transaction.
- **Consensus Mechanism** – set of predefined cryptographic methods which ensure correct sequencing and validations of transactions on the blockchain.

When a user initiates a transaction on a blockchain, the transaction goes into an aggregated pool of transactions. The network verifies the transactions using the public key of the users and a set of pre-defined cryptographic methods; then, these transactions are collated into a block. All the transaction details inside a block are encrypted so that the transaction details are not made public. Then, this block is broadcasted over the network, and miners verify using an algorithmic validation method, i.e., the consensus mechanism. Miners may be rewarded based on the consensus mechanism used. Once the block transactions are validated, they are appended to the existing transaction ledger, and updates are sent across the distributed blockchain network (Houben and Snyers, 2018).

While the above is the generic working mechanism of a blockchain, it is better understood with a specific blockchain example (refer to Figure 3 in Appendix). In a Bitcoin blockchain network, when Alice wants to buy a product from Bob using Bitcoin, she uses her private key and signs a message with the number of bitcoins and Bob’s address requesting a transaction. The Bitcoin network verifies the transaction and bundles it into a block with other verified transactions. Then, the block is broadcasted to all the mining nodes in the Bitcoin network. The miners then validate Alice’s transactions using a validation algorithm, i.e., a consensus mechanism. The first miner to validate the whole block receives a portion of the Bitcoin as a reward, and the transaction is completed after sending the Bitcoin to Bob’s address. The new block is added to the blockchain and updated throughout the network. The block is immutable, meaning it cannot be altered or modified once it is added to the blockchain. A blockchain is also known as a Chain of Blocks because each block is connected to its predecessor by retaining the hash information of the preceding block. The hash is derived from the block's report, and any changes inside the block result in a new hash.

Therefore, even minute changes to a block are sufficient to break the chain since the following blocks cannot detect the altered block due to a hash discrepancy. In such a scenario, the longest chain is picked as the best chain, and altered blockchains are finally eliminated (Imteaj, Amini and Pardalos, 2021).

2.2.2 Blockchain Consensus Mechanisms

Any participating network in a blockchain can propose the addition of new information to the blockchain if it's a permissionless blockchain. However, this feature of blockchain could lead to the problem of "*double-spending*", i.e., the same asset or payment instrument can be transferred more than once without a central authority controlling the validations. To validate whether a transaction is legitimate, the blockchain network uses consensus mechanisms (a set of predefined cryptographic validation methods). It ensures the correct sequencing of the overall network transactions, preventing double-spending (Houben and Snyers, 2018). Consensus mechanisms are the key to maintaining the overall blockchain infrastructure as they help to keep the core principle of removing third parties from any form of transactions.

Different blockchains have different consensus mechanisms; the commonly used consensus mechanisms are the **Proof of Work (PoW)** mechanism and the **Proof of Stake (PoS)** mechanism. Other consensus mechanisms such as proof of history, proof of service and proof of elapsed time have been introduced to overcome the flaws of PoW and PoS, mainly related to energy efficiency and sustainability. Various new blockchains use these new consensus mechanisms. For example, Solana's new and emerging blockchain uses proof of history as its consensus mechanism.

- **Proof of Work (PoW)**

In the PoW consensus mechanism, each node on the blockchain needs to show that it has performed some work to add a block to the blockchain. Bitcoin network employs this consensus mechanism where a node must solve a mathematical problem of hashing to find a hash value that should be less than the difficulty level. Finding a hash value is called mining (Baliga, 2020). The Bitcoin protocol dynamically sets the difficulty level, which guarantees block production. The node finding the winning hash is rewarded with a digital form of value, a new coin in the case of bitcoin. Due to its distributed nature, multiple nodes compete to find the winning hash value, and more than one node can find the winning hash. In this case, each winning node adds the block to its blockchain and broadcasts it to the network, creating temporary forks of the blockchain. However, as more blocks are added to these forks, the protocol ensures that the longest chain with maximum PoW gets included in the main blockchain, and others get discarded to create consistency (Baliga, 2020).

Finding hash value becomes computation-heavy as the input becomes more extensive, which consumes high electricity, resulting in higher mining costs (Houben and Snyers, 2018). Other cryptocurrencies such as Litecoin and Bitcoin Cash also use the PoW consensus mechanism.

- **Proof of Stake (PoS)**
  The PoW consensus mechanism is often criticised for its high electricity consumption; in theory, the PoS consensus algorithms are designed to overcome such disadvantages (Baliga, 2020). In the PoS consensus mechanism, a transaction validator has to prove the ownership of certain assets (a certain amount of coins in the case of cryptocurrencies) to participate in the transaction validation process, and the whole process is referred to as “forging”(Houben and Snyers, 2018). For example, cryptocurrencies such as Cardano use the PoS consensus mechanism where a transaction validator will have to prove their stake of all coins to be allowed to validate a transaction. The higher the stake, the higher the chances of getting allowed to validate a transaction.

2.2.3 Cryptocurrencies – Understanding The Popular Use Case of Blockchain

It isn’t easy to establish a definition of cryptocurrency. Like blockchain, cryptocurrencies have become a "buzzword" for various technological advancements using encryption (Houben and Snyers, 2018). Cryptography is the method for securing information by changing it (i.e., encrypting it) into an unreadable format that can only be understood (or decrypted) by a person possessing a secret key. Using an inventive system of public and private digital keys generated using the cryptographic method, the cryptocurrencies such as Bitcoin maintain their security and standards.

The whole ecosystem of cryptocurrencies exists at the intersection of technological innovation and financial growth. Then, we may describe a cryptocurrency as a digital asset based on encryption technology that emerges as a decentralised means of trade and transfer, without the need for an intermediary, and protects the privacy of its users (Chohan, 2017). In other words, a cryptocurrency is a system that fulfils these criteria: (I) it is not dependent on a centralised authority; (II) the ownership of minted cryptocurrency is controlled; (III) the method by which new cryptocurrency units may be generated and owned is fully defined; (IV) the proof of ownership can only be established cryptographically; (V) the transactions involving the transfer of cryptocurrency ownership are only permitted when a third party validates the existing owner's ownership; and (VI) in the event of two simultaneous transactions involving the same cryptocurrency units, the system will only authorise one of them (Gonzálvez-Gallego and Pérez-Cárceles, 2021). Since the birth of Bitcoin in 2009, the issue of cryptocurrencies has been examined by various policymakers, each of whom has uniquely approached the topic.

- **Bank of England (BoE)**

  The BoE classifies cryptocurrencies as crypto assets generally held as investments by the general public with an expectation of gaining value over time (Bank of England, 2020). It further defines cryptocurrencies as a type of electronic cash which use a peer-to-peer system and are riskier as the central bank or the government does not manage them.

- **European Central Bank (ECB)**

  The ECB treats cryptocurrencies as a subset of *virtual currencies. It* describes virtual currencies as digital representations of value that a central bank, credit institution does not issue, or e-money institution may be used as a replacement to currency in certain situations. Additionally, it highlighted those cryptocurrencies, such as Bitcoin, form a decentralised bilateral (i.e., bilateral) virtual money (Houben and Snyers, 2018).

- **International Monetary Fund (IMF)**

  The IMF also classifies cryptocurrencies as a subclass of virtual currencies. It describes them as digital representations of value created by private developers and denominated in their unit of account. According to the IMF, the concept of virtual currencies encompasses a broader range of 'currencies,' including simple IOUs (the phonetic abbreviation "I owe you" refers to a document that admits the existence of a debt) issued by issuers (such as the Internet or mobile coupons and airline miles), virtual currencies backed by assets such as gold, and cryptocurrencies such as Bitcoin (He *et al.*, 2016).

- **World Bank**

  The World Bank classifies cryptocurrencies as a subset of digital currencies which relies on cryptographic techniques to achieve consensus and defines digital currencies as the digital representations of value denominated in their unit of account, as opposed to e-money, which is only a digital payment mechanism representing and denominated in fiat currency (Natarajan, Krause and Gradstein, 2017).

- **Financial Action Task Force (FATF)**

  Taking a similar approach to other policymakers, the FATF defines cryptocurrencies as decentralised virtual currencies distributed, open-source[6], math-based peer-to-peer virtual currencies with no central administration, surveillance, or control (FATF, 2014).

From the above definitions of cryptocurrencies, a primary conclusion can be derived that there is no universally agreed definition for the term in the regulatory space apart from the standard warning issued by the regulatory bodies (mainly central banks in different states), citing the pitfall of investing in the unregulated cryptocurrency market.

[6] **Open-Source** refers to the source code of a computer program that is publicly accessible for modification and redistribution without any cost.

Most policymakers approach cryptocurrencies as a subset or a digital or virtual currency. Cryptocurrencies and blockchain are popular subjects and have become a topic of discussion among regulators. Although they are commonly mentioned together and related, they are not interchangeable. Blockchain is a distributed ledger that underpins the crypto market. It's the technology underpinning cryptocurrencies. Its scope and applicability are not restricted. As mentioned previously, blockchain may be used in many different fields. These applications differ from cryptocurrencies, which use blockchain technology. Regulators need not fear impeding innovation when addressing cryptocurrency.

2.2.4 Understanding Flow of Cryptocurrencies and Key Players Involved

This research presented how the overall blockchain technology works in an earlier chapter (refer to chapter 2.2.1). The working mechanism of cryptocurrencies is not so different as cryptocurrencies are an application of blockchain technologies. However, the cryptocurrency market is a brand-new playing ground where various parties are involved in making the ecosystem work. In this section, the key players involved in the cryptocurrency market are briefly discussed, which helps to shed some light on the working of the market.

Unlike traditional banknotes or coins, cryptocurrencies do not exist in physical form and cannot be transferred physically. The flow of cryptocurrency is entirely digital and involves mainly – the cryptocurrency user, digital wallet, cryptocurrency exchange and cryptocurrency coin creator.

2.2.4.1 Cryptocurrency Users

The first and most important participant in the cryptocurrency user. A cryptocurrency user is a natural person or legal entity who acquires coins to buy real or virtual goods or services, conduct P2P payments, or keep them for investment reasons (i.e., with a speculative motive to gain profit) (Houben and Snyers, 2018**)**. To initiate a transaction, a cryptocurrency user needs to acquire cryptocurrency, which can be done in multiple ways:

- Buy coins/tokens (coins and tokens are often used to refer to a unit of cryptocurrency based on their type) on exchanges or trading platforms by exchanging fiat money.
- Use P2P exchange to buy coins/tokens from another cryptocurrency user.
- Create a new coin/token or become a miner to get rewarded with a coin/token for validating transactions.
- Get coins/tokens from sale by the creator or as a gift or donation.

2.2.4.2 Cryptocurrency Wallet

Cryptocurrency wallets are a vital part of the whole crypto ecosystem as they are used for storing coins/tokens securely. There are standalone wallets which users can download the software and keep on their system. While different wallet providers and cryptocurrency exchanges also provide digital wallets or e-wallets for holding, storing, and transacting. This wallet keeps users' cryptographic keys and provides the user's cryptocurrency transaction history in a readable format.

Wallets can be further classified into different types – hot wallet (software wallet, mobile or desktop wallet, cold wallet (hardware wallet, paper wallet), custodial and non-custodial wallet **(**Cryptopedia, 2022**)**.

- **Hot Wallet** – These wallets are connected to the internet and are available to users for immediate transactions. The wallet provided by exchanges and trading platforms is a hot wallet as it is convenient for quick transactions.
- **Cold Wallet** – These wallets are mostly disconnected from the internet and used for safe cryptocurrency storage, preventing unauthorised access. Different hardware wallets, such as the Ledger, which works using the USB port on the computer, are cold wallets. Paper wallets are also cold wallets as the private keys are printed on paper and stored in a safe location.
- **Custodial and Non-Custodial Wallets** – A custodial wallet is a digital wallet in which key storage and wallet maintenance are delegated to a third party, usually the cryptocurrency exchanges. A non-custodial wallet is where the user is responsible for key storage and wallet maintenance. Hot wallets are mostly custodial wallets, and cold wallets are non-custodial. While non-custodial wallets

are a safer way of storage, users prefer custodial wallets as the responsibilities for management are delegated to the third party (Cryptopedia, 2022).

2.2.4.3 Cryptocurrency Exchanges and Trading Platforms

The cryptocurrency exchanges and trading platforms are also vital in the cryptocurrency ecosystem as they provide cryptocurrency users services against a specific commission or exchange fee (Houben and Snyers, 2018). The cryptocurrency exchanges mainly offer services to buy/sell cryptocurrency against fiat currency, and the trading platforms provide advanced trading features like stock trading platforms. Coinbase, Binance, ByBit, etc., are some popular cryptocurrency exchanges.

The modern cryptocurrency exchanges also provide P2P payments, an NFT marketplace, and crypto savings services. While these cryptocurrencies are often referred to as CeFi (Centralised Finance) as they are operated by a central entity such as a private company, there is an increasing number of DeFi (Decentralised Finance) platforms enabling permissionless decentralised transactions (Iredale, 2020). The DeFi platforms, often referred to as DEXs, use smart contracts using blockchain and decentralised protocols to execute trades. Anyone with a crypto wallet can conduct a transaction on DEXs without going through any KYC/AML procedure. However, they are limited to crypto-to-crypto transactions and do not support direct fiat transactions like centralised exchanges.

2.2.5 Exploring the Crypto Market

The cryptocurrency market in 2022 has been brutal to its investors as significant cryptocurrencies such as Bitcoin lost half of their value. However, the market is still active, and as of July 2022, the whole cryptocurrency market cap has reached $1 trillion with the rising importance of different cryptocurrencies (CNN Business, 2022). At the same time, other innovations in the market, such as NFTs, have driven the market valuation further. More cryptocurrencies and crypto-related innovations pop up regularly; hence this research tries to segregate the crypto market for better understanding.

There are dozens of cryptocurrencies, and many more are created daily. There are subtle and not-so-subtle distinctions between them, even though they all depend on the same idea of a consensus-based, decentralised, and irreversible ledger to transfer value digitally between untrustworthy parties (Loo, 2022). In general, cryptocurrencies other than Bitcoin are referred to as "*Altcoins*" as they were invented as an alternative to Bitcoin. However, the cryptocurrencies market can be further segregated into four main categories based on their nature and use cases:

2.2.5.1 Payment Cryptocurrency

Major cryptocurrencies such as Bitcoin and Litecoin are considered payment cryptocurrencies. These cryptocurrencies are solely made to facilitate P2P digital cash transactions. In addition, these payment cryptocurrencies often have a finite supply of digital currency, which renders them inherently deflationary. As fewer of these digital coins can be mined, it is anticipated that the value of digital money will increase (Loo, 2022).

2.2.5.2 Utility Tokens

Utility Tokens are the second-most popular cryptocurrency. Tokens are blockchain-based cryptographic assets. The Ethereum network was the first to enable other crypto assets to piggyback on its blockchain. Vitalik Buterin, the inventor of Ethereum, envisioned his cryptocurrency as programmable money that could disintermediate existing financial and legal bodies by allowing intelligent contracts and decentralised applications to run on the blockchain. Utility tokens can be further categorised into service tokens, finance tokens and media tokens based on their applicability (Loo, 2022). For example, Binance has its cryptocurrency token, Binance Coin (BNB), which can be used to pay transaction fees and reward users.

2.2.5.3 Stablecoins

Considering the volatility of several digital assets, stablecoins are meant to serve as a store of value. This cryptocurrency maintains its value because, although being constructed on a blockchain, it can be traded for one or more fiat currencies. A fiat currency thus backs stablecoins, often the U.S. dollar or the Euro, but does not imply that they are subject to government regulation or oversight. Tether's (a privately owned company associated with BitFinex) USDT is a stablecoin and the third largest cryptocurrency by market capitalisation (Loo, 2022). Some stablecoins maintain their value using intelligent algorithms instead of fiat currency; however, with the collapse of TerraUSD, a high-profile stablecoin based on algorithmic stability to retain its value of $1, these types of stablecoins are questionable (Boom, 2022).

2.2.5.4 Central Bank Digital Currencies (CBDC)

Central banks in countries like China (Digital Yuan) issue their own Central Bank Digital Currency. Central banks issue CBDCs as tokens or electronic records tied to the local currency. Since central banks issue CBDC, they regulate it. CBDCs are still in the early phases of deployment in many nations' financial systems and monetary policies, although they may grow more popular over time. CBDCs use blockchain technology, like cryptocurrencies, to boost payment efficiency and reduce transaction costs. CBDCs are currently in the early phases of development for several central banks throughout the globe, but they utilise the same ideas and technology as Bitcoin. The currency's token form or electronic ownership records make it comparable to other cryptocurrencies. CBDC holders lose lost decentralisation, pseudonymity, and lack of censorship due to government monitoring and control. CBDCs keep a "paper trail" of government transactions, which may lead to taxes and other economic rents. CBDCs may keep their value or follow the pegged physical currency in a stable political and inflationary environment (Loo, 2022).

2.2.6 Lucrative Features of Cryptocurrencies That Attract Terrorists, Money Launderers and Other Criminals

What features would you want in a value-transfer tool if you were a terrorist, money launderer, or criminal who tried to utilise the Internet to move cash worldwide to assist your drug selling or human trafficking operations? Anonymity, Worldwide Reach, Transaction Speed and Low-Cost Transfer, No Central Authority for Verification and

Limited or No KYC/AML Policies, etc., are some features that might be lucrative for such activities (Keene, 2014).

- **Anonymity** – Any terrorist, money launderer or others carrying out illegal activities would always try to be anonymous to stay out of legal surveillance. Some cryptocurrency like Monero, Dash and Zcoin provides complete anonymity and other privacy features for performing transactions (Vermaak, 2021). While the idea behind these privacy coins was to overcome the pseudonymous nature of bitcoin and provide advanced privacy features to users suppressed by an authoritarian regime, the same concept of privacy is often misused by criminals or terrorist organisations.
- **Worldwide Reach of Cryptocurrencies –** Cryptocurrencies are borderless and can operate anywhere with internet access. This borderless concept of cryptocurrencies allows it to be accessible by anyone from anywhere, which is a good idea; however, for a criminal, this might be a lucrative feature as they can perform transactions without actually being in the location of their crime (Keene, 2014).
- **Crypto Transactions are Usually Fast and Cheap –** Generally, cryptocurrency transactions are faster. They have a low overhead cost as they don't have to wait for intermediary parties to settle the transaction. While there might be cases where a cryptocurrency service provider charges a premium for their services, most cryptocurrency transactions are fast and cheaper. This gives criminals higher chances of evading interception from law enforcement bodies and getting blocked from performing the transaction.
- **No Central Authority and Lack of KYC/AML Policies in Crypto World** – If a criminal uses the average bank for their transactions, they will immediately fall under the scrutiny of central bodies as banks are regulated and required to have strict KYC/AML policies. However, it is entirely different in the crypto space; the cryptocurrency exchanges such as Binance have been scrutinised for not having strict KYC/AML policies and being investigated for possible money laundering cases (Reuters, 2022). While the cryptocurrency exchanges must have KYC/AML policies, there are other

decentralised exchanges (DEXs) where anyone can carry out transactions without having any identity checks. Without these policies, it is more complex and consumes more time to trace the users' identities, which gives the criminals an advantage.

- **Availability of Cryptocurrency Mixers for Obfuscation–** Some cryptocurrency mixers like Tornado Cash have been popular among money launderers and terrorists to obfuscate their cryptocurrency transactions. The US law enforcement bodies identified the North Korean hacking group, Lazarus, for stealing almost $600 million from the NFT-based video game Axie Infinity but couldn't stop the laundering process due to the use of open-source mixers such as Tornado (Newmyer and B. Merrill, 2022).

2.2.7 Crypto Opportunities for Law Enforcement Agencies

As noted earlier, some properties of cryptocurrencies and their decentralised nature make them an excellent tool for criminals. However, every day, legitimate individuals deal with bitcoin and other cryptocurrencies, exchanging money and purchasing goods and services safely and anonymously. Thus, it is fair to explore features of cryptocurrencies that can be unattractive to criminals and even provide opportunities for law enforcement agencies to better monitor transactions on the blockchain to prevent crimes. Several features of cryptocurrencies and blockchain make them ideal for investigating financial crimes more effectively (Weinstein, 2015):

- There are no data retention issues because of blockchain, a persistent problem for law enforcement bodies as organisations fail to keep a record for extended periods.
- Blockchain transactions are immutable and recorded in chronological order. There is no issue of suspicious transactions being modified or erased.
- The "third party doctrine" issue does not exist in blockchain as the law enforcement bodies can easily access blockchain records without creating a subpoena or a search warrant.

