

Combatting Illicit Activity

Utilizing Financial

Technologies and

Cryptocurrencies

Phase II

A Focus on the Evolution of

Digital Assets by Threat Actors

and Organized Criminal Groups



Abstract

Private and public sector professionals and subject matter experts working in the cyber financial landscape gathered to examine the use of financial technologies and cryptocurrencies by illicit actors. Phase 1 of this research focused on a general overview of the emerging illicit activity pertaining to digital assets and the peer-to-peer payment space. This included discovering the most common illicit finance activities, the most exploited elements of financial technologies, the legal vulnerabilities that allow exploitation, pseudo-anonymity in online transactions, weaknesses in Know-Your-Customer laws, and the risks of other emerging blockchain applications (i.e. NFTs).

Phase 2 of the research serves to build upon the foundation laid in Phase 1. The Phase 2 research further explores: the criminal groups utilizing digital assets in illegal activities; how these criminal groups are conducting illicit activity and recruiting members; cryptocurrency ATMs and Point-of-Sales illicit uses; generative AI applications in cybercrime; darknet market use of digital assets; the evolving use of cryptocurrencies (especially the year to date change); criminal activity's impact on government and private sector; and additional policy recommendations. Although illicit use can never be completely eliminated, it can be mitigated by increased consumer knowledge, proactive law enforcement investigations, and better practices and regulations issued by key stakeholders.

DISCLAIMER STATEMENT: The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Companies whose analysts participated in the Public-Private Analytic Exchange Program. This document is provided for educational and informational purposes only and may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.



Team Introductions

MEMBERS	COMPANY/AGENCY
Champion: Stephen Deininger	NSA
Kevin Lyons, Sec+, CFE	U.S. Secret Service
Mattonna Wahlgren, CFCS	Western Union
Melanie Gersten	Mastercard
Chad Ratashak, CFCS	Wells Fargo
Heather Jones	DoD
Seth Sattler	Digital Mint
Jessica Leonard	DoD
David Housman	Mastercard
Julia Maguire	Citibank
Jon McWilliams	FBI

Table of Contents

Abstract	1
Team Introductions	3
Table of Contents	4
Current Use of Digital Assets by Illicit Actors & Criminal Groups	7
Russia	7
North Korea (DPRK)	11
Cartel Finance	15
Terrorist Financing	20
Growth and Capacity of Criminal Groups Engaging in Illicit Digital Asset Activity	21
Ransomware	22
Scams	24
Cryptocurrency Point-of-Sales	26
Growth of the Market	26
A Change in Landscape	26
Controlling the Growth	27
The Intersection Of Mass Appeal And Nefarious Actors	28
Moves To Change The Reputation	31
Generative AI and Cybercrime: Impact on Digital Assets and Cryptocurrencies	32
A conversation with ChatGPT 4:	34
Darknet Market Use of Digital Assets	42
Growth of Darknet Market Use	42
Case Study: Arrest of Anatoly Legkodymov, the founder of cryptocurrency exchange Bitzlato, in January 2023	43
Current Darknet Markets & Significant Takedowns	43
Case Studies: Hydra and Dream Market Shutdowns	45
Privacy Coins on Darknet Markets	47
Combating Illicit Drug Sales on Darknet Markets	47
Exchanges and Mixers on the Darknet	48
Case Study: ChipMixer Shutdown	48
Outlook on Darknet Market Usage	49
The Evolving Use of Digital Assets by Criminal Organizations	50
DeFi Hacks and Exploits	50
Unlawful Hacking is Unlawful Hacking	50

Is Code Law?	50
Draining Liquidity Pools	51
Oracle Problems.....	51
North Korean (DPRK) Bridge Hacks.....	51
Case Study: Harmony Bridge (Paragraph 165 from S/2023/171).....	52
Case Study: Axie Infinity Ronin Bridge.....	53
Governance Attacks on Decentralized Autonomous Organizations (DAOs)	53
Case study: Build Finance DAO governance attack	54
Case study: Beanstalk DAO flash loan governance attack.....	55
TTP: Transferring Funds to Third-Party During Trial or Legal Proceeding	55
Case Study: Helix Mixer Brothers ⁸⁷	55
Other Examples.....	55
Summary from AEP 2022 Ransomware Attacks on Critical Infrastructure Sectors ⁸⁸	56
Dollars or other fiat.....	56
Cryptocurrency	56
Back to fiat	56
Asset Seizures and Clawbacks.....	57
NFTs: Rug Pulls and Wash Trading.....	57
Case Study: Frosties/Embers NFT Rug Pull	57
Wash Trading ⁹⁰	58
Dusting Attacks Following Tornado Cash Sanctions	58
Impact on Government and Private Sector.....	59
Public-Private Partnerships.....	59
Advanced Tools and Traditional Methods.....	60
Emerging Policy.....	60
Leveraging IC3 Data	61
Future Regulations, Forecast, and Areas for Future Study	64
Cryptocurrency Naming Conventions (Refer to Appendix B for Naming Convention Chart)	65
Analytic Dissemination Plan	69
Endnotes	70
Citations Separated by Section	75
Citations for Current Use of Digital Assets by Illicit Actors & Criminal Groups	75
Citations for Growth and Capacity of Criminal Groups Engaging in Illicit Digital Asset Activity.....	78
Citations for Cryptocurrency Point-of-Sales.....	79