- The cryptocurrencies are borderless, which was earlier discussed as an advantage for criminals. However, the exact borderless nature can be helpful for law enforcement bodies as they do not have to seek foreign government permission to obtain any records associated with a crime.

Some law enforcement agencies have been actively using and developing technology to monitor and track suspicious cryptocurrency transactions. Various private blockchain forensic companies also provide blockchain analysis services, such as "Chainalysis", which can index and analyse cryptocurrency transactions and addresses, providing important information about the cryptocurrency ecosystem, including user behaviour and trends. CipherTrace and Elliptic are other well-known companies that engage with law enforcement in cryptocurrency and blockchain intelligence. These companies engage with various enterprises and public sector entities to monitor and trace cryptocurrency transactions. They provide a fee-based service that aims to assist cryptocurrency wallet hosts and exchanges in avoiding the acceptance of illegally obtained funds by drafting the transactions of each cryptocurrency and indicating whether the funds originate from cryptocurrency mixers, Darknet marketplaces or digital wallets flagged as criminal or suspicious.

Colonial Pipeline, an oil pipeline corporation that distributes energy to the southern United States, was briefly forced to suspend operations on May 7, 2021, due to a ransomware assault. Within hours after the strike, Colonial paid DarkSide, the Russian cybercriminal gang responsible for the hack, 75 Bitcoin, or around $4.4 million at the time. Six days later, Colonial was able to restart operations, although, during that time, widespread gasoline shortages ensued from the suspension and subsequent panic purchasing. Following an FBI investigation, the Department of Justice revealed one month later that it had successfully seized $2.3 million worth of Bitcoin from Colonial's ransom payment. The blockchain analytics tools from Chainalysis assisted the FBI in tracing the monies after the incident **(Chainalysis, 2022a)**. This is one example of where cryptocurrencies have provided better opportunities for law enforcement bodies to conduct investigations.

2.2.8 Regulatory and Compliance Challenges Associated With Cryptocurrencies

The earlier section identified how cryptocurrencies could help law enforcement bodies by assisting in the investigation. However, there are some significant issues that regulatory bodies face as the cryptocurrency market spreads. Since the inception of Bitcoin, the regulatory space has been continuously evolving as the idea of a decentralised peer-to-peer payment network designed by Satoshi facilitates the user with anonymity and other features to bypass the central authorities, which were established to regulate the traditional financial instruments. This has led to some significant issues which jurisdiction faces, such as issues revolving around the legality of the cryptocurrencies market, taxation issues and policy issues regarding Anti-Money Laundering (AML)/ Counter-Terrorism Financing (CTF) (Turner, McCombie and Uhlmann, 2020). The cryptocurrency landscape is rapidly evolving, which adds complexity to the state and regulatory bodies to keep up with the rules and regulations.

2.2.8.1 Legality of Cryptocurrency Market and Ongoing Regulatory Practices

Any cryptocurrency transaction can occur without the involvement of the government, central banks, authorised payment networks or regulators. Without these legal bodies, cryptocurrency can be perceived as being illegal. However, this is not the case as cryptocurrency transaction are based on trust and observes different functions of money, thus leading to different opinions and hence various regulations (Sapovadia, 2015). Major economies around the globe are attempting to regulate the crypto space, and these regulations shed light on the necessity and developing trends in cryptocurrency regulation and legal status. This section highlights the legal status of cryptocurrencies and regulation attempts in some major economies worldwide.

- **United States of America (USA)**

  In the USA, cryptocurrencies are not considered legal tender, and the legal approaches differ at the state level. However, some progress has been made in the federal-level legislation. Because the cryptocurrency tokens are “other value that substitutes currency", the Financial Crimes Enforcement Network (FinCEN)[7] considers the cryptocurrency exchanges as money transmitters. Still, it does not consider the cryptocurrency to be legal tender. The Internal Revenue Service (IRS)[8] takes a similar approach where it does not consider the cryptocurrency a legal lender but a representation of value that can be exchanged and act as a store of value, guiding taxations (Mohsin, 2022).

Cryptocurrency exchanges are legal in many states, and regulation varies by state. In the United States, cryptocurrency exchanges are legal and governed by the Bank Secrecy Act (BSA)[9]. This implies that bitcoin exchange service providers must get a licence from FINCEN, execute an AML/CFT and Sanctions programme, keep adequate records, and make timely reports to the proper authorities. The US Securities and Exchange Commission (SEC)[10] views cryptocurrencies as securities and broadly applies securities laws to digital wallets that impact both exchanges and investors. In contrast, the Commodity Futures Trading Commission (CFTC)[11] has taken a more accommodating stance, recognising Bitcoin and Ethereum as 'commodities' and permitting other virtual and cryptocurrency futures to trade openly on exchanges it oversees (Lucking, Aravind and LLP, 2019). After the Financial Action Task Force (FATF) published their guidelines in June 2019, FinCEN clarified that it expects cryptocurrency exchanges to comply with record-

[7] **Financial Crimes Enforcement Network (FinCEN)** is a bureau within the United States Department of the Treasury responsible for gathering and analysing information regarding financial transactions to combat domestic and international money laundering, financing of terrorist organisations, and other financial crimes.

[8] **Internal Revenue Service (IRS)** is a federal organisation in the United States that oversees the collection of taxes and the enforcement of tax regulations.

[9] The **Bank Secrecy Act** of 1970, also known as the Currency and Foreign Transactions Reporting Act, is a United States legislation requiring financial institutions to help federal authorities identify and combat financial institutions to assist national authorities in identifying and combating money laundering.

[10] The **United States Securities and Exchange Commission (SEC)** was established as an independent agency of the federal government in the wake of the 1929 stock market crash to uphold the law against market manipulation.

[11] **The Commodity Futures Trading Commission (CFTC)** is a 1974-established independent agency of the United States government that oversees U.S. derivatives markets, including futures, swaps, and some types of options, and forbids fraudulent behaviour.

keeping requirements and the "Travel Rule" by disclosing information about the originators and beneficiaries of cryptocurrency transactions. The United States regulates virtual currency exchanges similarly to conventional AML/CFT gatekeepers, financial institutions, and money transmitters enforcing similar rules.

The US Treasury says crypto rules are needed to battle global and local crime. In 2018, Treasury Secretary Steve Mnuchin announced a new Financial Stability Oversight Council (FSOC) working group to explore the crowded cryptocurrency market. In December 2020, FinCEN proposed a new data collection requirement for those managing cryptocurrency exchanges, digital assets, DTLs, and crypto payment private digital wallets. This regulation, if implemented, would require cryptocurrency exchanges to submit Suspicious Activity Reports (SAR/CTR) for transactions over $10,000 and non-registered financial institutions or Money Services Businesses (MSB) wallet owners to identify themselves when sending $3,000 or more in a single or series of linked transactions. The Justice Department coordinates with the SEC, CFTC, and other agencies to guarantee proper consumer protection and simplified regulatory monitoring. The covid-19 problem has slowed the advancement in government attempts to regulate cryptocurrencies. Despite failures, US politicians want to regulate cryptocurrencies to avoid the possible destabilisation of the dominant US dollar (Mohsin, 2022).

- **United Kingdom (UK)**

  Post-Brexit, the UK's stance on cryptocurrency rules has developed. Despite confirming in 2020 that crypto assets are property, the UK has no cryptocurrency regulations, and cryptocurrencies are not considered legal tender. According to the Bank of England, cryptocurrencies are not considered 'money'. They do not represent a systemic danger to the stability of the banking environment since they lack conventional definitional qualities. Because the legal repercussions, rules, and status of crypto assets and currencies might vary based on their nature, kind, and application, the Financial Conduct Authority (FCA)[12] and the Bank of England have

[12] **The Financial Conduct Authority FCA** supervises UK financial services to protect customers, keep the industry stable, and promote healthy competition.

issued various cautions and recommendations regarding their use. These cautions pertain to the lack of legal and monetary protection, the position of cryptocurrencies as repositories of value, and the risks of speculative trading and volatility (Bank of England, 2020).

In 2018, the regulatory ambiguity around cryptocurrency spurred the British government to establish a specialised task group. Before launching a necessity for extra AML/CFT and taxes considerations, the task group identified three kinds of cryptocurrencies and three uses for crypto assets. The UK government's tax authority, Her Majesty's Revenue and Customs (HMRC), have issued a brief on the tax treatment of cryptocurrencies, stating that their "unique identity" means they cannot be compared to conventional investments or payments and that their "taxability" is dependent on the activities and parties involved. Cryptocurrency profits and losses are subject to capital gains tax (Mohsin, 2022).

Cryptocurrency exchanges operating in the UK need to be registered with FCA. The UK adopted 5AMLD[13] and 6AMLD [14] into domestic legislation before leaving the EU in 2020. All UK crypto assets businesses (including exchanges, advisors, investment managers, and professionals) must register with the Financial Conduct Authority by January 10, 2021. (FCA). These organisations must report AML/CFT and safeguard customers. FCA guideline emphasises that crypto-related businesses must also comply with the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (MLRs). The newest FATF standards were added to these laws in January 2020.

After 2020, it's expected that the UK's cryptocurrency legislation will generally stay consistent with the union, enacting directives akin to the EU's Markets in Crypto-Assets (MiCA[15]) and E-Money plans, along with different payment directives. The UK's crypto-regulatory environment may diverge from the EU in the future. HM

[13] **5AMLD** – the 5th Money Laundering Directive came into force on the 10th of January 2020 across all the EU nations to reinforce EU's AML/CFT and address emergent and ongoing compliance challenges.

[14] **6AMLD –** the 6th Money Laundering Directive was issued after 5AMLD and came into effect across the EU bloc on the 3rd of June 2021 with expanded AML regulations to accommodate new technologies.

[15] **Markets in Crypto-Assets (MiCA)** is a framework which is the most substantial piece of crypto regulation yet when it comes into effect.

Treasury recommendations provided through the UK Crypto Asset Task Force in January 2021 reiterated the UK's desire to put some cryptocurrencies under 'financial marketing regulation' and to continue considering a 'broader regulatory approach' to crypto assets (Mohsin, 2022).

- **China**

  China has a negative stance on cryptocurrencies as they have shadow-banned it apart from cryptocurrency not being a legal tender. The People's Bank of China (PBOC) prohibited Bitcoin transactions in 2013 and ICOs[16] and domestic cryptocurrency exchanges in 2017. PBOC classified ICO funding (which generates virtual currencies like Bitcoin or Ethereum via irregular token sales and circulation) as unlawful public financing without authorisation under Chinese law. China has a worldwide reputation for tight currency control rules on most foreign currencies, including cryptocurrencies. A 2020 modification to China's Civil Code gave state-approved cryptocurrency inheritance status (Mohsin, 2022).

  China bans local cryptocurrency exchanges, while overseas platforms and websites provide workarounds (most of which are not regulated by China). China had been a hub for crypto mining despite a near-total ban on crypto trading and associated services. However, in May 2021, the State Council's Financial Stability and Development Committee started cracking down on bitcoin mining to clamp down on illegal activities in the securities market, taking a sharp move against cryptocurrencies (Reuters, 2021). China's government also advised investors against speculative cryptocurrency trading and has forbidden financial institutions from offering services connected to cryptocurrency transactions. This seriously affected the overall mining industry as China’s share of global bitcoin mining capacity plummeted to near zero, causing a downfall in the overall cryptocurrency market. Despite Beijing's prohibition, a new report published in May 2022 suggests that several underground mines have opened nationwide. Cambridge Centre for Alternative Finance study offers that Chinese bitcoin mining has recovered as

[16] **ICOs** refers to Initial Coin Offering through which crypto company raise money just like public companies raising money through IPOs (Initial Public Offering).

miners in China refuse to give up despite the government's ban on the practice (Browne, 2022).

There is no indication of whether China will lift the ban or loosen the restrictions in the future, as recent development suggests that country is trying to be a leader in the crypto space, not by adopting the public cryptocurrency but rather by adopting blockchain technology and pushing out its cryptocurrency. Private companies such as Facebook announcing its currency, Diem (formerly Libra), prompted the Chinese central bank to accelerate its work to introduce its digital currency (Mohsin, 2022). China has been extensively pushing its digital yuan, a Central Bank Digital Currency (CBDC), launching a pilot version of a wallet app across multiple channels to expand its uses (Kharpal, 2022). In theory, the digital yuan can make transactions cheaper by eliminating the need for third-party settlement, which is the core feature of cryptocurrency. A centralised, government-owned ledger of people's transactions might become a Chinese Communist Party (CCP) financial monitoring weapon. The digital yuan would allow the government to reject people or enterprises from the financial system for infringement. Under the digital yuan system, it's unclear whether or how often the CCP will utilise this authority to impose a "financial death sentence" (Chainalysis, 2021).

- **India**

  Despite being a country with the second-highest number of cryptocurrency users, the Indian regulators have a negative stance on cryptocurrencies, with authorities trying to blanket ban cryptocurrencies. The Reserve Bank of India (RBI) decided to ban cryptocurrencies in April 2018. Still, this ban was overturned by the country's supreme court, citing no empirical evidence of harm caused by cryptocurrencies on the RBI-regulated entities (Peyton, 2020). During the previous session of Congress, the Indian government proposed the "Cryptocurrency and Regulation of Official Digital Currency Bill" to regulate cryptocurrencies. The law responds to worries that virtual currencies are reportedly exploited to deceive investors. There is currently no restriction or prohibition on the usage of cryptocurrencies in the nation (*Deccan Herald*, 2022).

Regulators introduced taxation policies in early 2022 to move towards profiting from cryptocurrencies allowing cryptocurrency exchanges to operate in the country. A 1% tax deducted at source (TDS) on crypto transactions in July 2022. This TDS obligation is the second key element of India's newly enacted crypto tax legislation, which implements a 30% capital gains tax on all crypto-related transactions after April 2022. The crypto community in India is outraged about the new regulations and has warned that they would have a devastating effect on crypto trading in India, particularly in light of the worldwide market decline (*The Economic Times*, 2022). The cryptocurrency exchanges in India are self-regulatory and follow KYC/AML compliance like that of regulated financial institutions.

The cryptocurrency exchanges welcomed the taxation move and taken as the government’s effort to embrace the rapidly growing technology despite criticism from crypto communities. However, in recent months the regulators have shown a different signal as the government expressed in the parliament that they want to ban cryptocurrencies, raising uncertainty in the world’s second-largest market for digital assets. The Finance Minister of India and RBI expressed their concerns about the destabilising effect of cryptocurrencies on the monetary stability of India (Singh and Singh, 2022). The disastrous experiences of various Crypto organisations, like Three Arrows crypto fund (3AC) in Singapore, and Voyager in the US, in the recent crypto market downturn, quickly support India's cautious stance on not embracing Cryptocurrency. According to experts, India accurately anticipated the nasty economic headwinds and may be spared many individuals from financial collapse (*The Economic Times*, 2022). This suggests that future regulation in India could be more aggressive towards discouraging cryptocurrency usage. The cryptocurrency being a legal tender in the country is not foreseeable in the current context.

- **El Salvador**

  El Salvador is the only country that uses Bitcoin as its official currency; the International Monetary Fund (IMF) warned against digital currencies—according to the IMF, adopting Bitcoin as legal cash generates several economic, financial, and legal challenges that require thorough examination. However, the government officials in El Salvador announced on June 9, 2021, that Bitcoin would be recognised as legal currency in the nation, and the law would be effective from September 7, 2021. Even though El Salvador has become the first nation in the world to recognise Bitcoin as a form of currency legally, it's too early to say what this means for the rest of the globe, but it's clear that this is the first domino to fall (Arslanian *et al.*, 2021).

Bitcoin became a legal tender in El Salvador through the "Bitcoin Law", which is the current law for cryptocurrency in the country, which constitutes the following noticeable articles (Alvarez, Argente and Van Patten, 2022):

- Article 1 - This legislation is intended to regulate bitcoin as unconstrained legal money with freeing power, limitless in any transaction and to any title that public or private natural or legal persons need carrying.
- Article 3: Bitcoin prices are permitted.
- Article 4: permits tax payments to be made in bitcoin.
- Article 7: stipulates that every economic agency shall accept bitcoin as payment when given by a customer.
- Article 8: Without prejudice to the operations of the private sector, the State must create alternatives enabling bitcoin transactions.

In conclusion, Chapter 2 discussed cryptocurrencies and the blockchain architecture in depth. The chapter started by discussing the problems with the centralised financial system, which led to the innovation of blockchain architecture and cryptocurrencies. Then, the technical terms, including consensus mechanism, were described, which are necessary to understand the overall working mechanism of the blockchain architecture and almost all the cryptocurrencies. From the perspective of different regulatory bodies worldwide, cryptocurrency definitions were given to show that there is no standard agreement on how to treat cryptocurrencies. Moving forward, to keep the reader updated about the market, current cryptocurrencies were classified into different types as the investigations in the following sections will come across these categories. Some significant features of cryptocurrencies were highlighted, which act as a supporting statement to the research question of whether cryptocurrencies are a threat or an opportunity for law enforcement and public administrative bodies. Chapter 2 ends with discussing regulatory practices in different countries; this helps the reader understand how the world economies are treating cryptocurrencies, which is a supporting statement for answering the future of cryptocurrencies and blockchain technologies.

3 Investigations and Empirical Analysis of Illicit Use Cases

The earlier sections gave a primer to cryptocurrency and blockchain technologies while explaining how they can be lucrative to criminals or used by law enforcement bodies and regulatory bodies to carry out investigations. Since the cryptocurrency ecosystem is so dynamic and complicated as it keeps rapidly evolving, it's impossible to say whether the presence and usage of cryptocurrencies constitute a direct danger or an investigative opportunity for law enforcement. While the legality is still in its infancy, the cryptocurrency industry has emerged as a worldwide force. Extortion, tax evasion, and other illegal acts like drug trafficking and terror funding have all been perpetrated using cryptocurrency. Is banning a better alternative than regulating? Are states and criminals better off or worse off because of the worldwide use of cryptocurrencies and emerging blockchain technologies? Under the existing confusing legal framework, how will law enforcement be able to keep control over and regulate cryptocurrency and blockchain technologies? Cryptocurrency's shifting environment necessitates caution in certain decisions, while others may be made with reasonable assurance. The importance of cryptocurrencies from the viewpoints of law enforcement and cyber criminals must be emphasised and presented.

This thesis section investigates the real-world use cases of cryptocurrencies and blockchain technologies by criminal and law enforcement or regulatory bodies.

3.1 How do Criminal Use Cryptocurrency? Understanding the Money Flow

Since the advent of Bitcoin, cryptocurrencies have been linked with instances of extortion, tax evasion, and other illegal activities, including the drug trade, ransom, and terror funding. In the earlier section, various features of cryptocurrencies might be lucrative to criminals (refer to Chapter 2.6). There have been several instances where these lucrative features proved helpful for criminals. In this section, various real-world crimes are investigated that were perpetrated using cryptocurrency and other blockchain technologies.

3.1.1 Illegal Darknet Market

The internet is one of the beautiful innovations of technology which is now an essential part of daily human life and the overall nation’s economy. While the internet is known to everyone and easily accessible, there is a network known as the "darknet," like the internet but only accessible via specific communication protocols that provide better anonymity than the internet. Darknet markets are like eBay, but they use anonymous communication. As a result, they are more difficult to get entry to than regular internet retailers. Trades on darknet marketplaces are more common since the names of both buyers and sellers are hiding. There are an estimated 30,000 domains on the darknet (Foley, Karlsen and Putniņš, 2019). Incognito Market, AlphaBay, Tor2Doo and DarkFox are an example of currently operating darknet markets and are actively involved in illegal activities (Darknet One, 2022).

For illegal products and services merchants, the rise of dark web marketplaces has provided them with new distribution channels that allow them to deal with consumers worldwide. As well as narcotics and banned substances, these markets offer explosives and firearms, ivory and wildlife trafficking, antiques and materials related to child sexual abuse in return for cryptocurrency. “Crime-as-a-Service” and other items like exploit kits for Distributed Denial of Service (DDoS)[17] or phishing tools may also be purchased on the dark web's markets (Silfversten *et al.*, 2020). The first darknet market, The Farmers Market, appeared on the Tor[18] network. It was later shut down after its founder was arrested for selling narcotics and laundering money over the internet. The Farmers Market was the first one, but it didn’t get much attention as the Silk Road, the first-ever darknet market to reach over 100,000 customers (Aiden, 2020). The Silk Road used Bitcoin for payment and the dark web, which would provide the operators with anonymity and conduct illegal business beyond the reach of law enforcement. Silk Road market had a payment escrow system where both buyer and vendor would have to deposit some bitcoin, and that bitcoin would be held in escrow until both parties

[17] A **Distributed Denial of Service (DDoS)** is a type of cyber-attack that interrupts the targeted server, service or network by flooding it or surrounding infrastructure with internet traffic (Cloudflare, 2022).

[18] **Tor** stands for The Onion Router, open-source software for enabling anonymous communication while hiding the user’s location and activity from the network monitors using internet traffic relays.

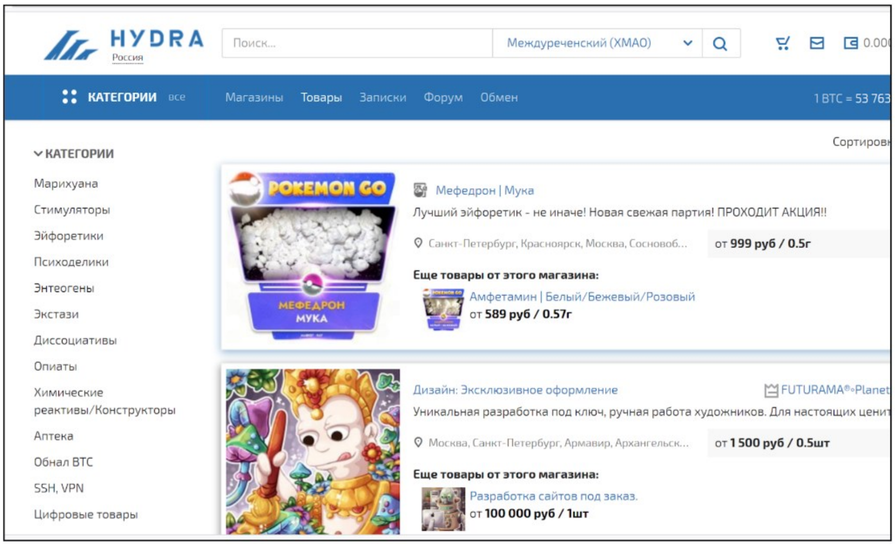
confirmed the order; the Silk Road would then take a commission for the order completion (refer to Figure 4 in Appendix).

Every year, there are thousands of darknet markets launched. However, this market does not have longevity as it can disappear as quickly as it can be set up. If you're interested in making money on the dark web, you don't have to spend much money to get started. The Empire market administrators earned an estimated $30 million from their exit fraud alone, not considering the money they made over their two-year operation. There was $12 million worth of user bitcoins on the Evolution market when it closed its doors. Every year, new darknet marketplaces spring up because of this. They eventually end up being seized by government authorities, hacked, an exit scam (a scam where the darknet market suspends its operation and takes away the cryptocurrency held in the escrow which was deposited by the buyer and vendor for the illegal transaction) or temporarily shut down (Aiden, 2020). The researchers at CipherTrace tracked and monitored more than 35 darknet markets, finding that more than half of the monitored darknet markets performed exit scams. Others were either seized by the government or shut down voluntarily (refer to Figure 5 in Appendix).

Case Study I: Hydra – Silk Road From Russia

In 2021, darknet marketplaces generated a new revenue record of $2.1 billion in bitcoin and other cryptocurrencies. About $300 million of total money came from fraud businesses, which handled the sale of stolen logins and other sensitive data. The remainder, more than $1.8 billion, was earned by marketplaces that cater specifically to illegal drugs (Chainalysis, 2022b) (refer to Figure. 6 in the Appendix). Among the many darknet markets, Hydra (shut down in early 2022) was one of the notable ones as it accounted for 80% of the total darknet revenue.

Hydra was launched in 2015 to cater to the Russian market and served countries like Russia, Ukraine, Belarus, Kazakhstan, Azerbaijan, Kyrgyzstan, and Moldova. It became dominant in the darknet market after the closure of RAMP (Russian Anonymous Marketplace) in 2017 and aggressively launched advertisements on YouTube while conducting DDoS attacks on its darknet competitors like SOLARIS and RuSilk (Barragan, 2021). Hydra mainly acted as a go-between for buyers and sellers while simultaneously concentrating primarily on selling illicit substances. Additionally, it had a segment for selling counterfeit bank notes, hacking services, counterfeit papers, and other illegal goods. A report published by The Project, a Russian investigative outlet, estimated that there were 2.5 million accounts registered on the site, and the number of users continued to expand each month (Barragan, 2021).



Мефедрон | Мука
Лучший эйфоретик - не иначе! Новая свежая партия! ПРОХОДИТ АКЦИЯ!!
Санкт-Петербург, Красноярск, Москва, Сосновоб... от 999 руб / 0.5г
Еще товары от этого магазина:
Амфетамин | Белый/Бежевый/Розовый
от 589 руб / 0.57г

Дизайн: Эксклюзивное оформление
Уникальная разработка под ключ, ручная работа художников. Для настоящих ценит
Москва, Санкт-Петербург, Армавир, Архангельск... от 1 500 руб / 0.5шт
Еще товары от этого магазина:
Разработка сайтов под заказ.
от 100 000 руб / 1шт

Figure 1. The Hydra marketplace's main web page. Synthetic stimulant Mephedrone is offered in the top advertising, while fraudulent papers are provided at the bottom (Source: GeminiAdvisors)

"If you chop off one head, two more will grow back in its place" this was Hydra's business concept associated with a mythical multi-headed snake when it hit the market. Customers may open and manage their drug stores using Hydra, which functions as a middleman for all completed transactions. Hydra's "professional grade" delivery and enhanced anonymity make it an attractive option for many online shoppers. The market has established direct suppliers in China to establish itself as a market recognised for its vast volumes of low-cost synthetic drugs (FlashPointIntel and Chainalysis, 2022). For most darknet marketplaces, tangible products are transported directly from the vendor to the customer through the mail. Hydra is a whole other animal. To sell illegal products, sellers produce "клад" or "treasures," concealed packages containing unlawful commodities. The boxes will be buried, magnetised, or otherwise placed in an unnoticeable location ("таник") to avoid detection. Instant orders and pre-orders are two sorts of purchasing. A customer may acquire an immediate order and instantly obtain the "клад" location or coordinates. After both parties agree on the purchase terms (mostly cryptocurrency) and the seller hides and identifies a place for the merchandise, the buyer receives a notification. They then go to that location to collect the goods. The customer, seller, and courier never meet face-to-face during business (Barragan, 2021). Multiple "treasures" may be found throughout Hydra's supply routes. "Master treasures" are massive stashes of narcotics created by suppliers, chemists, and growers in Russia. They are picked up by "warehousemen," who then distribute them to smaller couriers. These couriers create final “treasures”. On Hydra, the store operator plays a key role. The operator is responsible for coordinating the supply chain and resolving customer complaints. Workers of a store on Hydra know precisely what to do if one of their suppliers gets arrested (Barragan, 2021).

Hydra’s Money Trail

The Russia-based Hydra dominated the overall darknet market revenue throughout its existence. The Chainalysis research showed that over 85% of darknet market revenue in 2021 came from Hydra servers.

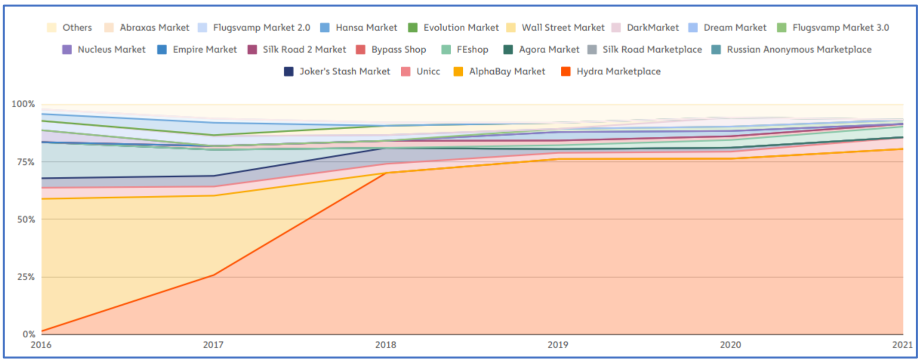


Figure 2. Darknet Markets by Total Revenue Share 2016 – 2021(Chainalysis, 2022b)

With the help of Hydra, Eastern Europe's unique crypto crime environment had one of the highest rates of cryptocurrency transaction volume related to criminal activity. It was the only illegal service provider becoming one of the region's top 10 cryptocurrency value providers.

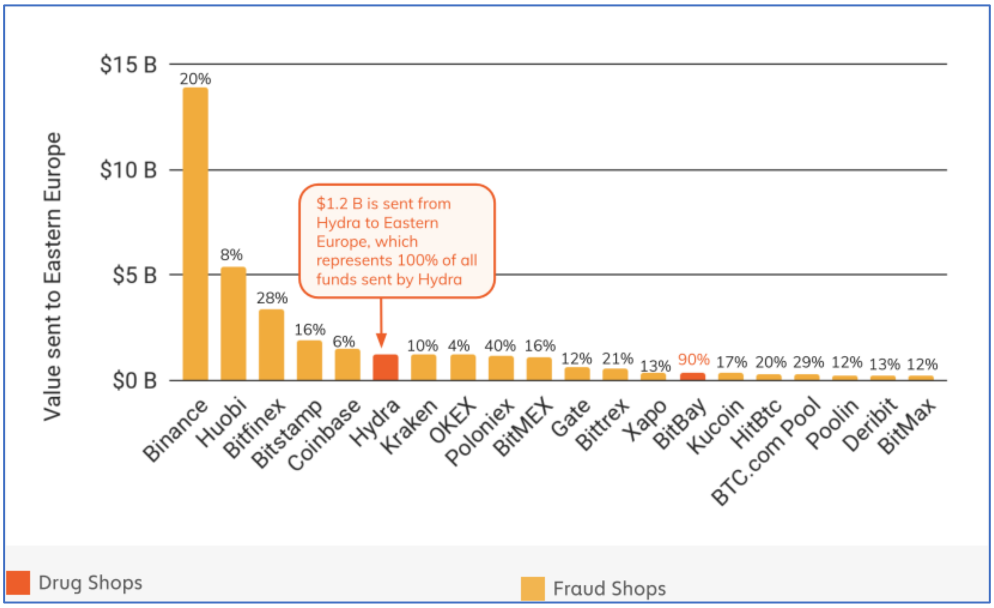


Figure 3. Top 20 Services By Value Sent to Eastern Europe (Chainalysis, 2022b)

Hydra was sending and receiving large sums in different cryptocurrency exchanges. The FlashPointIntel, with the help of Chainalysis, pointed out that Hydra transacted with diverse exchanges, among which several are classified as high-risk[19] and illicit cryptocurrency addresses[20] (FlashPointIntel and Chainalysis, 2022).

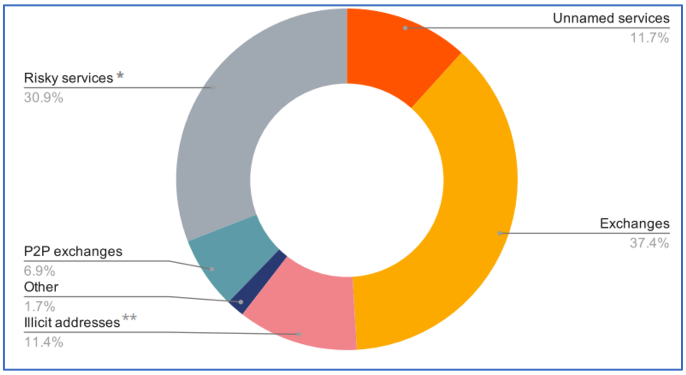


Figure 4. The volume of Transaction In Exchanges Linked With Hydra (FlashPointIntel and Chainalysis, 2022)

[19] **High-risk** exchanges include crypto exchanges, mixers, gambling platforms, and other payment services deemed risky by regulatory adherence and Security that Chainalysis observes during its research.

[20] **Illicit Crypto Addresses** are wallet address and accounts holding cryptocurrencies which are owned by cybercriminals or groups linked to illicit activities or transactions.

The actors behind the addresses on the above exchanges are anonymous and unknown. However, they are most likely to be wallet addresses of over-the-counter (OTC) brokers who help to obfuscate the cryptocurrency. These OTC brokers have several addresses at the cryptocurrency exchanges, which then are used for depositing crypto from illicit addresses linked to Hydra servers. This OTC broker then helps launder cryptocurrencies. The figure below shows an illustrative example where OTC brokers help Hydra sellers convert their cryptocurrencies into fiat money via their nested services.

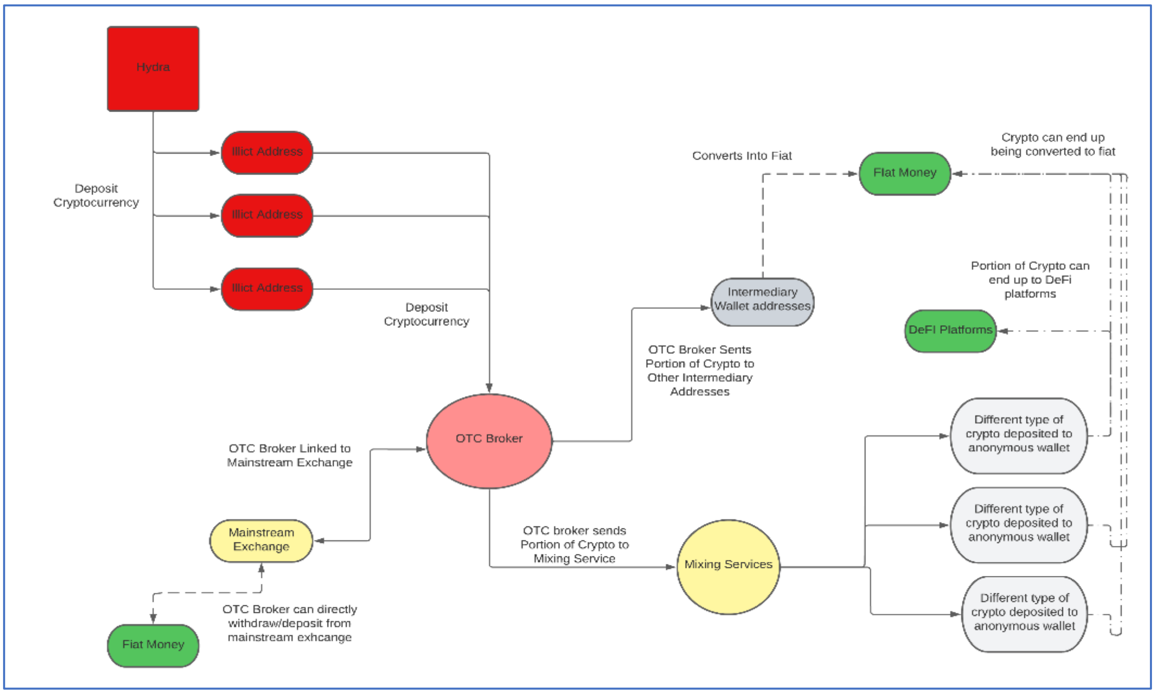

Hydra
Deposit Cryptocurrency
Illicit Address
Illicit Address
Illicit Address
Deposit Cryptocurrency
Converts Into Fiat
Fiat Money
Crypto can end up being converted to fiat
Portion of Crypto can end up to DeFi platforms
Intermediary Wallet addresses
DeFI Platforms
OTC Broker Sents Portion of Crypto to Other Intermediary Addresses
OTC Broker Linked to Mainstream Exchange
OTC Broker
Different type of crypto deposited to anonymous wallet
Mainstream Exchange
OTC broker sends Portion of Crypto to Mixing Service
Mixing Services
Different type of crypto deposited to anonymous wallet
Different type of crypto deposited to anonymous wallet
OTC Broker can directly withdraw/deposit from mainstream exhcange
Fiat Money

Figure 5. Illustrative Example of OTC Brokers Laundering Cryptocurrency for Hydra Sellers

After a few years of rapid growth, Hydra went through significant changes. It restricted buyers from transferring cryptocurrencies out of the marketplace while prohibiting sellers from withdrawing cryptocurrencies directly from the embedded wallet. These tight restrictions forced the sellers to convert their cryptocurrency proceeds into Russian roubles through specific regionally operated OTC brokers. Most monies left Hydra flow via in-region exchanges and accounts as the next destination in the continuous criminal financial chain, as confirmed by blockchain analysis of Hydra crypto transactions (FlashPointIntel and Chainalysis, 2022). The reasons for these changes were not clear.

However, experts believe it was related to increased security and compliance measures adopted in the cryptocurrency ecosystem, such as identification requirements.

Hydra dominated the Eastern Europe market and tried to enter the western darknet market in 2019 with the launch of an ICO raising $146 million for creating Eternos, a darknet marketplace serving the global community with unique, sophisticated operations such as delivery services using anonymous drug delivery agents that drops of the packages in hidden locations shared to the buyers swaying away from the traditional postal system and integrated encrypted messenger for better anonymity. However, there were no updates after the ICO, and the platform was never launched (Barragan, 2021).

In April 2022, it was reported that the Hydra darknet market was seized with the collaborative effort of US law enforcement and German authorities while taking $25 million worth of bitcoin from the marketplace. The Federal Criminal Police Office (BKA) and the Central Office for Combating Cybercrime (ZIT) announced that they closed the darknet marketplace after acquiring the server infrastructure in Germany (CipherTrace, 2022). In addition, the US Department of Justice identified 30-year-old Dmitry Olegovich Pavlov as Hydra's market operator and charged him with conspiracy to distribute narcotics and money laundering (Mangan, 2022).

Darknet Market and Decentralization

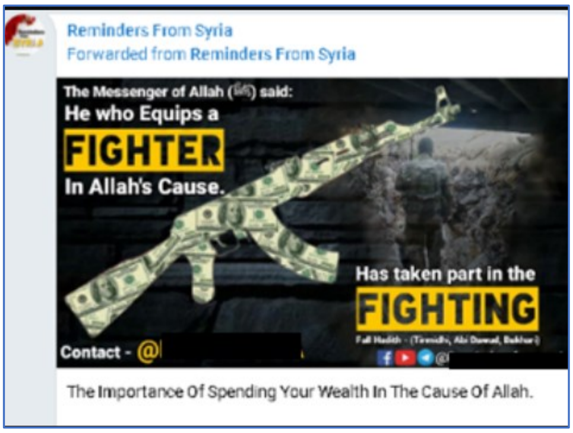
While the Hydra servers are dead, there is plenty of other darknet markets in operation, and the new decentralised model for the darknet market is rising. A Telegram-based app called "Televend" has been popular among darknet vendors where they can sell drugs and other illicit substances through automated chatbots with encrypted messages. (Redman, 2020). Buyers can access Televend's Telegram group, search through the drug vendor's directory and place their order. The app generates a Bitcoin address for payment and takes a commission from the sales. However, this app was taken down by Telegram after the news broke out, but these platforms are likely to grow as their decentralised nature makes them more resilient to attack and law enforcement.

3.1.2 Terrorism Funding Using Crypto

Regulators and counterterrorism organisations are increasingly concerned about the potential of cryptocurrency in terrorist funding. At least some terrorist groups have shown an interest in cryptocurrency and have used it to seek donations from sponsors or supporters. As a part of this new technique of transporting money, cryptocurrencies provide a speedier, more anonymous, and worldwide route that may be less bound by international and national Anti-Money laundering (AML) and Countering the Financing of Terrorism (CFT) regulations. However, new research has demonstrated that the use of cryptocurrencies for terrorist funding is episodic primarily and not as ubiquitous as previously thought as compared to more conventional methods (Silfversten *et al.*, 2020). But with, cryptocurrencies such as "Zcash" offer enhanced privacy using zero-knowledge proof, which suggests the cryptocurrencies are likely to be exploited by malicious actors in search of better anonymity. There are several cases where financial facilitators and infrastructures such as unlicensed money services businesses (MSBs) and hawala networks have utilised cryptocurrency to transport money for terrorist organisations. This research analyses some significant terrorism financing acts carried out using cryptocurrencies.