Citations for Generative AI and Cybercrime: Unraveling the Impact on Digital Assets and Cryptocurrencies80

Citations for Darknet Market Use of Digital Assets80

Citations for The Evolving Use of Digital Assets by Criminal Organizations.....82

Citations for Impact on Government and Private Sector | Future Regulations, Forecast, and Areas for Future Study84

Appendices 86

Appendix A: Cryptocurrency Brochure 86

Appendix B: Cryptocurrency Naming Conventions Chart..... 87

Current Use of Digital Assets by Illicit Actors & Criminal Groups

Russia

Cryptocurrency leveraged as a new conduit for sanctions evasion via prepaid card schemes

Since the inception of the Russia-Ukraine Crisis, the Russian economy has been significantly impacted as a result of the international sanctions that have been levied against the state. This has subsequently led to both Russian cybercriminals, Russian state actors and intelligence services needing to find a variety of workarounds to move their illicit funds. Among these methods, cryptocurrency has emerged as a viable means for funding illicit cyber activity, as well as Russian intelligence and military operations, posing immediate risks to US national security interests.

Research conducted by the blockchain analytics firm, *Elliptic*, revealed that cryptocurrency is now almost certainly going to be leveraged in Russia's sanctions evasion tactics. Elliptic's research has identified over 400 virtual asset services providers which allow the purchasing of cryptocurrency with rubles. Elliptic has also connected several million cryptocurrency addresses to these service providers, many of which are unregulated, do not enforce Know Your Customer laws, and can be used anonymously. Additionally, their research has directly connected over 15 million cryptocurrency addresses associated with criminal activity to Russian actors, to include several hundred thousand cryptocurrency addresses linked to Russian-based actors who have already been sanctioned.¹

One of the common illicit finance schemes that has been historically leveraged by a variety of Russian threat actors is the acquisition of prepaid cards from neighboring countries. These cards can then be used to order subscriptions or goods that are later delivered through intermediaries in neighboring countries, to include the transiting point of delivery, prior to entering Russia. Loose Know Your Customer "KYC" policies facilitate pseudo-anonymous abilities for threat actors who utilize this method to operate relatively undetected; however, law enforcement entities have become increasingly more witting to these tactics in recent months, as evidenced by the joint Financial Crimes Enforcement Network (FinCEN) and US Department of Commerce's Bureau of Industry and Security (BIS) alert released in June 2022. The alert restricted exports that were known to pass through certain countries such as Belarus, prior to reaching Russian buyers. This alert also provided financial institutions with an overview of BIS's current export restrictions, a list of commodities of concern for possible export controls evasion, as well as specific transactional and behavioral red flags that would assist financial institutions in identifying suspicious transactions that could be related to evasion activity. Given the more stringent level of restrictions that has been placed on illicit actors obtaining prepaid

cards, these threat actors are now turning to foreign-issued prepaid virtual credit cards that are backed by cryptocurrency, which are also known as “VCCs.”

Research conducted by The Inskit Group of Recorded Future found that there are many Russian freelancers, IT professionals and criminals that are already receiving direct payments in cryptocurrency. Conversion from Russian rubles to cryptocurrency is also a quick and easy process through a variety of third-party services. Consequently, this method naturally facilitates immediate access to United States dollars anywhere the payment service is accepted within the United States, with minimal, and in some cases non-existent, abilities for law enforcement or intelligence entities to determine attribution. Additionally, some of these cards can be loaded with up to \$1,000 and do not require any form of user verification, nor do they follow KYC laws.

The below case example was taken from the dark web forum “*Exploit*” and consists of an inquiry regarding anonymous online cryptocurrency-based payment methods for Russian residents.