Case Study II: Al-Qaeda's Terrorism Financing Infrastructure Backed By Cryptocurrencies

In August 2020, the US Department of Justice (DOJ) announced the dismissals of various terrorism financing cyber campaigns launched by different terrorist groups, including al-Qassam Brigades, Hamas's military wing, al-Qaeda and the Islamic State of Iraq and the Levant (ISIS) (US Department of Justice, 2020). The multi-agency investigation conducted by significant investigation authorities such as the FBI and IRS led to the largest seizure of cryptocurrency assets associated with terrorism financing. Cyber tools were used to collect cryptocurrency contributions from around the globe in these three terror financing activities. Terrorist organisations worldwide have used similar cyber-based methods of financing their operations. Each organisation turned to cryptocurrencies and social media to get attention and earn money for their terrorist activities. Over 300 bitcoin accounts, four websites and four Facebook pages, all linked to the criminal business, were confiscated by U.S. officials under judicially authorised warrants (US Department of Justice, 2020). Multiple terrorist groups operated their campaigns over social media campaigns and then used multi-layered transactions to obfuscate their money trail. They collected the funds to a central hub, redistributing them to individual groups. “BitcoinTransfer”, a Syria-based cryptocurrency, acted as the central hub and facilitated financing to these terrorist groups (Chainalysis, 2020). While BitcoinTransfer claims to be a bitcoin exchange, it has been linked to multiple terrorism funding schemes and looks to be entirely under the control of terrorist organisations. More than $280,000 worth of Bitcoin has been transferred using BitcoinTransfer since the service went live in late December 2018, which is believed to be used for mostly terrorism financing (Katz, 2019).



Reminders From Syria
Forwarded from Reminders From Syria

The Importance Of Spending Your Wealth In The Cause Of Allah.

Figure 6. Telegram Message Showing Funding Campaign by Reminder for Syria, a charity that was seeking to finance terrorism (Source: Chainalysis)

While several terrorist organisations attempted to raise money for their cause, almost each used the same social media marketing strategy. These groups used social media and messaging sites, such as Telegram and Facebook, and claimed to be Syrian charities to request Bitcoin payments as a form of donation (Chainalysis, 2020). A screenshot in Figure 6 shows that despite the charities' charitable appearance, these organisations often published postings suggesting that funds would be used to purchase weapons for violent groups.

In the past, jihadists have used humanitarian initiatives to their advantage, and it is not the first time they have been involved in such activities. Still, this time it was different as the campaign was taking funds using cryptocurrency. Individuals and organisations have used humanitarian needs in Syria and Iraq to hide foreign combatants, collect cash for terrorist groups, and evade detection by the international security community. As part of the more significant issue of terrorist funding, multilateral organisations such as the Financial Action Task Force (FATF) recognise that charitable contributions under disguise are one component of the overall terrorism financing (Shanahan, 2018).

In May 2019, US government agents monitored several Telegram groups masquerading as charitable agents, raising money for terrorism. One of these groups, Tawheed & Jihad Media, had a single Bitcoin address published on its Telegram page promoting a funding campaign, "bullets and rockets for the mujahideen". In the DOJ lawsuit and the Chainalysis Reactor graph shown in Figure 7, the address is referred to as "Defendant Property AQ1." (Chainalysis, 2020) From the figure, it is seen that as the funds came in for donation groups such as The Merciful Hands, Al Sadaqah and others, administrators from these groups would eventually move the funds to a cryptocurrency wallet address linked to BitcoinTransfer noted as "Defendant Property AQ1." Following the investigations, the DOJ seized all funds associated with the al-Qaeda-controlled address. However, the central BitcoinTransfer exchange remained active as a service.

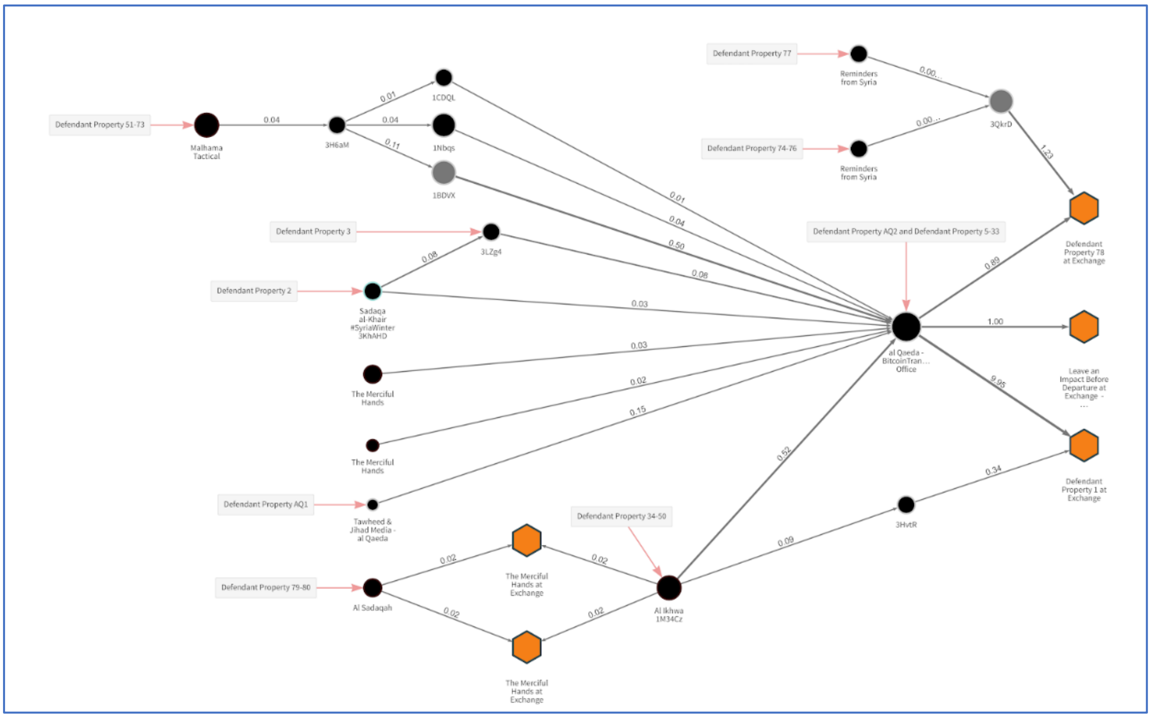


Figure 7. Graph Showing Funds Moving From Charity Organization to al-Qaeda BitcoinTransfer Account (Source: Chainalysis)

In late July 2021, the U.S. Office of Foreign Asset Control (OFAC) sanctioned Turkey-based Farrukh Furkatovitch for supporting Hay’et Tahrir al-Sham (HTS), a militant group actively engaged in the Syrian Civil War. This was another compelling case where terrorism financing was done through the Hydra darknet market and other channels using cryptocurrencies (U.S. Department of the Treasury, 2021). His crypto wallet address was tracked by Chainalysis, which revealed the funds coming from different channels, some from centralised and P2P exchanges where minimum or no KYC was needed. The graph below depicts Farrukh's on-chain activity (the trail of blockchain transactions) (Chainalysis, 2022b).

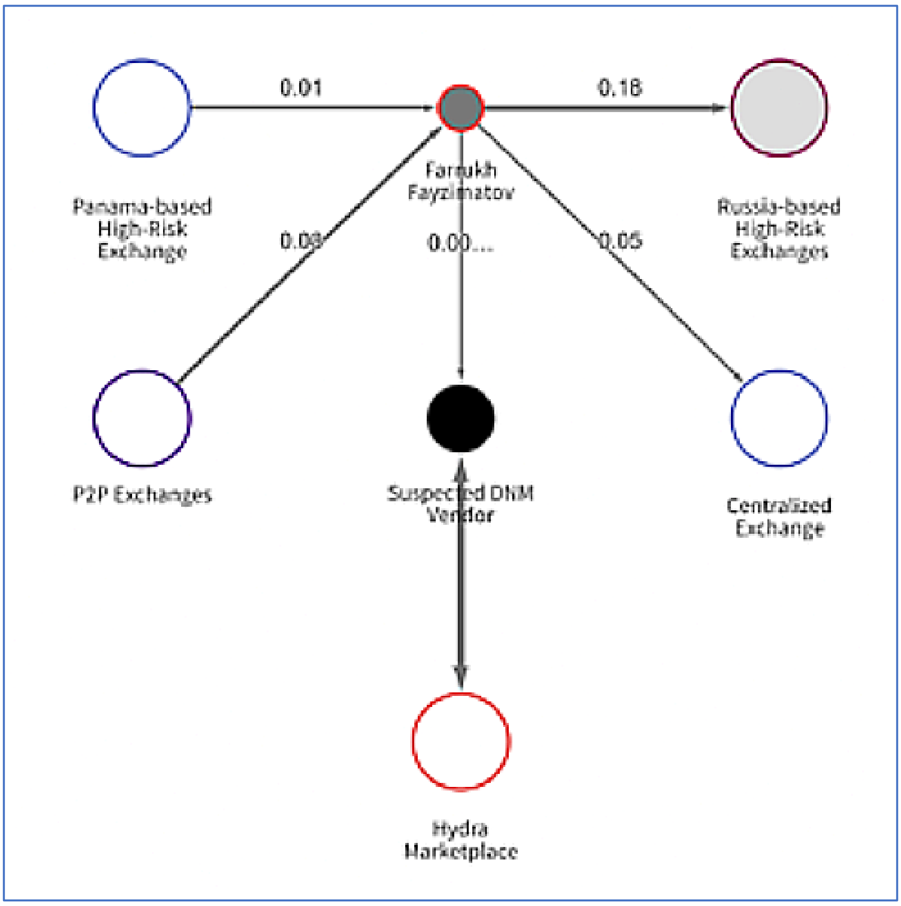


Figure 8. On-Chain Activity of Address Linked With Farrukh Furkatovitc (Source: Chainalysis)

For HTS, Farrukh used social media to disseminate propaganda, attract recruits, and raise funds for equipment purchases. Funding for the purchases came through

Fayzimatov's community fundraising activities ('Farrukh Furkatovitch Fayzimatov | Counter Extremism Project', 2022). Figure 8 depicts his wallet activities to illustrate his fundraising efforts. It was discovered that Fayzimatov had received payments directly through centralised and P2P exchanges that did not gather know-your-customer information and some Panama-based high-risk trades. This suggests that Fayzimatov received bitcoins from people who wanted to remain anonymous. On the right, we can see that Fayzimatov sent cash to high-risk Russian exchanges, a centralised exchange that did gather KYC information, and a tiny quantity to a suspicious seller at Hydra Marketplace, a Russian darknet market. Fayzimatov's on-chain activities halted when OFAC sanctioned him (Chainalysis, 2022b).

From case studies I and II, we can see that the darknet marketplace is often connected. In the case studies presented above, Hydra, the darknet market, acted as an indirect intermediary between Farrukh Furkatovitch and other terrorist financers. Farrukh's on-chain activity (refer to Figure 8) shows he was in contact with a darknet market vendor on Hydra marketplace where he had sent some funds, and the suspected Darknet Market (DNM) vendor has a two-way link to Hydra marketplace, which implies that the DNM vendor was an active vendor on the market. At the same time, it is unclear whether Farrukh sent funds to the DNM vendor to launder them to terrorist groups or paid for the purchase of illegal substance as the DNM vendor is anonymous, and the funds sent to the DNM vendor is relatively low than the funds sent to Russia-based High-Risk exchanges.

3.1.3 Evading Sanctions Using Cryptocurrencies

Sanctions have been a powerful economic tool in the global political context. For example, the United States has more than 9,000 sanctions on countries like North Korea, Iran, and Venezuela for aiding terrorism, abusing human rights, or engaging in other illegal activities. A strong US dollar and its status as the world's reserve currency imply that the United States may shut out nations, organisations, or people from most of the global financial system at their leisure. As a result, attempts to develop new methods to avoid U.S. sanctions, such as employing digital currencies that do not flow through the regular banking system, have increased. The Biden Administration in October 2021 warned that digital currencies, alternative payment systems, and new techniques to hide cross-border transactions all have the potential to diminish the effectiveness of American sanctions after a Treasury analysis. Because of this, "malicious actors can keep and move money outside the conventional dollar-based financial system.” (Rappeport, 2021)

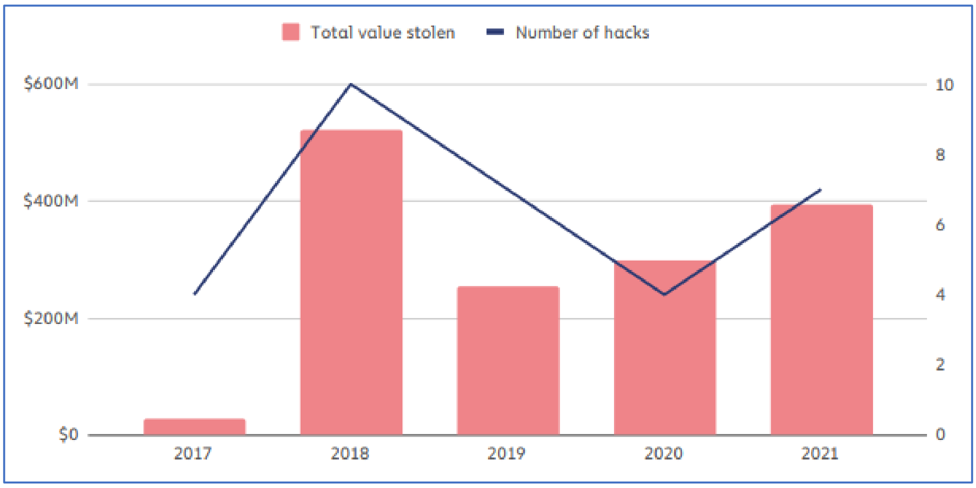
Whether cryptocurrencies can be used for evading sanctions is feasible or not came into the spotlight when the western countries decided to sanction Russia due to the war with Ukraine. The US regulatory body Financial Crimes Enforcement Network (FinCEN) notified different banking and financial institutions about possible questionable actions which Russia might use to avoid economic sanctions imposed by the western countries. According to the FinCEN, Russia's government and wealthy oligarchs may try to get around the sanctions by doing business with some unsanctioned Russian banks that have access to the international financial system and using cryptocurrencies such as Bitcoin convertible virtual currencies (CVCs). Ransomware operations linked to Russia have also been highlighted as a threat to financial institutions (Ramakrishnan, 2022). Russia-Ukraine war and sanctions might have brought attention to the topic; however, different countries such as North Korea and Iran have already been using cryptocurrencies to mitigate the effects of the sanctions imposed on them. A report published by UN Security Council in early 2022 found North Korea was developing nuclear weapons using the cryptocurrencies stolen over the year in different cyberattacks (Nichols, 2022).

Case Study III: North Korea Using Stolen Crypto For Funding Nuclear Programs

After North Korea's first nuclear test in 2006, the United Nations Security Council imposed sanctions on the country, which have steadily increased over the years. Despite the sanctions, the Democratic People’s Republic of Korea (DPRK) has gradually increased its nuclear capabilities over the year. According to UN watchdogs, cryptocurrency gained from cyberattacks has been an important revenue source for DPRK. North Korean cybercriminals continue to target institutions related to finance and cryptocurrencies (Nichols, 2022). At least seven assaults against cryptocurrency platforms were launched in 2021 by North Korean hackers, resulting in the theft of approximately $400 million in digital assets (refer to Figure 9). As a result of these assaults, DPRK controlled "hot" wallets belonging to investment enterprises and centralised exchanges, which were syphoned out through phishing, malware, and other social engineering techniques. They initiated a rigorous money laundering operation once North Korea had control of the monies (Chainalysis, 2022b). As a result of the DPRK's use of complicated tactics and procedures, several security experts have categorised DPRK cyber operators as advanced persistent threats (APTs). APT 38, or "Lazarus Group," is directed by the Reconnaissance General Bureau, the DPRK's principal intelligence organisation. Most of the cyber assaults were carried out by the Lazarus Group **(**Chainalysis, 2022b).

Initially known for its WannaCry [21]and Sony Pictures hacks, Lazarus Group has recently shifted its focus to bitcoin crim, where it has found tremendous success. Every year since 2018, the organisation has stolen and laundered more than $200 million in virtual currency. One attack on KuCoin and another on an undisclosed cryptocurrency exchange were the most lucrative, netting over $250 million (Chainalysis, 2022b). According to the UN Security Council, these intrusions produce income for North Korea's WMD and ballistic missile development.

The hacking activity of North Korea was at an all-time high in 2021 as the number of hacks related to North Korean hackers significantly increased from 2020 to 2021, and the data from Chainalysis suggests a rise in 40% of value extracted from the hacking activities.



[21] **WannaCry** ransomware attack targeted Microsoft Windows operating system and demanded ransom payments in Bitcoin for restoring encrypted data on the system.

Figure 9. Total Value Stolen and Total Number of Hacks Linked to North Korea

Interestingly, Bitcoin is currently worth less than a quarter of the cryptocurrency taken by the DPRK in terms of monetary value, per the report provided by Chainalysis. Bitcoin made up just 20% of the stolen assets in 2021, while ERC-20[22] tokens and altcoins accounted for the other 22%. A whopping 58% of the assets taken were in Ether[23], setting a record (Chainalysis, 2022b).

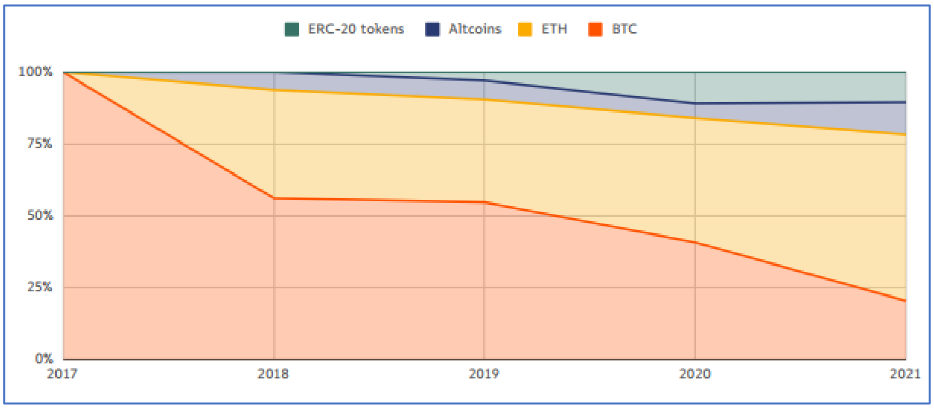


Figure 10. Type of Cryptocurrency Stolen by North Korean Hackers

After stealing a variety of cryptocurrencies, DPRK goes through complex cryptocurrency laundering operations, which includes various process:

- Using a decentralised exchange (DEX), the ERC-20 tokens are swapped for Ether
- Ether is then mixed using different mixers
- Mixed Ethers are then traded for Bitcoin again via DEXs
- Bitcoin mixers are used
- New wallet addresses are created for the consolidation of mixed bitcoin
- Bitcoin is then sent to a deposit address on a crypto-to-fiat exchange based in Asia, which are potential cash-out points for the stolen funds.

[22] **ERC-20 (Ethereum Request for Comments 20)** refers to a standard protocol for token creation within the Ethereum network using smart contracts.

[23] **Ether** is the native cryptocurrency of the Ethereum blockchain.

In August 2021, Liquid, a Japan-based cryptocurrency exchange, reported that its hot wallets were compromised, resulting in a loss of funds. About 67 different ERC-20 tokens, along with Ether and Bitcoin, were transferred from these hot wallets to addresses controlled by a part on behalf of North Korea. The hackers then followed the usual laundering routine; the ERC-20 tokens were swapped into Ether using decentralised exchanges such as SushiSwap and UniSwap; then, they mixed the Ether for Bitcoin and mixed Bitcoin using Tornado Cash, consolidating into new wallets addresses and finally deposited into fiat exchanges in Asia where it was likely to be swapped with fiat currency like China's Renminbi. Throughout the process, the hackers were able to launder $91 million (Elliptic, 2021).