Example 1:

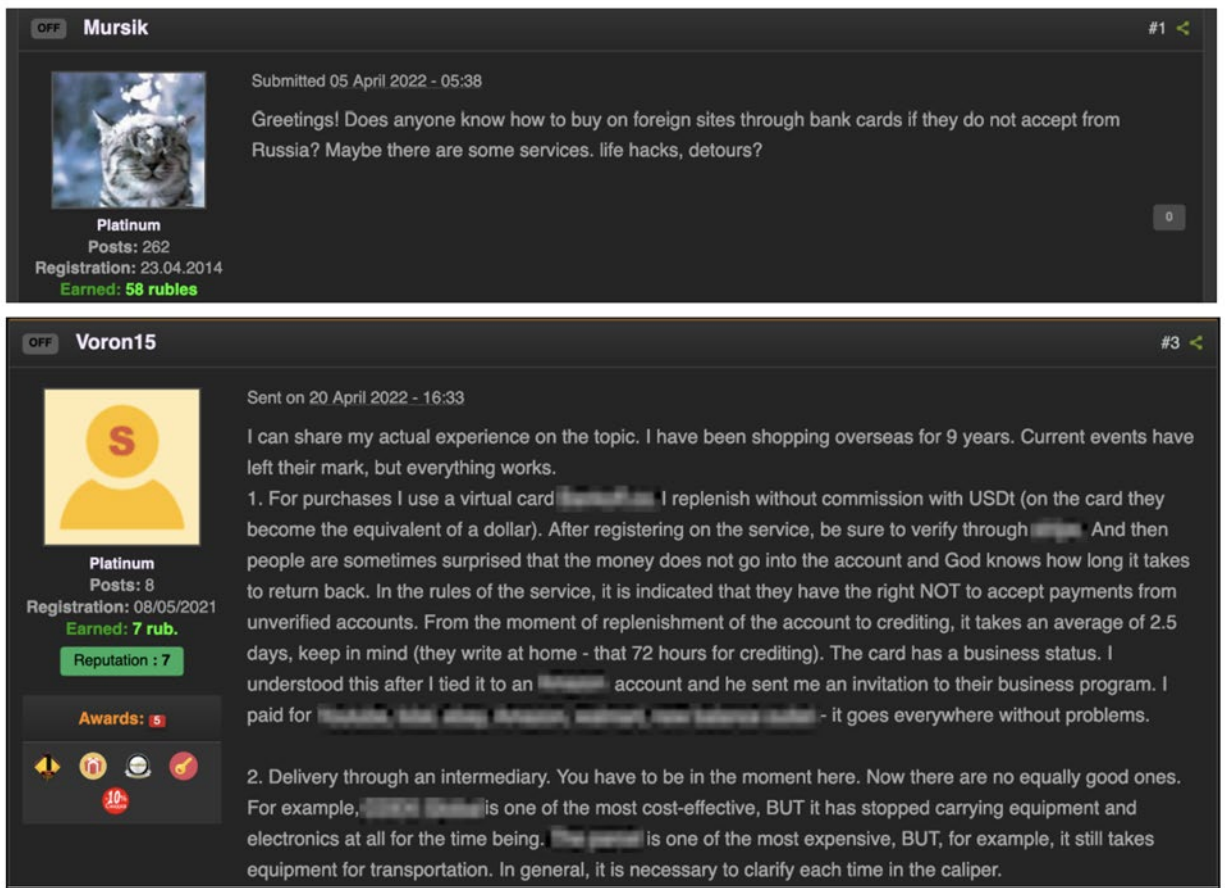


(Recorded Future Cyber Threat Analysis: Russia – Russian Sanctions Evasion Puts Merchants and Banks at Risk, Authored by Inskit Group – Figures 2 – 5)

These VCC services serve a dual function both for ordinary Russian consumers who seek to purchase international goods abroad, as well as those who intend to remain in a non-

attributable state for illicit or criminal purposes. Within this tradecraft model, there also exists the need to have the goods delivered. Thus, Russian entities will seek out mail forwarding services, also known as “re-shippers,” in the process of evading sanctions. Purchases made abroad can be delivered to a tax-free warehouse, where they are then repackaged and sent to Russia. An example of this can be found in the below exchange between two threat actors utilizing the dark web forum “Slivup.”

Example 2:



(Recorded Future Cyber Threat Analysis: Russia – *Russian Sanctions Evasion Puts Merchants and Banks at Risk*, Authored by Insikt Group – Figures 2 – 5)

Similar to VCC services, there are a variety of popular re-shipping services that exist which enable sanctions evasion practices. Given that the user-market for most cryptocurrency investors resides in peer-to-peer environments with minimal oversight or regulation, it is very easy for illicit actors to engage with one another and share leading services amongst their peers which maximize clandestine activity and naturally non-attributable tradecraft.²³

Russian Intelligence Services Leveraging Cryptocurrency for Operational Purposes

Due to the ability to facilitate clandestine payments through a variety of different tradecraft methods, cryptocurrency has been leveraged by not only Russian-based non-state actors and criminal groups, but also by state-sponsored Russian Government entities and intelligence services. On 9 June 2023, the US Department of Justice (DOJ), released a public statement detailing a variety of unsealed charges related to cryptocurrency exchange hacks, money laundering, and illicit activity conducted by multiple Russian threat actors, with direct ties to Russian intelligence services.