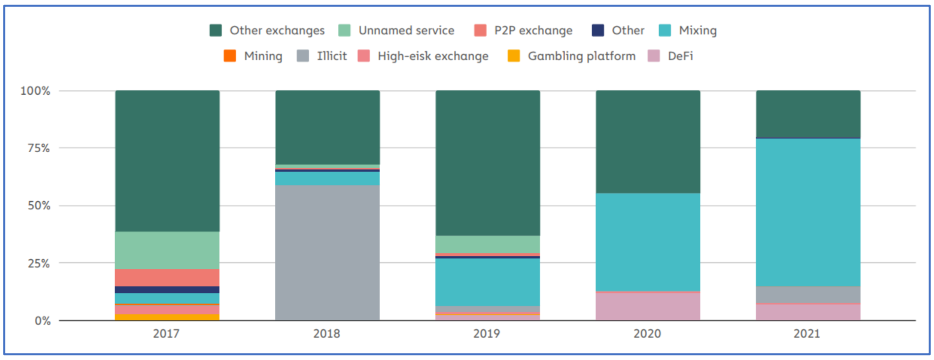


Figure 11. Laundering Channels Used By DPRK

From the data provided by Chainalysis, it is observed that mixing services are most favoured by the DPRK hacking groups as there is an increasing number of mixer usage from 2020 to 2021. The data suggests that more than 65% of stolen funds by DPRK's hacking group were laundered using mixers in 2021. This is likely because threat actors are cautious as regulation and compliance measures in centralised exchanges are increasing. Using multiple mixers can help to scramble cryptocurrencies into thousands of addresses obscuring the origin. The North Korean hackers choose DEXs to provide liquidity for different ERC-20 tokens. Swapping these tokens for Ether or Bitcoin makes the fund more liquid as these cryptocurrencies are widely accepted. Another primary reason for hackers using the DEXs would be that the decentralised exchanges do not collect any KYC information and never take any custody of users' funds, removing the risk of identity exposure and frozen assets.

Case Study IV: Russian Sanctions and Cryptocurrencies

Russia had been facing sanctions from the west since 2014, when it first tried to annex Crimea. A rapid and significant blow was dealt to Russia's economy in 2014 when the United States banned American citizens from doing business with Russian banks, oil and gas producers and other enterprises due to Russia's invasion of Crimea. According to economists, the sanctions imposed by Western countries cost Russia $50 billion a year sanctions imposed by Western countries cost Russia $50 billion year, according to economists. Cryptocurrency and other digital asset markets have grown exponentially since then—good news for Russia and bad news for the sanction enforcers (Flitter and Yaffe-Bellany, 2022). With the latest sanctions enforced on Russia after it attempted to invade Ukraine, there have been several ongoing debates about whether Russia could use cryptocurrencies to evade sanctions or mitigates its effect.

Russia is a leader in using cryptocurrencies, but the tale of its cryptocurrency usage is not favourable. Individuals and organisations headquartered in Russia, some of which have been sanctioned by the United States in recent years, account for a disproportionate percentage of activity in several types of cryptocurrency-related criminality. Russian hackers have a reputation for being among the best in the world. Cybersecurity experts attribute much of this to the country's high quality of computer science education and the lack of job opportunities for people with the necessary skills. In this context, it is no surprise that Russia is leading the charge in cybercrimes such as ransomware attacks. Nevertheless, it's alarming to see the amount of ransomware originating in Russia taking the lead (Chainalysis, 2022b).

More than $400 million worth of cryptocurrencies flowed to groups "very likely to be associated with Russia in some manner" in 2021 through ransomware assaults, which amounted to 74% of overall ransomware earnings. In general, ransomware strains are linked to Russian hackers based on three factors, including the Russian exchange of documents and announcements. Ransomware strains were partly identified because of their connections to Evil Corp., a Russian-based cybercriminal organisation, and cyber assaults that avoided former Soviet nations. More than a third of ransomware victims' payments flowed to Russian services, according to the Chainalysis report, which used blockchain research and web-traffic statistics (Chainalysis, 2022b).

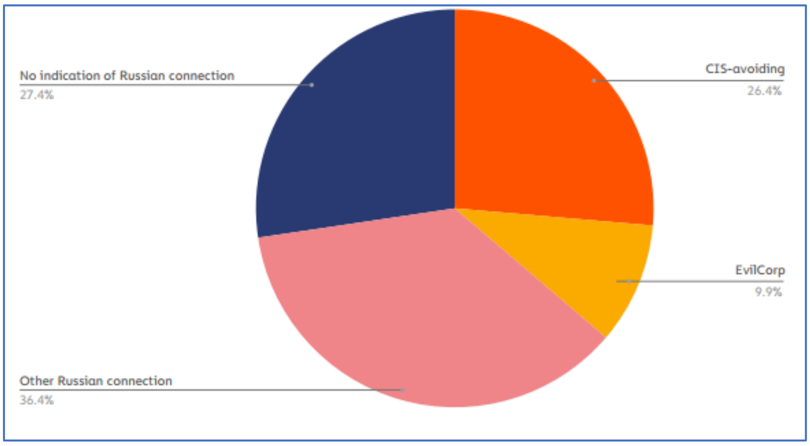


Figure 12. Ransomware Revenue Distribution Based on Russian Affiliate Strain (Source: Chainalysis)

Apart from Ransomware, Moscow City's cryptocurrency firms use many money-laundering practices. Some may be large enough to collect millions of dollars in illegal payments. Still, they only represent 10% or less of the total bitcoin they receive. Those incidents might be ascribed to a lack of awareness by the firm rather than a deliberate act of criminality. Most of Moscow City's bitcoin enterprises may be catering to a cybercriminal clientele, with illegal cash accounting for as much as 30 per cent of all cryptocurrency receipts (Chainalysis, 2022b).

Russia has a track record of laundering cryptocurrencies associated with illicit activities; the Russian government can likely use cryptocurrencies to evade sanctions. The sanction evasion by Russian can happen in different scenarios, as explained below:

- Taking a similar approach to North Korea, Russia can increase the number of cyberattacks and ransomware to generate cryptocurrencies which can be laundered, as mentioned earlier.
- The blockchain analytic firm Elliptic estimated that 4.5% of all Bitcoin mining occurred in Iran, enabling the government to evade trade embargoes and generate hundreds of millions of dollars in crypto assets that may be used to buy imports and dodge sanctions. This has ramifications for financial institutions involved in crypto asset transactions, which should ensure safeguards to prevent sanctions breaches (Robinson, 2021). Russia

could follow the same step and create Bitcoin mining farms, enabling them to evade trade embargoes generating revenue in cryptocurrencies.

- Russia could establish its own CBDC (“Digital Rubel”) and avoid trade directly with partners who agree to settle on Rubel without needing to convert it into US dollars. The Bank of Russia (BoR) mentioned that evading economic sanctions would be one reason to introduce a Rubel-backed digital currency (CBDC) (Baydakova, 2020).

Russia can likely evade sanctions using cryptocurrencies but based on the current market statistic, it is doubtful as the cryptocurrency market does not have enough liquidity to allow mass sanction evasion, and sanction evasion that takes place would be on a lower scale. The evasion of Russian sanctions through cryptocurrency would likely mirror traditional money laundering, in which small quantities of cryptocurrency are gradually transferred to cash-out providers instead of systematic, large conversions between cryptocurrency and cash (Chainalysis, 2022b).

3.1.4 Crypto Scams, Rug-Pull, and NFT Fraud

With the emergence of new crypto technologies, criminals have also found innovative ways to commit crimes using cryptocurrencies beyond cyberattacks and ransomware. NFTs and DeFi had been gaining momentum recently. Criminals now use newer platforms such as the NFT marketplace and DeFi platforms to commit crimes. This section aims to give readers ideas about modern criminal activities that criminals mostly use to exploit ordinary people. These crimes often involve a lower amount unless the crime or scam exhibitor has a large amount of money to build up liquidity in the market.

- **NFTs and Crime**

  Cryptocurrency's central story of 2021 revolved on non-fungible tokens. In contrast to typical cryptocurrencies, NFTs are blockchain-based digital objects that are supposed to be unique rather than interchangeable. Using blockchains like Ethereum and Solana, NFTs can store data about photographs, movies, music, and natural things. This data can be linked to memberships and numerous other emerging use cases. NFTs often grant the bearer ownership of the data or material the token is linked with and are widely traded on specialised markets. In 2021, NFT's popularity soared as the sales of NFTs skyrocketed to billion (Chainalysis, 2022b). One example the of NFT craze would be that more than $24.4 million was raised for the sale of the 107 non-fungible tokens (NFT) with cartoon monkey pictures (referred to as Bored Apes) (Howcroft, 2021).

As the NFT marketplace grabbed a lot of public attention, the criminals also found niche ways to commit crimes. The two most common crimes occurring in the NFT marketplace are:

1. **Wash Trading to Artificially Pumping Value**

   "Wash Trading" of NFTs refers to transactions in which the seller is on both sides of the deal to provide an inaccurate impression of an asset's worth and liquidity. In the past, cryptocurrency exchanges have worried about "wash trading," in which they try to inflate their trade volumes to make them look more substantial than they are. It's possible to make one's NFT look more valuable than it is by "selling" it to another wallet the original owner already owns. Theoretically, this would be simple with NFTs since many NFT trading platforms enable users to trade without identifying themselves by merely linking their wallets to the forum (Chainalysis, 2022b).

2. **Money Laundering Through Purchase of NFTs**

   Money laundering in the field of fine arts is widespread, and since the NFTs also fall under the same marketplace, they are susceptible to money laundering. Money launderers may use NFTs in the same manner that tangible art is used by money launderers (Owen and Chase, 2021).

   Theoretically, it should be relatively easy to launder money with NFTs. In the first place, NFTs don't need physical storage, and the leading NFT platforms don't have any KYC/AML standards. NFTs may be used for money laundering, just like any other method of value transfer in this case (Chipolina, 2021). However, the chances of money laundering through NFTs are rare as NFTs are on a public blockchain where all transactions are traceable. NFTs are difficult to obfuscate compared to average cryptocurrency.

- **Crypto Scams & Rug-Pulls in DeFi Platforms**
  Crypto scams and rug-pulls (a fraud where developers of cryptocurrency projects abandon the project unexpectedly after users invest funds in them) have been a severe issue in the DeFi platforms, where criminals have been taking cryptocurrencies from victims worldwide. And there are Ponzi schemes, such as the popular Finiko's billion-dollar Ponzi scam of December 2019, linked with Russian cybercriminals. The crypto scams and rug-pulls account for almost $7.5 billion stolen by scammers in 2021 (refer to Figure 13). Often, these stolen funds are used for illicit activities such as the drug trade (Chainalysis, 2022b).

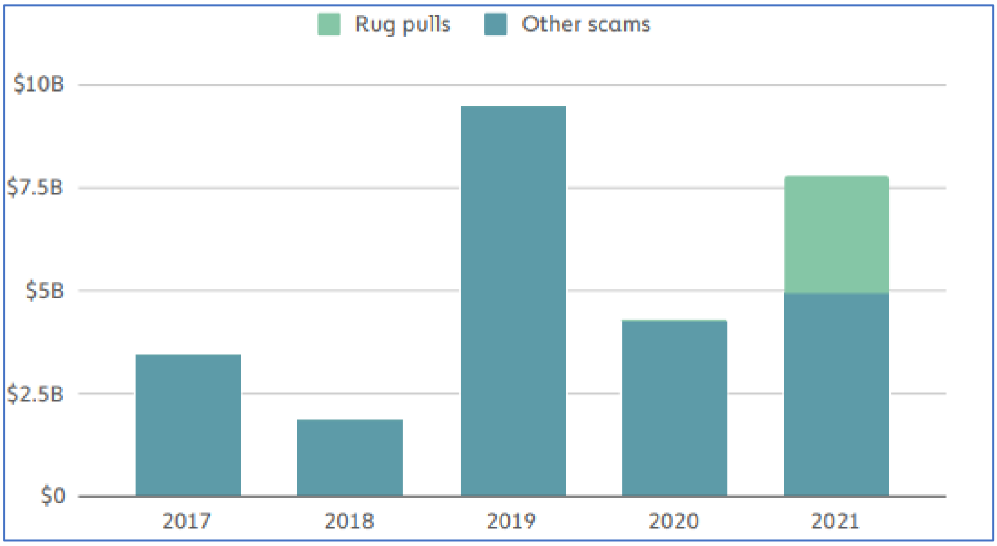


Figure 13. Total Value of Cryptocurrency Received by Scammers (Source: Chainalysis)

4 Exploring Legitimate Use Cases

Apart from legitimate users conducting daily transactions, money exchanges and purchases of goods or services using Bitcoin and other cryptocurrencies safely and anonymously, there are several other advantages of comprehensive blockchain technology which were discussed in Chapter 2.7, such as longer data retention with blockchain, no issues of "third party doctrine" and global reach. This section of the dissertation focuses on some case studies and use cases which will answer the research question of how blockchain and cryptocurrencies provide opportunities for enhancement of law enforcement agencies.

4.1 Blockchain Forensics Tools for Law Enforcement

Blockchain forensics uses science and technology to investigate and establish facts in criminal and civil law courts. In other words, blockchain forensics focuses mainly on the recovery and analysis of latent evidence left on the blockchain's digital ledger because of blockchain transaction activity. Blockchain forensics helps organisations and professionals to handle the financial crime and reputational risks connected with cryptocurrencies and other blockchain applications during client onboarding and ongoing maintenance. Blockchain forensics instils consumer confidence in the blockchain ecosystem and increases the transparency of blockchain transactions to dissuade their potential use in criminal activities (Phan, 2021).

Digital evidence plays an increasingly essential part in a forensic investigation, which is intended to connect people with illegal activity. Consequently, it is critical always to ensure evidence's integrity, traceability, and auditability. Data inaccessibility, attendance in numerous places, evidence transparency and traceability, and data analysis of enormous quantities are new difficulties for digital forensics (DF) in the context of cyber-physical systems (CPS). Cloud-based forensic analysis, evidence modelling, and assistance to the law enforcement community have all been the subject of significant academic initiatives in recent years. Blockchain forensic and cloud-based analytical tools can overcome the difficulties faced by digital forensics (Li, Qin and Min, 2019).

The law enforcement agencies are using and making tools that help them track and trace Bitcoin transactions that seem suspicious. Several private companies, like Chainalysis, offer blockchain analysis services. These companies can index and analyse Bitcoin transactions and addresses, giving them valuable information about the Bitcoin ecosystem, including how users act and generate user behaviour patterns. Chainalysis provides tools like Reactor, KYT and Kryptos to turn blockchain transactions into insights (Why Chainalysis, 2022). Then there are companies such as CipherTrace and CipherBlade, which works with law enforcement to gather intelligence about cryptocurrencies from several data sources. CipherTrace goes beyond providing insights by providing a pay-for-service that tries to help cryptocurrency wallet hosts and exchanges avoid accepting illegally obtained money by tracking the transactions of each Bitcoin and letting them know if the funds come from Bitcoin mixers, Darknet marketplaces, or digital wallets that have been flagged as criminal or suspicious.

Even though these services can be helpful, the analyses done by third-party actors don't always result in evidence that can be used in court. This is because most countries don't follow the rules for investigations or proof that the courts have set. However, these analyses have been helpful in various contexts and aided law enforcement bodies in their studies. In the case of the well-known Colonial Pipeline ransomware attack this year, the organisation was paid 75 Bitcoins to release the files. After spending the ransom, the FBI could get back 63.7 Bitcoins through blockchain forensics and other techniques and methods that are not public. The ransom payment was needed so that the FBI could track the money, look for specific transactions, and maybe find the IP addresses of the people who did it. Once the FBI had the IP address, they could use it to geolocate the host where the DarkSide affiliate ran the Bitcoin core. They could then use a seizure warrant to take the host and the private keys (Phan, 2021). The event showed how to look up partial blockchain addresses, the difficulties of seizing custodial vs noncustodial lectures, and techniques for clustering, among other things. The Colonial Pipeline case shows that, in the hands of skilled investigators, crime still doesn't pay. Using a pseudo-anonymous blockchain platform like Bitcoin and a combination of skills, tools, and techniques, it is still possible to find the criminals and get back any stolen money or ransom payments.

The expanding capacity of law enforcement to collect illicitly acquired bitcoin is a positive step in the battle against cryptocurrency-related criminality. In November 2021, for example, the IRS Criminal Investigations revealed that it had seized almost $3.5 billion worth of bitcoin in 2021 — entirely from non-tax investigations — representing 93% of total monies confiscated by the division at that time. Several examples of successful seizures by other agencies include $56 million seized by the Department of Justice during an investigation into a cryptocurrency scam, $2.3 million taken from the ransomware group responsible for the Colonial Pipeline attack, and an undisclosed amount seized by Israel's National Bureau for Counter Terror Financing in a case involving terrorism financing (Chainalysis, 2022b).

While blockchain forensics helps gather insights for investigations, blockchain technology can be used to maintain the integrity and authenticity of the evidence securing the chain of custody. Several frameworks have been proposed to use blockchain technology for a chain of custody to facilitate the security and transparency of digital evidence obtained in a criminal investigation.

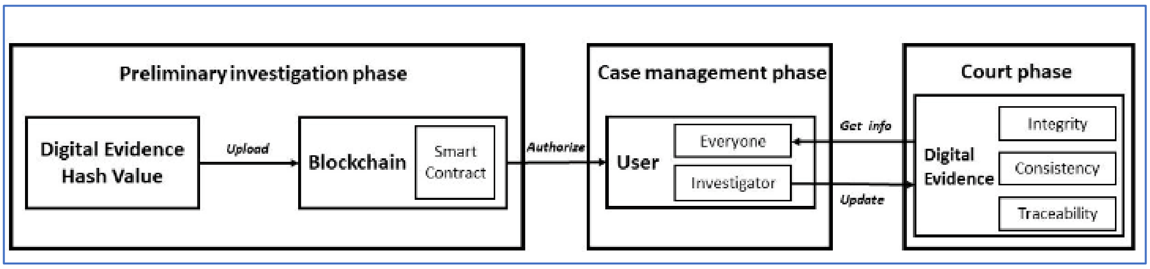


Figure 14. Blockchain of Custody Flowchart (Tsai, 2021)

Blockchain data can't be changed, making it easier to trust digital evidence and giving a good audit trail. One of the frameworks proposed shows how digital proof is handled from the crime scene to the courtroom in a clear and free of corruption. Figure 14 shows a general view of the proposed framework. The three main steps involved are the initial investigation phase, where the digital evidence's hash values are uploaded to a blockchain with a smart contract embedded to give authorisation to relevant parties for managing the case and going to court, where the integrity of evidence can be proved with consistency and traceability (Tsai, 2021).

4.2 Blockchain for E-government - Case Study of Estonia

E-government is the use of information and communication technology in government and public services for the benefit of the people. E-government effectively uses information and communication technology (ICT) to enhance citizens' government services and boost public engagement in policymaking and decision-making. Doing so will help improve government operations and increase the use of technology in government. By providing people with more precisely perceived service offerings via innovative practices, e-government aims to increase the social and economic aspects of the public with high performance and skills (Khanna et al., 2021).

The concept of "e-government" refers to the notion of e-government as the focal centre of practically all public sector innovation and a conceptual platform for experimenting with different information and communication technologies in government. In this regard, e-government reforms have always aimed to automate public service delivery models, whether implemented in developed or developing countries. As a result, e-government is also regarded as an electronic reflection of an authentic autonomous government, which is now enriched using a vast array of digital technologies for its primary operations: recording, processing, and delivering public information to its key stakeholders, namely citizens, businesses, and other government agencies (Kassen, 2022). Because of its immutability and decentralised nature, the blockchain has been used by various e-government leaders worldwide to enhance public administration services by developing a blockchain-based decentralised information management solution that can be automated, increasing government efficiency.

Estonia is one of the most active nations using blockchain technology in the public sector. It has long been a pioneer in information technology in the public sector, from ID cards to electronic voting to its current experimentation with e-residency. The Estonian parliament approved the Digital Signature Act in 2000, making digital signatures equally legally enforceable as handwritten ones. Historically, Estonians have had a high level of societal confidence in IT solutions, paired with a progressive attitude toward western ideas; the nation has enjoyed exceptional development since regaining independence. Today, information technology is fundamental to the running of the Estonian government. With the e-Residency initiative, the country intends to promote its IT skills and increase exports of IT infrastructure. Although blockchain and cryptocurrencies are pertinent in e-Residency, the project's empirical contribution is very lacking. Nevertheless, the X-Road, the central information technology system of the Estonian government, is one of the first broad blockchain platforms for public administration (Parol, 2018). X-Road, an anti-silo data management system developed by Estonians in 2001, allows public and commercial organisations to communicate data without fear of it being compromised securely. After discovering X-Road had been the target of cyberattacks, this work was squandered. Distributed ledger technology (DLT) resistant to hacker assaults became necessary. As a result, the country was the first to use blockchain technology for government governance in 2012 (Srivastava, 2021).

X-Road is the core of e-Estonia. According to the World Bank Development Report, X-Road helped Estonia become a digital society. It is a technological and organisational environment that allows information systems to safely exchange data over the Internet.

X-Road is based on an ecosystem that works with other systems. One example is a way for the police to check drivers' licences. A driver no longer has to carry their driver's licence with them because a police officer can use X-Road to check the database of the Road Administration to see if that person has a valid licence. The driver needs to show their identification. X-Road is also in place in Finland, Azerbaijan, Namibia, and the Faroe Islands. Through X-Road, data can be automatically shared between countries. Since 2017, Estonia and Finland have been able to exchange data automatically. Even sensitive information can be shared using X-Road. The Estonian government is based on the idea that the owner controls the data throughout the process, and the X-Road technology only allows for a secure exchange of data (Martinson, 2019).

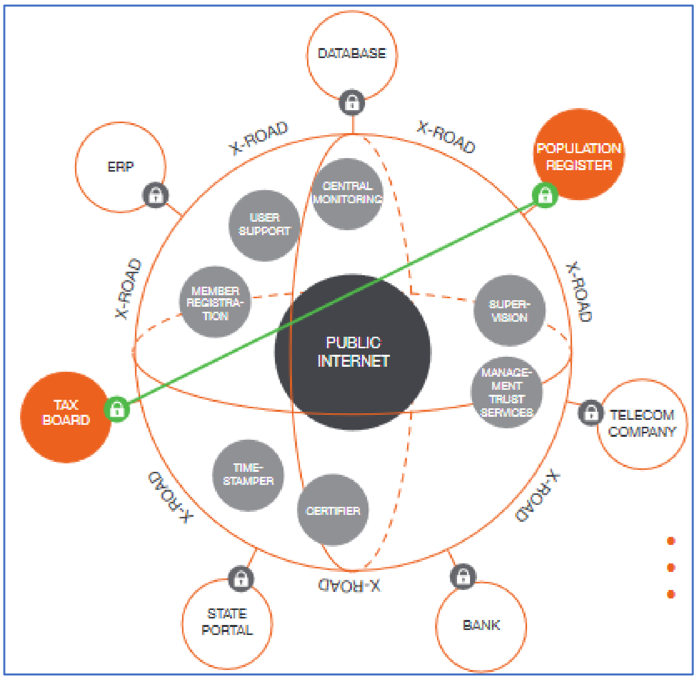


Figure 15. Estonia’s X-Road Interoperable Ecosystem(Martinson, 2019)

Different features of X-Road make it a secure, interoperable ecosystem built on blockchain infrastructure:

Decentralised architecture leads to no single point of failure

Independence of platform and architecture - the information systems of X-Road members, can run on any software platform.

Multilateralism - X-Road members can ask for access to any data services X-Road offers.

Availability and standardisation - International standards and protocols are used as much as possible when managing and developing X-Road.

Security - Exchanging data through X-Road does not change the data's integrity, availability, or privacy.

Estonia is one of the only nations using blockchain technology in the public sector. Blockchain allows their X-Road digital infrastructure, which the government heavily uses. The X-Road has proved helpful in enhancing the efficiency of the public sector so far. The Estonian instance has proved that blockchain technology first and foremost increases operational efficiency, but it might also be used to strengthen intragovernmental legitimacy and revolutionise public services. Future possible blockchain use cases, in addition to those currently supplied by the Estonian X-Road, might integrate blockchain technology with other technical developments. Considering the organisational need for machine learning and the possibilities of blockchain smart contracts, customised public services may be a win-win for both the government and the citizens. Smart contracts may be a secure method for automating organisational activities, while machine learning selects data most relevant to the citizen. In this manner, administrative and bureaucratic expenditures are reduced, and people obtain services suited to their needs. Open data government is another technique that may be used using blockchain technology. Available data government refers to people’s access to government data, whereas blockchain ensures the data's anonymity, security, and accessibility (Parol, 2018).

4.3 Blockchain for Greater Good

New technologies are altering people’s lives and their governance system. Governments throughout the globe are adopting digital advances to modernise their bureaucracies and reshape their relationships with people, therefore turning digital. Technology is altering how governments are expected to fulfil the increased quality, timeliness, and honesty demands of their citizenry. Digital people want better services and more government accountability, but most governments struggle to keep up and lack transparency.

Technology has become the greatest ally of transparency since it enables the use of insights derived from the exponential expansion of data. Digitally literate populations are far less tolerant of corruption and have more significant resources to expose it. There are expectations about blockchain's capacity to enhance the delivery of public services and boost government integrity due to blockchain’s core feature of maintaining security and integrity of information, as there is the issue of declining trust with current existing governance models. According to Mariana Dahan, creator of the World Identity Network (WIN), "Blockchain's decentralised nature and immutability of its records make it a formidable instrument in the battle against the greatest crimes, such as illegal trading, human trafficking and money laundering." (#Blockchain4Humanity: Use blockchain technology to help combat child trafficking in Moldova., 2018) Pilots and proofs of concept are increasing because of the proliferation of technology-driven start-ups across numerous sectors. This excitement fuels heated discussion, and a "bubble of expectations" swiftly forms (Santiso, 2018). To meet the expectations of digital literate populations and maintain integrity in the government, blockchain offers various value propositions - identity management, asset registrations, voting and supply chain tracing (White, Killmeyer and Chew, 2017).

4.3.1 Identity Management

The cornerstone for preventing money laundering is a universal and secure legal identity that allows one to verify the identities of persons and businesses. Bribery, fraud, and financial exclusion are fostered by the lack of an easy mechanism to prove one's identity. In addition to being a use case for blockchain, digital identity also serves as an enabler for the other blockchain assets we've examined. Whether you're dealing with a cryptocurrency or an automobile, you'll need a digital identity to participate in the transactions on a blockchain. Public sector players all around the globe acknowledge the enormity of this problem, where one-fifth of the world's population lacks a legally recognised identity (White, Killmeyer and Chew, 2017). With a secure, self-sovereign identity and an extensive range of asset classes to choose from, the blockchain may give a unique value proposition that might enable efficient transactions across a wide range of asset classes. Blockchain can be added to centralised identity management systems already in place. An estimated 1 billion people do not have a government-issued photo ID. Many of the world's 26 million refugees have significant challenges in establishing a legal identity, particularly if they have lost their original identification documents due to violence or natural catastrophes. Individuals organised by official identification systems confront significant impediments to full participation in economic and social institutions.

These difficulties may be addressed by using blockchain as the technological underpinning for "self-sovereign" identification systems, in which individuals keep and manage credentials rather than government agencies. Securing a portable identification record from unauthorised sources might be a possible advantage of SSI. The SSI, for example, may make it simpler for refugees to take their medical records, educational qualifications, and professional certifications from humanitarian organisations and utilise them when they leave the camps. It's important to note that these credentials largely depend on the recipient's acceptance. SSI may make it simpler for people to build a trusted relationship between themselves and these practical credentials. Still, political and legal change is needed before populations use these credentials instead of more basic identity verification (Crumpler, Flacks and Mandavilli, 2021).

For example, Aadhaar, a biometric identification system used in India, could use blockchain to store identity information securely and give the user more control over it. Some nations are actively using blockchain as a primary instrument for public administration. The Smart Dubai Office and the Dubai Future Foundation have developed an ambitious Dubai Blockchain Strategy. By placing all municipal transactions on the blockchain, this initiative hopes to improve government efficiency, reduce paper expenses, and eliminate red tape. Aisha Bin Bishr, director general of Smart Dubai, said, "By 2020, we want to create Dubai the world's first government to use blockchain technology." (Santiso, 2018)

4.3.2 Asset and Intellectual Property Registration

The second group of exciting applications relates to the registration of assets and the chain of custody, including property registrations and land titling. Building immutable title systems on the blockchain might aid in eradicating fraud and stimulate the registration of unregistered land and banks' lending money against the ground. Blockchain technology might reduce land administration hazards and participation costs in formal processes. Sweden is experimenting with a blockchain-based land registry to make the data of real estate transactions accessible to all parties concerned. Property disputes have been a long issue in Georgia, which is why the government has begun registering land titles using blockchain technology to increase transparency, safety and reliability of Public Registry services (Snip, 2017). In 2016, Georgia started collaborating with Bitfury, a software development firm, to test a blockchain-based land register system. The initiative envisioned a hybrid blockchain system in which documents recorded to the nation's primary digital database would be hashed and posted on the Bitcoin blockchain as a trustworthy reference. 3.5 million land titles have been issued on the blockchain as of 2021 (Crumpler, Flacks and Mandavilli, 2021).

4.3.3 Voting

Public voting is one of the essential and legitimacy-granting use cases where blockchain can secure voting transactions and prevent election fraud. With a blockchain-based voting system, citizens may cast ballots like they begin other secure transactions, confirm that their votes were cast, and even check election outcomes. Potential solutions are now attempting to combine secure digital identity management, anonymous vote casting, customised ballot procedures (such as a vote "token"), and ballot casting confirmation that can only be verified by the voter (White, Killmeyer and Chew, 2017).

Currently, the voting mechanism suffers from various issues - high costs related to the ballot and electronic voting machines. The increasing threat of cyberattacks compromising election results causes voting delays, inefficiencies, and a lack of transparency in the centralised selection process. A blockchain-based voting system would help save cost and provide superior security and integrity of the votes leading to greater transparency. Blockchain may prevent certain types of vote tampering if correctly deployed, as the voting systems are always dependent on other technology and software, leaving them susceptible to large-scale undetected exploitation and manipulation by corrupt authorities (Crumpler, Flacks and Mandavilli, 2021).

4.3.4 Supply Chain Tracing

Blockchain technology provides unique supply chain traceability prospects and should be investigated to enhance due diligence procedures and map supply chains. This endeavour shouldn't prioritise establishing tools and organisations for gathering and verifying labour conditions; a problem blockchain can't address. Over 24 million people are compelled to work, and tens of millions more work in harsh circumstances. Blockchain has facilitated more robust supply chain traceability and transparency as governments enforce human rights due diligence by end-user enterprises. Top corporations attempt to enhance respect for human rights in their supply chains (Crumpler, Flacks and Mandavilli, 2021).

Blockchain allows organisations to trace actual items as they travel through a supply chain and build a single, trustworthy record of their origin and manufacturing circumstances. Blockchain's transparency and distributed coordination might be helpful for supply chain tracking. Blockchain can store supply chain data such as harvest date and location to help organisations map their supply networks and detect high-risk items or components. Blockchain cannot verify data accuracy, making the system open to exploitation. Claims concerning working conditions are simple to falsify in a blockchain. Real-time traceability afforded by blockchain might be the most significant benefit for supply chain efforts, reducing the administrative load of due diligence procedures and enabling continuous supplier monitoring (Crumpler, Flacks and Mandavilli, 2021). Distributed blockchain systems may minimise the cost of deploying traceability programmes, enhance scalability, and build confidence among participating organisations. Traceability initiatives will still face significant obstacles, such as encouraging adoption throughout the supply chain, ensuring producers have access to the necessary technical infrastructure, and coordinating companies and government regulators on adopting common data reporting standards and interoperable platforms.

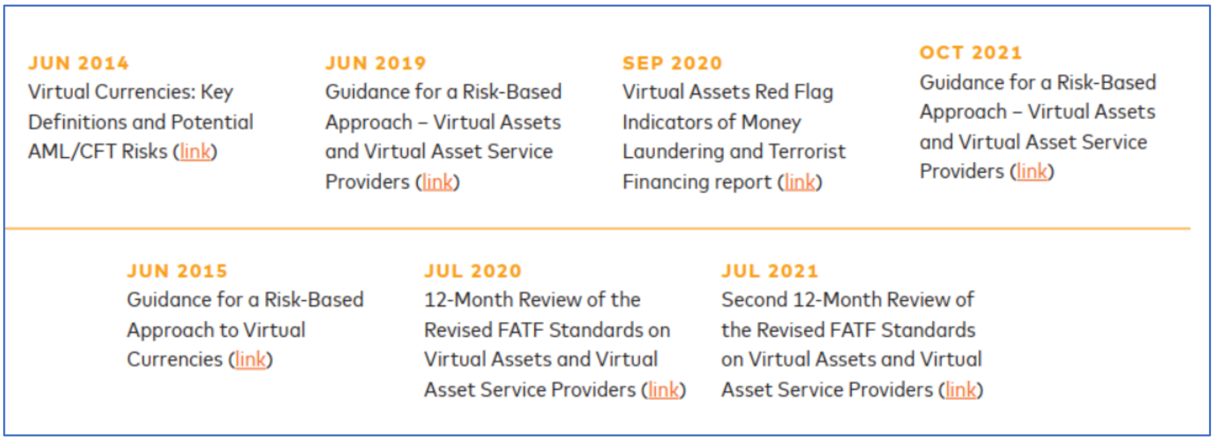
Chapter 4 discussed some legitimate use cases of blockchain, which included a discussion of how law enforcement can use blockchain forensics to aid their investigations, then the case study of the Estonian government using blockchain in the public administration infrastructure and finally, blockchain for the greater good which discusses human rights opportunities associated with the adoption of blockchain technologies. These discussions are presented as arguments to the research question of whether blockchain and cryptocurrencies provide opportunities for law enforcement bodies and how public administrative bodies can utilise blockchain.

5 New Regulations and Future of Cryptocurrencies

The future of cryptocurrencies can move towards two possibilities – one where the cryptocurrency market is regulated, and compliance-friendly, another where the anonymity feature overwhelms, and crypto markets are forced underground due to higher illegal activities. It is worth noting that crypto-related crime in 2021 was much higher and accounted for almost $14 billion in revenue (refer to Figure 2 in the Appendix). The growth of various privacy coins like ZCash, Monero and Bitcoin or cryptocurrency mixing applications is undeniable as these cryptocurrencies and mixing services help to achieve true anonymity, helping criminals delete their trails. The law enforcement bodies till now have options of blockchain forensic tools to gather insights from blockchain and illicit link transactions. There had been several successful cases where the state was able to return stolen funds, just like the case of the Colonial Pipeline hack. However, there has been an increase in mixers and privacy coins, which adds complexity to the investigations.

In early 2022, there has been significant progress in the cryptocurrency and blockchain technology regulatory work. In the US, President Joe Biden signed an executive order in early March for the responsible development of digital assets. The Executive Order will force the Administration, Congress, and several federal agencies to adopt rules and laws to guide the continuous development of digital assets. Even though multiple government and regulatory bodies have been striving to comprehend and control digital asset-related operations, this executive order established defined deliverables and deadlines for completing these distinct processes. The Executive Order also guarantees greater coordination of these efforts by establishing the guiding principles that must be attained via a balanced strategy. Protect US consumers, investors, and businesses; Protect the US and Global financial stability; Mitigate illicit finance and national security risks; Strengthen US leadership in the global financial system and technological and economic competitiveness; Promote access to safe and affordable financial services; and Support technological advances that promote the responsible development and use of digital assets. The US Treasury published the first framework on digital assets outlining how the US regulatory bodies should engage with other countries in cryptocurrencies. With lawmakers and regulatory bodies in different countries like the US and the UK moving towards regulating cryptocurrencies, more regulatory works will likely be explored in the upcoming years (Gailey and Haar, 2021). Regulators in the United Kingdom are proposing legislation permitting the use of certain stablecoins as payment instruments in the nation. The provisions are included in the long-awaited financial services and market legislation, which aims to improve the United Kingdom's financial sector after Brexit. The newly appointed finance minister, Nadhim Zahawi, detailed the new law in his first address on Tuesday. He said the decision "reinforces the United Kingdom's position as a leading technology centre as we embrace crypto assets responsibly." A copy of the law published on the government website indicates that the current standards for banking and payment systems will be amended or expanded to include digital assets. On 30 June, the European Union adopted some cryptocurrency legislation that will go into effect in the following months. These regulations are part of the Markets in Crypto Assets (MiCA) regulatory framework, which was approved in its first reading in February and will be fully implemented by the end of 2023 (Cacioppoli, 2022).

As early as 2014, the FATF published several documents on virtual assets (VAs) and virtual asset-backed securities (VASPs). The recommendations and publications of the FATF have had global influence, and they will continue to substantially impact the CFT/AML legislation and regulatory control of VAs/VASPs worldwide. Below is a visual representation of some of the most popular posts on this site:



JUN 2014
Virtual Currencies: Key Definitions and Potential AML/CFT Risks (link)

JUN 2019
Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers (link)

SEP 2020
Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing report (link)

OCT 2021
Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers (link)

JUN 2015
Guidance for a Risk-Based Approach to Virtual Currencies (link)

JUL 2020
12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers (link)

JUL 2021
Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers (link)

Figure 16. Series of Documents Published by FATF for Virtual Assets (Source: CipherTrace)

The latest publication by FATF was “Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Provider, “published in October 2021. This guidance paper focused on updating the standard for CFT/AML and emphasising risk-based methods for VAs and VASPs. This publication mainly focused on "Clarification of the definitions of VAs and VASPs; Guidance on how the FATF Standards apply to stablecoins; Additional guidance on the risks and the tools available to countries to address money laundering and terrorist financing risks for peer-to-peer transactions; Updated guidance on the licencing and registration of VASPs; Additional guidance for the public and private sectors on the implementation of the "travel rule" standards”. This paper explores the nuances of decentralised apps (dApps), decentralised finance (DeFi), non-fungible tokens (NFTs), and stablecoins. Depending on specific criteria, each of these may be classified as VAs or VASPs. FATF says that falling within VA/VASP categories depends more on the unique use case than on the language and technology (CipherTrace, 2022).

FATF provides worldwide leadership and advice to fight money laundering and terrorism funding, yet various approaches to virtual assets are currently available worldwide. Different areas, including North America, Latin America (LATAM), Europe, the Middle East, Africa (EMEA), and Asia-Pacific (APAC), view virtual assets differently. Different countries approach cryptocurrencies differently, which was discussed earlier in Chapter 2.2.7. There are a few other countries which have recently announced their legislative or regulatory framework around cryptocurrencies:

- **EMEA – Dubai**

  Law No. 4 of 2022 on the Regulation of VAs in the Emirate of Dubai was approved on February 28, 2022. (United Arab Emirates). This statute creates the Virtual Assets Regulatory Authority (VARA) as the principal regulator of virtual assets (VAs). VASPs will be required to get a licence, and the VARA will be responsible for ensuring more transparency, mitigating illicit conduct, and developing a formal supervision structure. The VARA is also entrusted with safeguarding the personal information of veterans, coordinating the issuing and trading of VAs, and combating price manipulation for VAs. Finally, the VARA will be expected to work closely with the UAE Central Bank on matters that contribute to financial stability. While there is still much work to be done, there are benefits to fostering the expansion of the regulated digital, virtual, and crypto asset ecosystem. As the duties of regulatory and government bodies become more distinct, the sector will be better equipped to comply with relevant regulations (CipherTrace, 2022).

- **Latin America – Brazil**

  In February 2022, Brazilian legislators submitted a plan to regulate the country's cryptocurrency business. The proposed law defines virtual assets and crypto service providers and focuses on reducing criminal behaviour by requiring virtual asset service providers to have AML processes to monitor illegal activities. This is only a proposed piece of law, but it is a significant first step for a nation where the usage of digital, virtual, and crypto assets continues to rise. Efforts to promote a more regulated environment will continue to be essential for combating illicit financing and safeguarding consumers (CipherTrace, 2022).

- **Asia Pacific – Hong Kong**
  The Hong Kong Monetary Authority (HKMA) and Securities and Futures Commission (SFC) released a combined circular and appendix on VA-related activities for intermediaries on January 28, 2022. The substance of typical circulars focuses primarily on investor protection and preventing illegal conduct. Specific standards for licenced intermediaries providing VA services are defined. The HKMA also released a pamphlet titled "Regulatory approach to Authorized Institutions (AIs)" to interact with Virtual Assets and Virtual Asset Service Providers on January 28, 2022. This section described several procedures about AML/CFT programme requirements when AIs deliver services to VASPs or other VA customers. In addition, the HKMA noted, "AIs seeking to participate in VA operations should consult with the HKMA (and other authorities where applicable) and get HKMA to comment on the soundness of the institution's risk management procedures before releasing relevant goods or services." 6. This strategy is compatible with the existing perspectives of the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation. The Hong Kong Monetary Authority and the Securities and Futures Commission prioritise regulation to safeguard consumers/investors and combat illegal money. These regulatory concerns increase the ecosystem's openness and confidence (CipherTrace, 2022).