Russian nationals Alexey Bilyuchenko and Aleksandr Verner, were charged with conspiring to launder approximately 647,000 bitcoins over the course of a three-year period, following their hack of major cryptocurrency exchange, Mt. Gox, dating back to 2011. Per the recently unsealed indictment, it was revealed that in 2011, both Bilyuchenko and Verner gained access to Mt. Gox users' data, transactional database, and the private keys, which were necessary to facilitate all trading movement on the exchange. Between 2011 and 2014, approximately 647,000 bitcoin was moved out of Mt. Gox hosted wallets to other cryptocurrency exchanges, which included BTC-e and TradeHill. Additional assets were also moved to Bilyuchenko's and Verner's own Mt. Gox accounts. Notably, the exchange BTC-e was administratively run by Bilyuchenko up until it's shut down in 2017 by the FBI for illicit activity and money laundering on behalf of Russian-based ransomware gangs. Additional investigative reports unsealed by the Department of Homeland Security (DHS), reveal that Bilyuchenko and Verner moved the bitcoin from Mt. Gox to the exchange BTC-e at the time it was operational, after which it was further transitioned to two now-defunct bitcoin companies, *BitInstant* and *Memory Dealers*. BitInstant was a cryptocurrency exchange that was founded by Charlie Shrem, who in 2014, was sentenced to two years in prison for money laundering.

Between April and November 2012, both Bilyuchenko and Verner received \$2.5 million from BitInstant and Memory Dealers, to a bank account for a BTC-e affiliated shell company, *Canton Business Corporation*, which was registered in the Seychelles, a known tax haven and home to extensive financial crimes. Wire payments from BitInstant and Memory Dealers were labeled as "Internet Advertisement Agreements," despite BTC-e never providing a single advertising service to either entity. Additional tradecraft methods included sending money from their various bitcoin sales through multiple PayPal accounts, which would further conceal the true origin of the funds as they liquidated all of their stolen assets. Under the guise of advertisement contracts, Bilyuchenko and Verner made regular requests to the owner and operator of a Bitcoin Brokerage Service known as the *New York Bitcoin Broker* to make large wire transfers into various offshore bank accounts, all of which corresponded to various shell companies that were controlled by Bilyuchenko, Verner, and their co-conspirators. Between

March 2012 and April 2013, the New York Bitcoin Broker allegedly transferred more than \$6.6 million to overseas bank accounts which were directly controlled by Bilyuchenko, Verner, and their co-conspirators, in exchange for a “credit” on the BTC-e exchange. This method allowed them to operate completely undetected by law enforcement as they clandestinely liquidated millions of dollars from their hack of the Mt. Gox exchange.

Prior to its shutdown in 2017 by the FBI, BTC-e served over one million users worldwide and moved millions in both bitcoin deposits and withdrawals. BTC-e also served as the home to large quantities of funds associated with computer intrusions, hacking incidents, ransomware events, identity theft schemes, corrupt public officials and narcotics distribution rings. As one of the main administrators of BTC-e, Bilyuchenko worked closely with the primary operator, Alexander Vinnik, who was arrested in Greece during the 2017 FBI takedown of BTC-e. Immediately following Vinnik’s arrest, Bilyuchenko fled to Russia, where he used the database of former BTC-e users to launch the cryptocurrency exchange platform known as WEX. Bilyuchenko worked closely with the official owner and over-the-counter (OTC) cryptocurrency trader, Dmitri Vasilev, who later sold the exchange to Dmitri Khavchenko, a local Russian militia fighter with connections to the well-known Russian oligarch and sponsor of the pro-Russian separatist forces in the war in Ukraine, Konstantin Malofeev.

During the summer of 2018, Bilyuchenko entered into talks with Malofeev, who at the time was attempting to gain access to WEX’s user database for the purposes of launching a new cryptocurrency exchange which would be known as Vladex. According to an audiotape that was obtained by the news outlet BBC, Malofeev’s intentions were to open a “government-friendly” crypto exchange to be leveraged by the Kremlin. Malofeev was pressuring Bilyuchenko for the user data via a former Russian Federal Security Service (FSB) officer, alleged to be Anton Nemkin. The contents of this audio recording were verified by audiovisual forensic experts, in addition to Bilyuchenko confessing to law enforcement that he was forced to send all cryptocurrency in WEX hosted customer wallets to unnamed staffers of the FSB just before the exchange was shut down. Bilyuchenko also told law enforcement that two FSB Officers forced him to give them flash drives which contained all of the cryptocurrency belonging to WEX users and to transfer the assets to FSB hosted wallets. The assets totaled approximately \$450 million at the time. In order to facilitate the transfers, Bilyuchenko met with FSB officers on multiple occasions both in FSB buildings and at the Lotte hotel, located in the center of Moscow.⁴⁵⁶⁷

North Korea (DPRK)

In April 2023, the US Department of Treasury released their first risk assessment on decentralized finance systems (DeFi), of which cryptocurrency, digital assets and peer to peer trading networks were assessed as primary topics of concern. While these DeFi systems are

exploited by a variety of threat actors, to include ransomware actors, scammers, and various forms of cyber criminals, the Democratic People’s Republic of Korea (DPRK) was highlighted as a leading nation state which exploits DeFi systems for the purposes of laundering their illicit funds. One of the largest advantages offered to illicit cyber actors, specifically those working on behalf of the DPRK, is the ability to easily move funds through a variety of international exchange platforms which are not subject to KYC compliance, or they lack oversight elements which would require compliance and dictate reporting thresholds.⁸

The United States issued Bank Secrecy Act (BSA) requires that all US financial institutions assist the US Government in the detection and prevention of all potential illicit financial activity, such as money laundering. To date, the present legal framework has not clearly defined whether or not DeFi services would fall under BSA reporting guidelines as “financial institutions,” and thus be required by law to implement Anti-Money Laundering (AML) Programs, collect KYC-customer data, and report all suspicious activity to FinCEN. Consequently, there are many open vulnerabilities for illicit actors to exploit as a result of these regulatory “gray areas” when moving illicit funds, namely the DPRK.⁹

North Korea has globally established itself as a leading nation state in the illicit use of cryptocurrency, in the form of theft and sanctions evasion. In 2022 alone, the DPRK was responsible for stealing approximately \$1 billion+ in cryptocurrency from various organizations via the US-sanctioned state-sponsored hackers, Lazarus Group. Additionally, the United Nations Security Council (UNSC) recognized as early as 2019, that the DPRK was relying on an influx of illicit cyber operations for the purpose of targeting cryptocurrency exchanges to steal all available assets. The majority of these stolen assets are being used to directly fund North Korea’s weapons of mass destruction (WMD) and ballistic missile programs, which creates an immediate US national security concern.¹⁰¹¹

As recently as July 2023, South Korean Diplomatic Officials met with US private cybersecurity firms such as Mandiant and Blockchain analytics firm, Chainalysis, for the purposes of understanding DPRK’s tradecraft and assessing ways to disrupt these illicit operations. One of the primary tradecraft methods the group identified was that North Korean hackers in particular, prefer to exploit DeFi protocols by only leveraging peer-to-peer digital exchanges. DeFi exchange platforms allow users to transition between cryptocurrencies without the platform ever taking custody of the customer’s funds in order to facilitate the transition. This allows DPRK cyber actors to determine exactly when to transition stolen cryptocurrency from one type of cryptocurrency to another, enabling attribution to be more difficult to determine or even trace.¹²

DPRK cyber actors experience high rates of success in their tradecraft methods for a variety of reasons which set them apart from other adversarial nation states. As a country itself,

North Korea has minimal to non-existent financial advantages, and struggles to meet the standard of what the majority of the global village would consider to be “economically stable.” As a result, North Korea is not a heavily targeted state, due to a majority of the population living in an offline environment, within minimal to non-existent access to a computer. The entirety of North Korea’s access to any cyber element, resides solely with the government and intelligence services, which substantially increases career recruitment appeal for aspiring students. The DPRK aggressively recruits students who demonstrate a high aptitude to further build out the government’s cyber operations. Students of middle and high school age who display promising capabilities are encouraged to use computers while at school. Those who excel in mathematics are placed in specialized high schools, and the highest performing students are offered the opportunity to travel abroad to compete internationally and further hone their skills. Two colleges in Pyongyang; Kim Chaek University of Technology and Kim Il Sung University, actively recruit and admit the highest performers from North Korea’s specialized math and computer high schools, where they are then trained in advanced coding. In many instances, students representing these universities at international competitions are often outperforming students from American and Chinese universities, to include students from Harvard and Stanford University.¹³

The experience of these students is very unique in that they are directly trained and deployed under a fully operated government program. The most elite high school students are immediately sent to Moranbong University, where they undergo intense hacker-training through various programs that are fully run by the Reconnaissance General Bureau (RGB), North Korea’s primary spy agency. Upon their college graduation, most students are immediately assigned to the RGB’s Cyberwarfare Division, otherwise known as Department 121. Thus, North Korea is estimated to have approximately 6,800 very highly trained personnel throughout their various cyber programs which includes 1,700 highly skilled hackers spread throughout seven different units, and approximately 5,100 technical support personnel. After being fully vetted, cyber agents are sent to work abroad in order to advance DPRK cyber operations, often posing as freelance computer engineers or IT professionals. These individuals are presently operating and obtaining resources for their operations in China, Russia, Belarus, Singapore, Malaysia, as well as other South Asian countries. Given the extent of training the DPRK ensures their cyber agents undergo, they are highly adaptive to the fast-paced and clandestine environment that cryptocurrency offers. Additionally, due to their higher levels of skill, their risk tolerance is much higher, and they are able to effectively exploit “gray areas” of use for cryptocurrency that include legal and policy gaps which are not fully defined or understood by regulatory authorities, further increasing their rate of success.¹⁴