5.1 Law Enforcement Activities and Enforcement Activities

Law enforcement bodies around the globe have been proactive in regulating digital assets as there is news of various enforcement actions taken by authorities in early 2022 alone. Some of the significant enforcement activities taken by different law enforcement bodies in 2022 till now (as of July 2022) are:

- Stablecoin giant Tether and its parent company Bitfinex were ordered to pay a $42.5 fine, $1.5 fine to Bitfinex for a civil monetary penalty in the US and a $41 million fine to Tether for failing to supply material facts, a misleading statement regarding their stablecoin USDT (US Dollar Pegged Tether). While CFTC also accused Bitfinex of engaging in unlawful, off-exchange retail commodities transactions with US citizens on its Bitfinex trading platform while operating as a futures commission merchant (FCM) without registering as required (CipherTrace, 2022).
- DeFi platform Polymarket was fined $1.4 million in January 2022 by CFTC for engaging in unregistered swaps. Polymarket sold off-exchange event-based binary options contracts without a specified contract market or swap execution facility registration. In addition, the CFTC ordered the company to reimburse fees associated with unregistered activity and discontinue operations. Polymarket aided the inquiry, and the fine was part of a settlement. In January 2022, three markets were broken (CipherTrace, 2022).
- The Federal Police of Brazil arrested Brazilian Bitcoin Ponzi Scam Leader Johann Steynbergil in December 2021. Multiple institutions, including Interpol and the Federal Bureau of Investigations, sought Steynberg's capture (FBI). Steynberg was the chief executive officer of a South African-based trading platform with over 165 thousand customers worldwide. Using cryptocurrency, he was able to syphon monies from multiple investing sites. South African authorities told Steynberg that he was operating an unlawful business that deceived consumers and that MTI lacked the required licences to provide cryptocurrency-based financial services.

It is undoubtedly accurate to assert that the world of cryptocurrencies had tremendous expansion in 2021, which led to a rise in illegal behaviour. As indicated in the sections on law and enforcement, the world's governments are beginning to take significant measures to prevent crypto space from becoming a modern-day Wild West. With substantial penalties, such as Tether's $41 million penalty and closure of the Hydra darknet market, these organisations will have a proper incentive to clean up their act or risk more severe damages from the government. It is unpredictable where the future of cryptocurrency lies but with new regulatory practices and increasing penalties, it is much more likely that the future of cryptocurrency lies in a regulated space.

6 Conclusion

The world of cryptocurrencies and the technology that supports them is continuously changing. Law enforcement investigations may benefit from using most cryptocurrencies, including Bitcoin and its blockchain technology. Law enforcement organisations that use blockchain to conduct investigations have taken advantage of Bitcoin's mainstream adoption. Original criminals initially used its activities can be traced to criminals thanks to available law enforcement analytic tools. Forensic blockchain technologies from Chainalysis and AML compliance solutions from CipherTrace, for example, have been created for law enforcement investigations and compliance adherence. Suspicious transactions, unlawful activity, and criminal transaction patterns all can be identified using these technologies, as seen from the case studies presented in the research where stolen funds have been returned or tracked to the destination. Numerous instances have shown that coordination between financial intelligence units and law enforcement may be very advantageous in discovering transactions originating from criminal sources.

In addition to providing investigators with new avenues for research, these technologies may provide crucial information on the blockchain's behaviour patterns. Regulation bodies have also adopted and implemented the required anti-money laundering (AML) procedures to combat money laundering and collect data on suspicious activity via financial organisations. Many incidents have shown that working with law enforcement and financial intelligence units may be very effective in discovering illegal activities. While the use of mixers and the adoption of fully anonymous cryptocurrency pose a grave threat to law enforcement as they can make the investigations more complex. With the rise in DeFi, decentralised exchanges that operate without any KYC and AML policies are also rising, which is also a threat to the investigative bodies. With more and more legislation and regulatory frameworks, the cryptocurrency world is becoming more transparent and obscure.

Finally, the research showed different legitimate use cases of blockchain, such as using blockchain technology to enhance e-government systems by analysing the case study of Estonia, establishing digital identity rights, recording assets and intellectual rights, improve voting mechanisms and supply chain tracking. The thesis then pointed out various legislative and regulatory topics adopted by multiple states for consumer protection and strict AML compliance. With the potential value prospects of blockchain and increasing regulatory and compliance efforts from various countries, it can be said that the cryptocurrency is moving towards a transparent and compliance-friendly ecosystem that will likely undermine its current illegitimate usage.

Cryptocurrencies have presented a unique challenge to how we manage our financial affairs. Despite legal and territorial jurisdictional difficulties, the cryptocurrency industry has acquired a worldwide presence despite the immaturity of its validity. Cryptocurrencies have been abused for extortion, tax evasion, and other illicit activities like drug trading and terrorism funding, as shown in case studies I and II. However, it is in the public interest to regulate cryptocurrencies rather than consider them a threat and abolish them. The government must reach out to and include all relevant parties to create new laws and regulations regulating cryptocurrencies and virtual currency exchanges. There is tremendous support for adopting cryptocurrencies from many sectors of the business and technology communities.

Bibliography

Aiden (2020) ‘Record Number of Dark Markets Online as Demand for Illicit Goods and Services Continues to Grow - CipherTrace’, 26 October. Available at: https://ciphertrace.com/record-number-of-dark-markets-online-as-demand-for-illicit-goods-and-services-continues-to-grow/ (Accessed: 23 July 2022).

Alvarez, F., Argente, D. and Van Patten, D. (2022) ‘Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador’. Available at: https://www.nber.org/system/files/working_papers/w29968/w29968.pdf (Accessed: 26 July 2022).

Arslanian, H. *et al.* (2021) *El Salvador’s law: a meaningful test for Bitcoin*. PWC, p. 11. Available at: https://www.pwc.com/gx/en/financial-services/pdf/el-salvadors-law-a-meaningful-test-for-bitcoin.pdf.

Baliga, D.A. (2020) ‘Understanding Blockchain Consensus Models’, p. 17.

Bank of England (2020) *What are cryptoassets (cryptocurrencies)?* Available at: https://www.bankofengland.co.uk/knowledgebank/what-are-cryptocurrencies (Accessed: 16 July 2022).

Barragan, J. (2021) ‘Case Study: Hydra—Russia’s Largest Dark Market - CipherTrace’, 28 June. Available at: https://ciphertrace.com/hydra-russias-largest-dark-market/ (Accessed: 24 July 2022).

Baydakova, A. (2020) *Digital Ruble Could Be Tool Against Sanctions, Bank of Russia Says*. Available at: https://www.coindesk.com/policy/2020/10/19/digital-ruble-could-be-tool-against-sanctions-bank-of-russia-says/ (Accessed: 25 July 2022).

#Blockchain4Humanity: Use blockchain technology to help combat child trafficking in Moldova. (2018) *United Nations, UNite Ideas*. Available at: https://ideas.unite.un.org/blockchain4humanity/Page/Home (Accessed: 25 July 2022).

Boom, D.V. (2022) *Luna Cryptocurrency Collapse: How UST Broke and Why It Matters*, *CNET*. Available at: https://www.cnet.com/personal-finance/crypto/luna-crypto-crash-how-ust-broke-and-whats-next-for-terra/ (Accessed: 20 July 2022).

Browne, R. (2022) *Bitcoin production roars back in China despite Beijing’s ban on crypto mining*, *CNBC*. Available at: https://www.cnbc.com/2022/05/18/china-is-second-biggest-bitcoin-mining-hub-as-miners-go-underground.html (Accessed: 22 July 2022).

Cacioppoli, V. (2022) ‘EU approves crypto regulatory framework’, *The Cryptonomist*, 25 July. Available at: https://en.cryptonomist.ch/2022/07/25/eu-approves-crypto-regulatory-framework/ (Accessed: 25 July 2022).

Chainalysis (2020) *BitcoinTransfer: Syria-based Cryptocurrency Exchange Facilitating Terrorism Financing*. Intelligence Brief. Chainanalysis. Available at: https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis%20Intelligence%20Brief%20-%20BitcoinTransfer.pdf (Accessed: 24 July 2022).

Chainalysis (2021) *[REPORT PREVIEW] Why Is China Launching the Digital Yuan?*, *Chainalysis*. Available at: https://blog.chainalysis.com/reports/china-report-preview-digital-yuan/ (Accessed: 22 July 2022).

Chainalysis (2022a) *Chainalysis In Action: How FBI Investigators Traced DarkSide's Funds Following the Colonial Pipeline Ransomware Attack*, *Chainalysis*. Available at: https://blog.chainalysis.com/reports/darkside-colonial-pipeline-ransomware-seizure-case-study/ (Accessed: 21 July 2022).

Chainalysis (2022b) *Crypto Crime Report 2022*. Available at: https://go.chainalysis.com/2022-crypto-crime-report.html (Accessed: 14 June 2022).

Chipolina, D./ S. (2021) *Art Has a Money Laundering Problem. NFTs Could Make It Worse*, *Decrypt*. Available at: https://decrypt.co/70190/art-has-a-money-laundering-problem-nfts-could-make-it-worse (Accessed: 25 July 2022).

Chohan, U. (2017) 'Cryptocurrencies: A Brief Thematic Review', *SSRN Electronic Journal* [Preprint]. Available at: https://doi.org/10.2139/ssrn.3024330.

CipherTrace (2022) *CipherTrace Cryptocurrency Crime and Anti-Money Laundering Report, June 2022*. CipherTrace, p. 20. Available at: https://ciphertrace.com/crime-and-anti-money-laundering-report/ (Accessed: 24 June 2022).

Cloudflare (2022) *What is a distributed denial-of-service (DDoS) attack?*, *Cloudflare*. Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (Accessed: 23 July 2022).

CNN Business (2022) *Crypto is making a big comeback. Will it last?*, *CNN*. Available at: https://www.cnn.com/2022/07/19/investing/bitcoin-cryptocurrencies-stocks-coinbase/index.html (Accessed: 20 July 2022).

Crumpler, W., Flacks, M. and Mandavilli, A. (2021) 'The Human Rights Risks and Opportunities in Blockchain', p. 90.

Cryptopedia (2022) *Crypto Wallet Types: Compared*, *Gemini*. Available at: https://www.gemini.com/cryptopedia/crypto-wallet-types, https://www.gemini.com/cryptopedia/crypto-wallet-types (Accessed: 20 July 2022).

Darknet One (2022) *#1 Darknet Markets List 2022*, *DarknetOne*. Available at: https://darknetone.com/markets/ (Accessed: 23 July 2022).

Deccan Herald (2022) 'India has second-highest cryptocurrency users in world: Report', 7 February. Available at: https://www.deccanherald.com/business/business-news/india-has-second-highest-cryptocurrency-users-in-world-report-1079046.html (Accessed: 22 July 2022).

Elliptic (2021) *Liquid Exchange Hacked: $97 Million Stolen*. Available at: https://www.elliptic.co/blog/liquid-exchange-hacked-94-million-stolen (Accessed: 25 July 2022).

‘Farrukh Furkatovitch Fayzimatov | Counter Extremism Project’ (2022) *Terrorists and Extremists Database*. Counter Extremism Project. Available at: https://www.counterextremism.com/extremists/farrukh-furkatovitch-fayzimatov (Accessed: 24 July 2022).

FATF (2014) *Virtual currencies – Key Definitions and Potential AML/CFT Risks*. Financial Action Task Force (FATF), p. 17. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (Accessed: 16 July 2022).

FlashPointIntel and Chainalysis (2022) *Hydra: Where Cryptocurrency Cybercrime Goes Dark*. Chainanalysis. Available at: https://flashpoint.io/resources/research/flashpoint-and-chainalysis-investigate-hydra-where-cryptocurrency-cybercrime-goes-dark/ (Accessed: 24 July 2022).

Flitter, E. and Yaffe-Bellany, D. (2022) ‘Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions’, *The New York Times*, 23 February. Available at: https://www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html (Accessed: 25 July 2022).

Foley, S., Karlsen, J.R. and Putniņš, T.J. (2019) ‘Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?’, *The Review of Financial Studies*, 32(5), pp. 1798–1853. Available at: https://doi.org/10.1093/rfs/hhz015.

Gailey, A. and Haar, R. (2021) ‘The Future of Cryptocurrency: 8 Experts Share Predictions for the Second Half of 2022’, *Time*, 19 August. Available at: https://time.com/nextadvisor/investing/cryptocurrency/future-of-cryptocurrency/ (Accessed: 25 July 2022).

Gonzálvez-Gallego, N. and Pérez-Cárceles, M.C. (2021) ‘Cryptocurrencies and illicit practices: The role of governance’, *Economic Analysis and Policy*, 72, pp. 203–212. Available at: https://doi.org/10.1016/j.eap.2021.08.003.

He, D. *et al.* (2016) ‘Virtual Currencies and Beyond: Initial Considerations’, *Staff Discussion Notes*, 16(03), p. 1. Available at: https://doi.org/10.5089/9781498363273.006.

Houben, D.R. and Snyers, A. (2018) ‘Cryptocurrencies and blockchain’. Policy Department for Economic, Scientific and Quality of Life Policies European Parliament. Available at: http://www.europarl.europa.eu/supporting-analyses (Accessed: 25 November 2021).

Howcroft, E. (2021) ‘Set of “Bored Ape” NFTs sells for $24.4 mln in Sotheby’s online auction’, *Reuters*, 9 September. Available at: https://www.reuters.com/lifestyle/set-bored-ape-nfts-sell-244-mln-sothebys-online-auction-2021-09-09/ (Accessed: 25 July 2022).

Imteaj, A., Amini, M.H. and Pardalos, P.M. (2021) *Foundations of Blockchain: Theory and Applications*. Cham: Springer International Publishing (SpringerBriefs in Computer Science). Available at: https://doi.org/10.1007/978-3-030-75025-1.

Iredale, G. (2020) ‘DeFi vs CeFi - Understanding the Differences’, *101 Blockchains*, 17 October. Available at: https://101blockchains.com/defi-vs-cefi/ (Accessed: 20 July 2022).

Kassen, M. (2022) 'Blockchain and e-government innovation: Automation of public information processes', *Information Systems*, 103, p. 101862. Available at: https://doi.org/10.1016/j.is.2021.101862.

Katz, R. (2019) 'Tales of Crypto-Currency: Bitcoin Jihad in Syria and Beyond', *The Daily Beast*, 13 October. Available at: https://www.thedailybeast.com/the-bitcoin-jihad-in-syria-and-beyond-tales-of-crypto-currency (Accessed: 24 July 2022).

Keene, L. (2014) 'Cryptocurrencies: The Next Generation of Terrorist Financing?', *Defence Against Terrorism*, 6, p. 24.

Khanna, A. *et al.* (2021) 'Blockchain: Future of e-Governance in Smart Cities', *Sustainability*, 13(21), p. 11840. Available at: https://doi.org/10.3390/su132111840.

Kharpal, A. (2022) *China launches app for its own digital currency as it looks to expand usage*, *CNBC*. Available at: https://www.cnbc.com/2022/01/04/china-launches-digital-currency-app-to-expand-usage.html (Accessed: 22 July 2022).

Li, S., Qin, T. and Min, G. (2019) 'Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems', *IEEE Transactions on Computational Social Systems*, 6(6), pp. 1433–1441. Available at: https://doi.org/10.1109/TCSS.2019.2927431.

Loo, A. (2022) *Types of Cryptocurrency*, *Corporate Finance Institute*. Available at: https://corporatefinanceinstitute.com/resources/knowledge/other/types-of-cryptocurrency/ (Accessed: 20 July 2022).

Lucking, D., Aravind, V. and LLP, O. (2019) 'Cryptocurrency as a Commodity: The CFTC's Regulatory Framework', p. 296. Available at: https://www.allenovery.com/global/-/media/allenovery/2_documents/news_and_insights/publications/2019/8/cryptocurrency_as_a_commodity_the_cftcs_regulator_framework.pdf?la=en-gb&hash=8FB9966803A518C6CDC922AE1C6880AA (Accessed: 21 July 2022).

Mangan, D. (2022) *World's biggest darknet marketplace, Russia-linked Hydra Market, seized and shut down, DOJ says*, *CNBC*. Available at: https://www.cnbc.com/2022/04/05/darknet-hydra-market-site-seized-and-shut-down-doj-says.html (Accessed: 24 July 2022).

Martinson, P. (2019) *Estonia – the Digital Republic Secured by Blockchain*. PWC, p. 12. Available at: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf.

Mohsin, K. (2022) 'Cryptocurrency Legality and Regulations – An International Scenario', *International Journal of Cryptocurrency Research*, 2(1), pp. 19–29. Available at: https://doi.org/10.51483/IJCCR.2.1.2022.19-29.

Nakamoto, S. (2008) 'Bitcoin: A Peer-to-Peer Electronic Cash System', p. 9.

Natarajan, H., Krause, S. and Gradstein, H. (2017) 'Distributed Ledger Technology (DLT) and Blockchain'. International Bank for Reconstruction and Development / the World Bank. Available at:

https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf (Accessed: 13 July 2022).

Newmyer, T. and B. Merrill, jeremy (2022) 'U.S. hasn't stopped N. Korean gang from laundering its crypto haul', *Washington Post*, 23 April. Available at: https://www.washingtonpost.com/business/2022/04/23/north-korea-hack-crypto-access/ (Accessed: 20 July 2022).

Nichols, M. (2022) 'EXCLUSIVE North Korea grows nuclear, missiles programs, profits from cyberattacks -U.N. report', *Reuters*, 7 February. Available at: https://www.reuters.com/world/asia-pacific/exclusive-nkorea-grows-nuclear-missiles-programs-profits-cyberattacks-un-report-2022-02-05/ (Accessed: 24 July 2022).

Owen, A. and Chase, I. (2021) *NFTs: A New Frontier for Money Laundering?* Available at: https://rusi.org/explore-our-research/publications/commentary/nfts-new-frontier-money-laundering (Accessed: 25 July 2022).

Parol, J. (2018) *Blockchain from Public Administration Perspective: Case of Estonia*. Talinn University of Technology. Available at: https://digikogu.taltech.ee/en/Download/d591ed87-3350-44a1-acb3-f0e184f9dc18/PlokkahelavalikuhaldusevaatenurgastEestiKaas.pdf (Accessed: 28 November 2021).

Peyton, A. (2020) 'India's Supreme Court overturns cryptocurrency ban – Fintech Direct', 5 March. Available at: https://www.fintechdirect.net/2020/03/05/indias-supreme-court-overturns-cryptocurrency-ban/ (Accessed: 22 July 2022).

Phan, T. (2021) *Exploring Blockchain Forensics*, *ISACA*. Available at: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-36/exploring-blockchain-forensics (Accessed: 25 July 2022).

Ramakrishnan, V. (2022) 'FinCEN Warns of Potential Russian Sanctions Evasion', *Investopedia*, 8 March. Available at: https://www.investopedia.com/fincen-warning-sanctions-evasion-5221429 (Accessed: 24 July 2022).

Rappeport, A. (2021) 'Treasury Warns That Digital Currencies Could Weaken U.S. Sanctions', *The New York Times*, 18 October. Available at: https://www.nytimes.com/2021/10/18/us/politics/sanctions-cryptocurrency-treasury.html (Accessed: 25 July 2022).

Redman, J. (2020) *A System of Robot Drug Dealers on Telegram Allows People to Buy Illegal Products for Bitcoin – Bitcoin News*, *Bitcoin.com*. Available at: https://news.bitcoin.com/a-system-of-robot-drug-dealers-on-telegram-allows-people-to-buy-illegal-products-for-bitcoin/ (Accessed: 24 July 2022).

Reuters (2021) 'China vows to crack down on bitcoin mining, trading activities', *Reuters*, 21 May. Available at: https://www.reuters.com/technology/china-says-it-will-crack-down-bitcoin-mining-trading-activities-2021-05-21/ (Accessed: 22 July 2022).

Reuters (2022) ‘Crypto giant Binance kept weak money-laundering checks, documents show’, January. Available at: https://www.reuters.com/investigates/special-report/finance-crypto-currency-binance/ (Accessed: 20 July 2022).

Robinson, Dr.T. (2021) *How Iran Uses Bitcoin Mining to Evade Sanctions and “Export” Millions of Barrels of Oil*, *Elliptic*. Available at: https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions (Accessed: 25 July 2022).

Santiso, C. (2018) *Will Blockchain Disrupt Government Corruption? (SSIR)*. Available at: https://ssir.org/articles/entry/will_blockchain_disrupt_government_corruption (Accessed: 25 July 2022).