In stark contrast to other nation states, DPRK hackers are incredibly skilled at leveraging social engineering tactics for the purposes of breaching cryptocurrency wallets through

phishing attacks. They will look to target employees of online cryptocurrency exchanges and then lure their victims in through fake LinkedIn recruiting pages while impersonating employees of other legitimate IT companies, such as Lockheed Martin. Once they connect with their targets, they will transition their communication channels to a different messaging app such as WhatsApp, where they eventually entice them to download zip files that are allegedly related to legitimate work. These files contain malicious documents that lead to the execution of malware. This then allows them to back-end access their victim's network and ultimately gain access to the online exchange, after which they drain all of the available assets and transition them to various DPRK controlled wallets that are hosted on multiple exchanges, the majority of which do not adhere to any level of oversight or customer vetting.¹⁵

These individuals also excel in using a variety of illicit methods to avoid detection and ensure attribution is exceedingly difficult. They launder stolen funds through mixing services, which are often offered on cryptocurrency exchange platforms that do not employ KYC policies or AML regulations. Mixing services blend cryptocurrencies from many users together, in order to obfuscate the origin and owner of the funds. Due to cryptocurrencies such as Bitcoin, Ethereum and others maintaining public blockchains which allow for transparent activity, mixing services are most often used by illicit actors as a means of avoiding detection.¹⁶ Given that Bitcoin is one of the most liquid cryptocurrencies in circulation, the need for illicit actors such as the DPRK to leverage mixing services is often very high, as the end-state goal is to convert to a fiat currency as quickly as possible for the purposes of funding their missile programs. The DPRK is also very methodical in how they move their funds, often opting to move small amounts over longer periods of time to further avoid detection.¹⁷

These tactics can be seen in multiple exchange hacks associated with the DPRK's state-sponsored cyber crime group, the Lazarus Group. In April 2018, DPRK hackers compromised the cryptocurrency exchange, "Gate.io," which the CEO initially failed to publicly acknowledge. Gate.io was a formerly China-based cryptocurrency exchange, which has since been incorporated in the Cayman Islands. After the DPRK operative researched the CEO of the exchange to learn about the organization and potential vulnerabilities, an employee was eventually targeted through a phishing campaign. The employee received a link which they clicked and unknowingly downloaded a malicious file that granted the hackers access to the exchange's virtual wallet keys. Once the DPRK had access to the exchange, they successfully stole almost \$230 million in Bitcoin, Ethereum, Litecoin, and Dogecoin, among several other types of cryptocurrencies. In conjunction with two Chinese nationals, DPRK's Lazarus Group successfully laundered over \$100 million of these stolen funds by dispersing the assets between 113 different DPRK controlled cryptocurrency addresses located in Lazarus-affiliated wallets. The addresses and wallets were being hosted on multiple exchanges to avoid overloading only a handful of exchanges with large amounts of illicit funds, thereby raising suspicion of breaching

AML compliance. Additionally, a series of layering techniques were used through automation techniques that produced a large amount of transactions that were then split into complex patterns that involved transitioning between multiple cryptocurrencies, otherwise known as “peel-chaining,” before ultimately converting to fiat, which they leveraged external help for via two Chinese nationals who utilized over-the-counter (OTC) brokers to cash out.¹⁸

In September 2020, the Lazarus Group demonstrated a significant increase in their tradecraft and adaptability, following their successful hack of the KuCoin exchange. Although the exact point of intrusion and method of access is not publicly known, Lazarus Group hackers successfully gained access to all of the exchange’s wallet keys, which enabled them to steal and move the cryptocurrency. They then transitioned to laundering the funds through three separate mixing services: Wasabi Wallet, ChipMixer and Tornado Cash, a tactic they had not employed during the Gate.io hack. After mixing their stolen proceeds, the Lazarus Group transitioned the cryptocurrency to DeFi platforms, to further avoid detection. This decisive transition in tradecraft is a key indicator to how formidable the DPRK has become in their illicit use of cryptocurrency, as it demonstrates their high aptitude to determine regulatory weaknesses, and exploit them.¹⁹

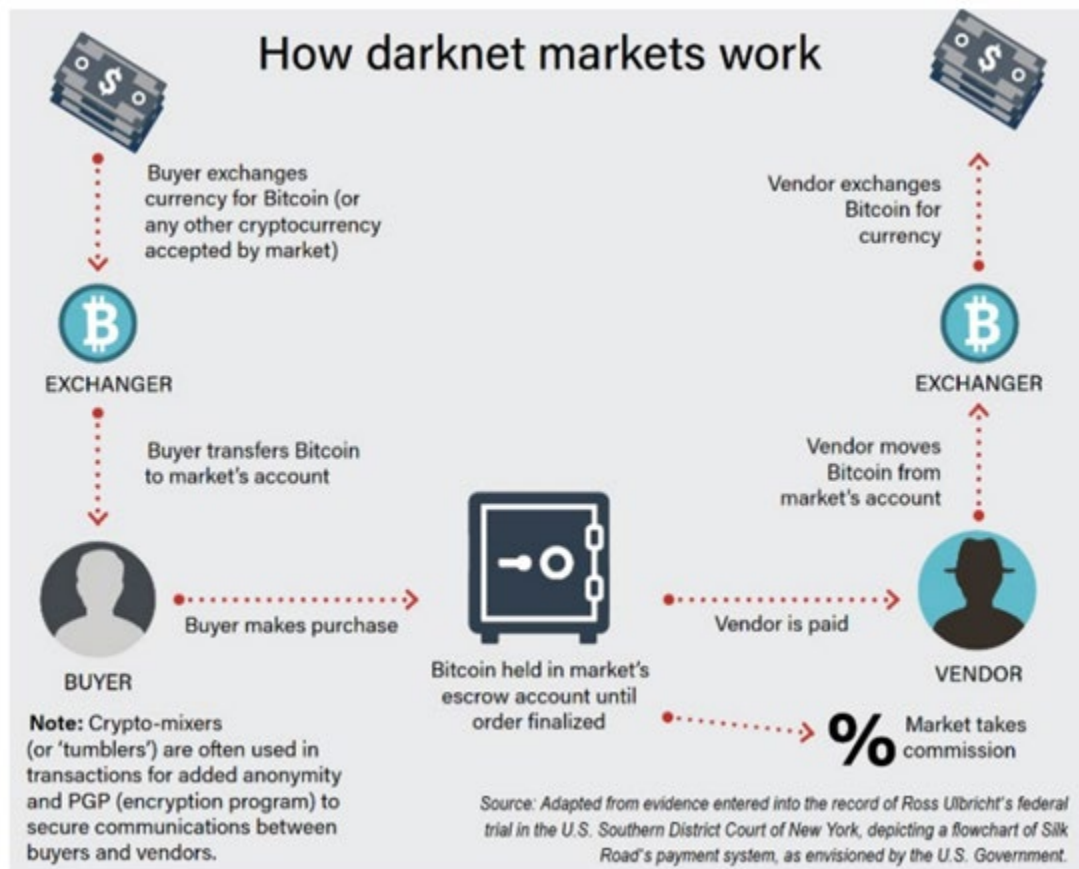
Cartel Finance

Mexican-based drug cartels have historically generated significant amounts of illicit proceeds through their global presence and narcotics distribution rings. A recently released report from the International Narcotics Control Board estimates that Mexican drug cartels are believed to launder approximately \$25 billion per year in Mexico. Subsequently, their need to conceal these proceeds and launder their funds is necessary to maintain the success of their operations. In April 2023, the FBI and DEA indicted twelve people associated with the Sinaloa cartel, a transnational criminal organization that allegedly laundered over \$16.5 million, a majority of which was moved via large bulk cash drops in hotel rooms and parking lots of various US cities to include Chicago, Boston, New York City, Baltimore, Philadelphia, among many others. The funds would then be laundered through multiple shell companies, after which they were ultimately transferred to bank accounts in Mexico. In a recent investigation led by the US Drug Enforcement Agency (DEA), it was determined that an illicit drug cartel was moving methamphetamine and cocaine across the US, Mexico, Europe, and Australia by leveraging the world’s largest cryptocurrency exchange, Binance. The group allegedly laundered over \$40 million in illicit proceeds via this exchange.²⁰²¹²²

Due to enhanced AML controls, and the shifting focus of law enforcement into these tradecraft methods, cartels such as the Sinaloa Cartel and Cartel de Jalisco Nueva Generacion (CJNG) are increasingly turning to small online purchases in bitcoin, to avoid being detected by

law enforcement. Similar to other adversarial nation state actors, these Mexican cartels are equally attracted to the speed of transactions and levels of anonymity cryptocurrencies offer. The ability to leverage cryptocurrencies also allows them to shift away from their historically complex tradecraft methods which often required using a series of large layering schemes, various shell companies, and significant amounts of large in-person bulk cash drops, all of which increases the level of risk of detection. After splitting the proceeds of their drug sales up into small amounts, these cartels will then buy a series of small amounts of bitcoin online, which allows them to further obscure the origin of their assets, as well as pay their international associates located throughout the world. Additionally, they will leverage illicit online vendors to sell illicit drugs. These websites will often advertise fentanyl-laced pills as Xanax, Adderall or Oxycodone. In most instances, those who purchase these drugs online are completely unaware they are ingesting fentanyl. These online vendors further enable false advertisement by allowing the cartels to use old recipes for synthetic narcotics which had previously stopped circulating due to their negative side effects. Overall, illicit online forums which accept virtual payment systems such as cryptocurrency, allow cartels to move narcotics more quickly and clandestinely, in conjunction with allowing them to double their product by cutting the drugs with a variety of other substances, all while falsely advertising them as pure.²³