Sapovadia, V. (2015) ‘Legal Issues in Cryptocurrency’, in, pp. 253–266. Available at: https://doi.org/10.1016/B978-0-12-802117-0.00013-8.

Shanahan, R. (2018) *Charities and terrorism: Lessons from the Syrian crisis*. Lowy Institute. Available at: https://charts.lowyinstitute.org/archive/charities-and-terrorism-lessons-from-the-syrian-crisis/ (Accessed: 24 July 2022).

Silfversten, E. *et al.* (2020) *Exploring the use of Zcash cryptocurrency for illicit or criminal purposes*. RAND Corporation. Available at: https://doi.org/10.7249/RR4418.

Singh, J. and Singh, M. (2022) ‘India’s central bank wants to ban cryptocurrencies govt says’, *TechCrunch*, 18 July. Available at: https://social.techcrunch.com/2022/07/18/indias-central-bank-wants-to-ban-cryptocurrencies/ (Accessed: 22 July 2022).

Snip, I. (2017) *Georgia: Authorities Use Blockchain Technology for Developing Land Registry | Eurasianet*, *Eurasianet*. Available at: https://eurasianet.org/georgia-authorities-use-blockchain-technology-for-developing-land-registry (Accessed: 25 July 2022).

Srivastava, N. (2021) ‘Blockchain Governance in Estonia may be Inspiration for the Entire World -’, *Blockchain Council*, 20 January. Available at: https://www.blockchain-council.org/blockchain/blockchain-governance-in-estonia-may-be-inspiration-for-the-entire-world/ (Accessed: 25 July 2022).

Starkie, H. (2017) ‘Usage of Blockchain in the UN System’, August. Available at: https://unite.un.org/sites/unite.un.org/files/session_3_b_blockchain_un_initiatives_final.pdf (Accessed: 10 July 2022).

The Economic Times (2022) ‘India’s position on Cryptocurrency vindicated by global trends’, 5 July. Available at: https://economictimes.indiatimes.com/tech/technology/indias-position-on-cryptocurrency-vindicated-by-global-trends/articleshow/92668864.cms (Accessed: 22 July 2022).

Tsai, F.-C. (2021) ‘The Application of Blockchain of Custody in Criminal Investigation Process’, *Procedia Computer Science*, 192, pp. 2779–2788. Available at: https://doi.org/10.1016/j.procs.2021.09.048.

Turner, A.B., McCombie, S. and Uhlmann, A.J. (2020) 'Analysis Techniques for Illicit Bitcoin Transactions', *Frontiers in Computer Science*, 2, p. 600596. Available at: https://doi.org/10.3389/fcomp.2020.600596.

US Department of Justice (2020) 'Global Disruption of Three Terror Finance Cyber-Enabled Campaigns', 12 August. Available at: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns (Accessed: 24 July 2022).

U.S. Department of the Treasury (2021) 'Treasury Designates Al-Qa'ida-Linked Financial Facilitators in Turkey and Syria', 28 July. Available at: https://home.treasury.gov/news/press-releases/jy0293 (Accessed: 24 July 2022).

USC U.S.-China Institute (2021) 'China Bans Cryptocurrencies | US-China Institute', 30 September. Available at: https://china.usc.edu/china-bans-cryptocurrencies (Accessed: 10 July 2022).

Vermaak, W. (2021) *What Are Privacy Coins? | CoinMarketCap*, *CoinMarketCap Alexandria*. Available at: https://coinmarketcap.com/alexandria/article/what-are-privacy-coins (Accessed: 20 July 2022).

Weinstein, J. (2015) *How can law enforcement leverage the blockchain in investigations?*, *Coin Center*. Available at: https://www.coincenter.org/education/policy-and-regulation/how-can-law-enforcement-leverage-the-blockchain-in-investigations/ (Accessed: 21 July 2022).

White, M., Killmeyer, J. and Chew, B. (2017) *Will blockchain transform the public sector?*, *Deloitte Insights*. Available at: https://www2.deloitte.com/us/en/insights/industry/public-sector/understanding-basics-of-blockchain-in-government.html (Accessed: 25 July 2022).

Why Chainalysis (2022) *Chainalysis*. Available at: https://www.chainalysis.com/why-chainalysis/ (Accessed: 25 July 2022).

Appendix

Figure 1. **Total Market Capitalisation of Cryptocurrency between 2013 to 2022 (Source – CoinMarketCap)**

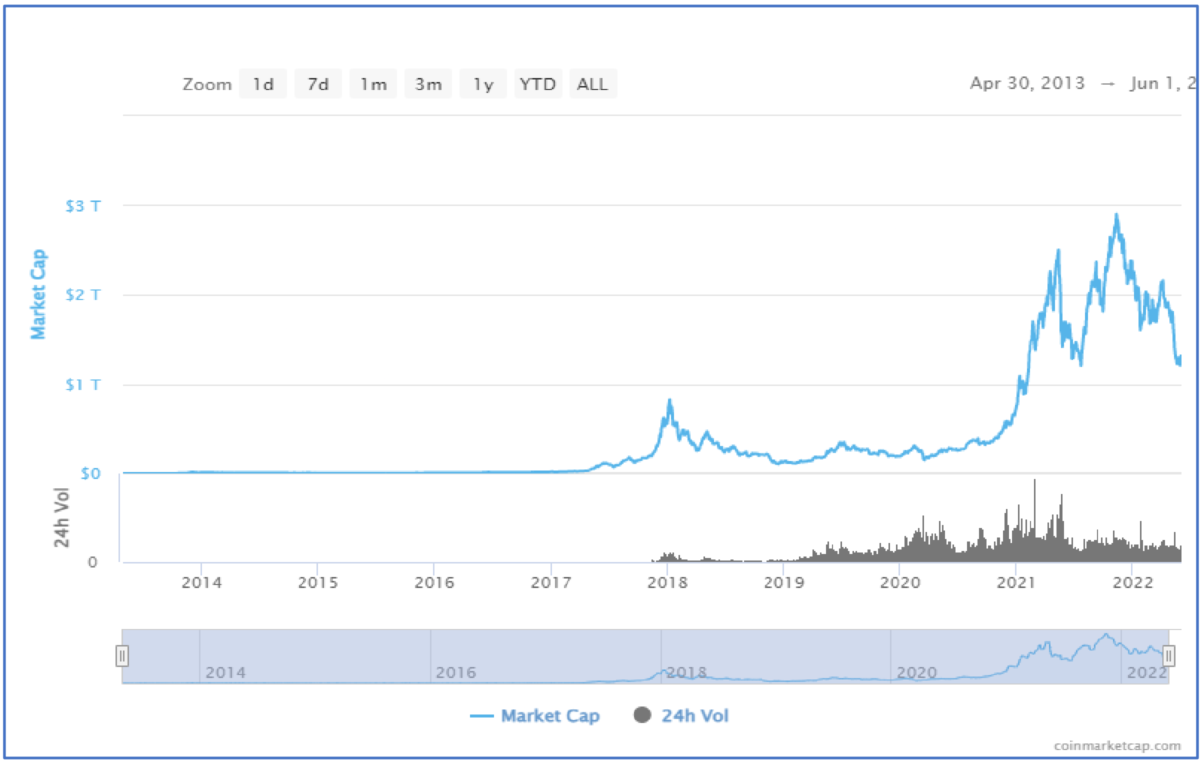


Figure 2. **Total Cryptocurrency Value Received by Illicit Addresses, 2017-2021 for various illicit activities**

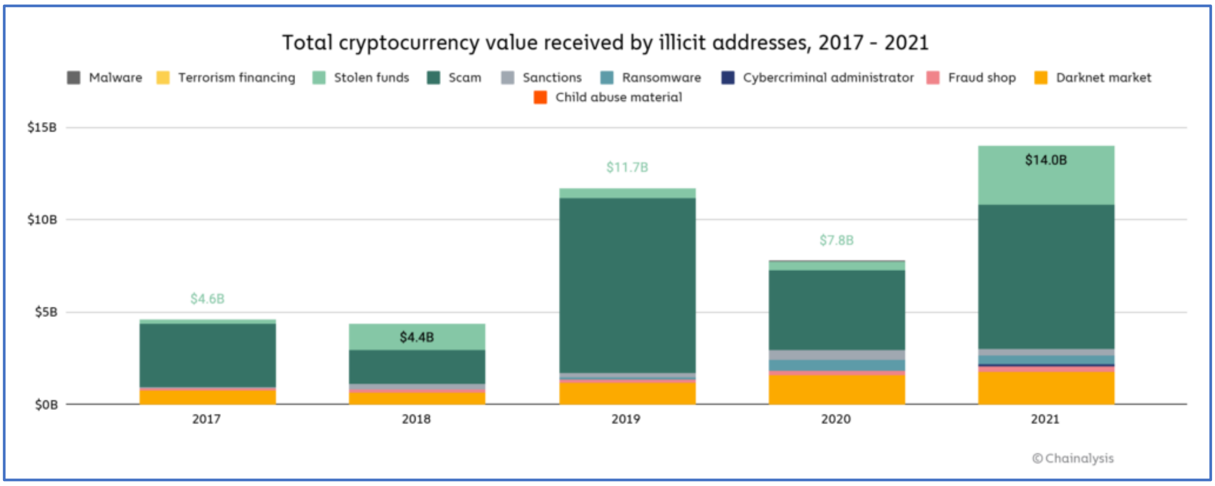


Figure 3. **What is Bitcoin Mining? How do Bitcoin Transactions work? (Source: BitPanda)**

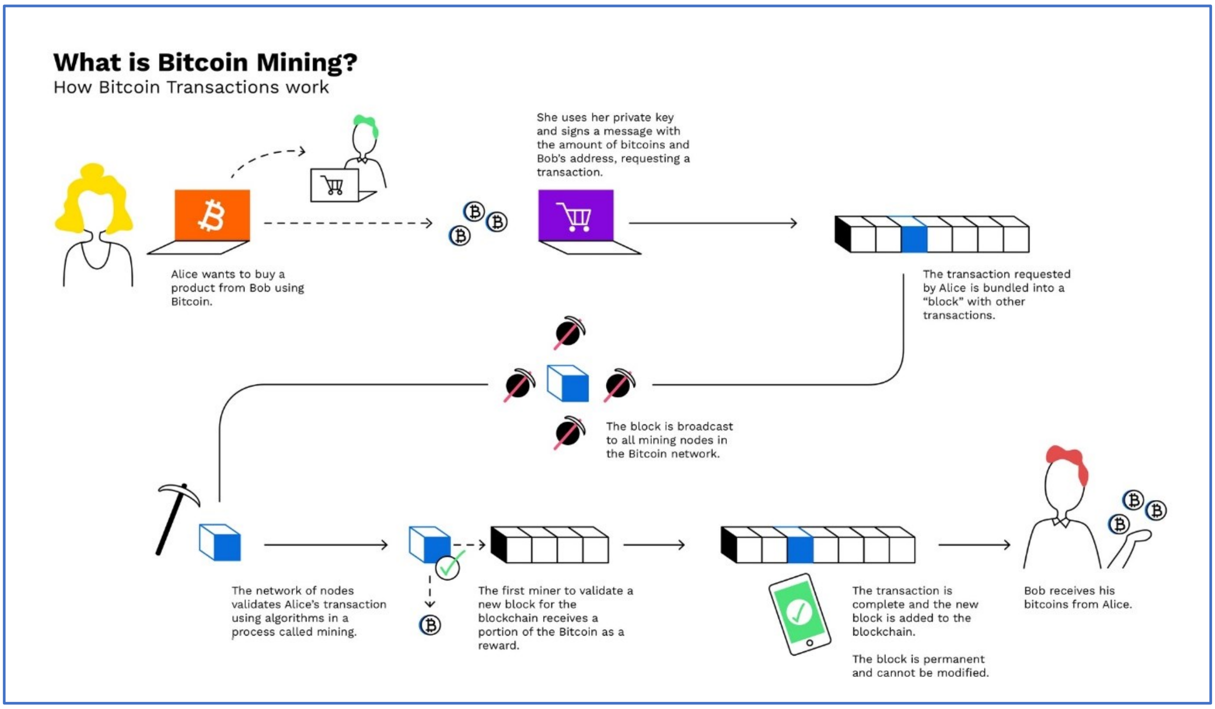

What is Bitcoin Mining?
How Bitcoin Transactions work
She uses her private key and signs a message with the amount of bitcoins and Bob's address, requesting a transaction.
Alice wants to buy a product from Bob using Bitcoin.
The transaction requested by Alice is bundled into a "block" with other transactions.
The block is broadcast to all mining nodes in the Bitcoin network.
The network of nodes validates Alice's transaction using algorithms in a process called mining.
The first miner to validate a new block for the blockchain receives a portion of the Bitcoin as a reward.
The transaction is complete and the new block is added to the blockchain.
The block is permanent and cannot be modified.
Bob receives his bitcoins from Alice.

Figure 4. **Silk Road Payment System Using Bitcoin in Escrow (Source: Ciphertrace)**

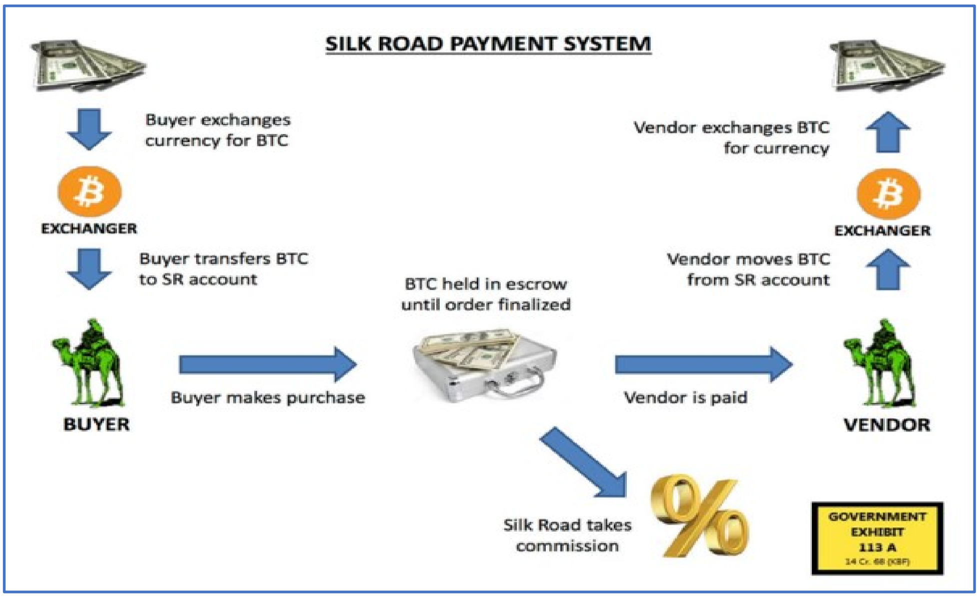

SILK ROAD PAYMENT SYSTEM
Buyer exchanges currency for BTC
EXCHANGER
Buyer transfers BTC to SR account
BUYER
Buyer makes purchase
BTC held in escrow until order finalized
Vendor is paid
VENDOR
Vendor exchanges BTC for currency
EXCHANGER
Vendor moves BTC from SR account
Silk Road takes commission
GOVERNMENT EXHIBIT 113 A
14 Cr. 68 (KBF)

Figure 5. **Darknet Market Timeline from Jan 2018 to Oct 2020 (Source: [CyperTrace Cryptocurrency Intelligence]())**

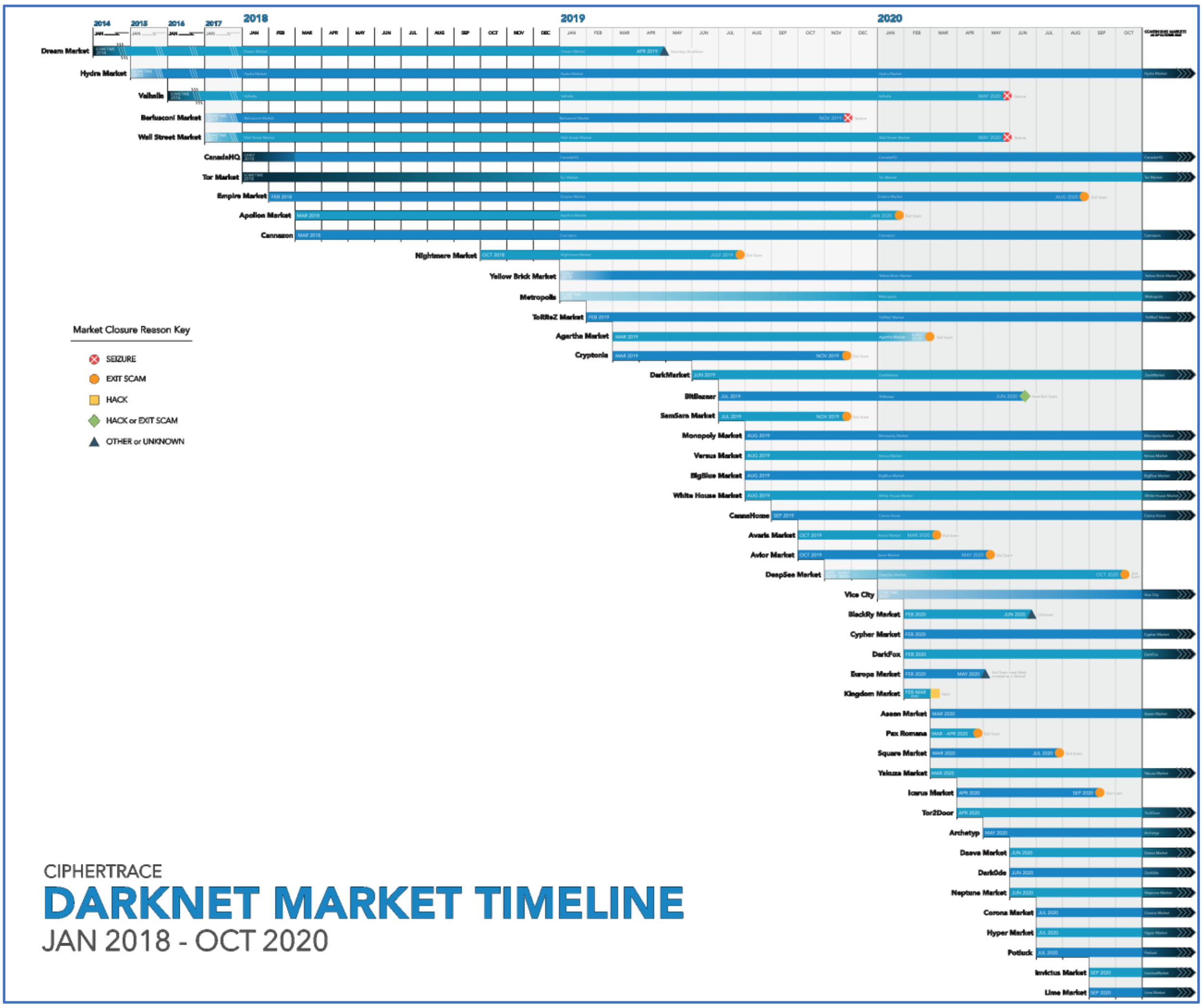
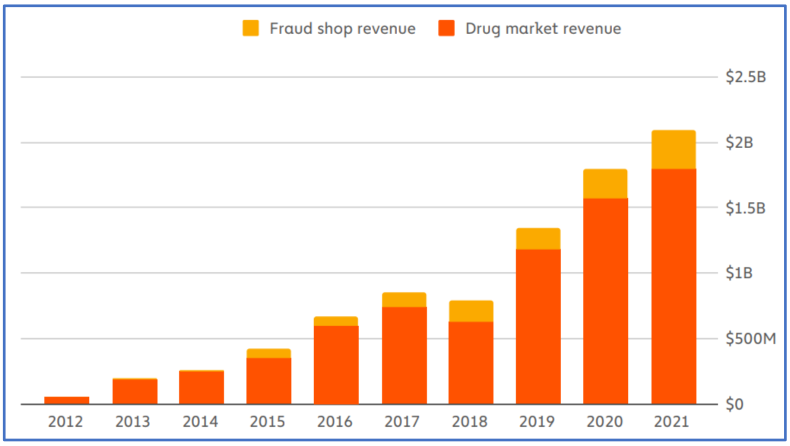


Figure 6. **Darknet Market Revenue By Market Category, 2013 -2021 (Source: Crypto Crime Report 2022 by Chainalysis)**


Fraud shop revenue
Drug market revenue
$2.5B
$2B
$1.5B
$1B
$500M
$0