In a recently released report from the United Nations Office on Drugs and Crime, it was determined that due to the increase in online trafficking of synthetic drugs, cryptocurrency has become the most preferred method of payment. Outside of the pseudo-anonymity they offer, cryptocurrencies also serve as the most common form of payment on darknet markets, where these drugs are frequently sold. While bitcoin is presently the most frequently used cryptocurrency due to its liquidity, the growth in use of anonymity enhancing coins (AEC) by illicit actors cannot be ignored.



(Source: United Nations Office on Drugs and Crime (UNDOC): *The Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribbean* – Figures 18)

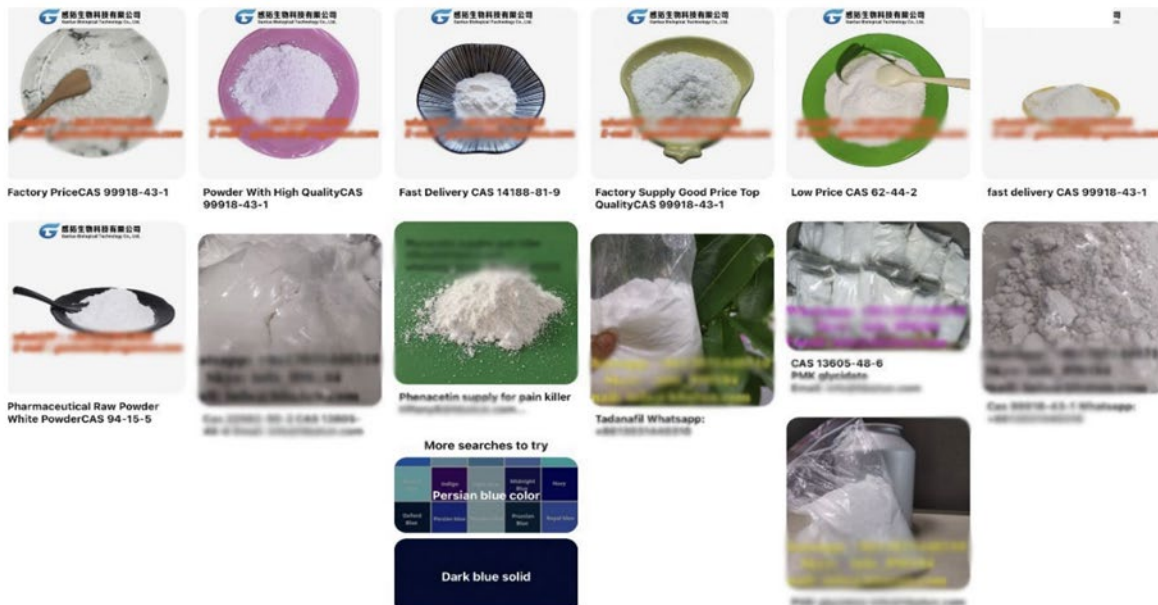
Due to its public blockchain, law enforcement entities are able to trace illicit financial movement in bitcoin by leveraging blockchain analytics tools such as Chainalysis, TRM Labs, and CipherTrace, among others. These analytic tools are a great aid to law enforcement investigations; however, limitations exist when criminal actors transition from bitcoin to an AEC. The primary limitation to this type of tradecraft is that AECs do not have public blockchains and therefore, their activity is not visible or in the majority of instances, completely untraceable. Despite the fact that the US employs a national law enforcement infrastructure that is capable of handling complex cases that employ various forms of money laundering tradecraft, law enforcement entities in Latin America and the Caribbean often lack those capabilities, and are unable to aid in the investigation of complex online drug trafficking marketplaces, specifically those that are hosted on the dark web.²⁴

One of the more recent national security concerns which has gained increasing prominence, is the sale and distribution of precursor chemicals in the making of synthetic

drugs. The clandestine laboratories where these drugs are being made can essentially be set up in any location without detection, as the logistics and resources needed to run them are minimal.

Mexican-based cartels are presently playing a very large role in the acquisition of precursor chemicals from China which are being used for the large-scale production of synthetic drugs. Producers of the precursor chemicals ship them from laboratories in China to cartels located in Columbia and Mexico, after which they are moved via air or sea onto their consumer base. The drugs will be passed off as food containers or other legal items. The two most dominant cartels of these illicit distribution practices are the Cartel de Jalisco Nueva Generacion (CJNG) and the Sinaloa Cartel, both of which are based in Mexico. The Sinaloa Cartel in particular, will pay off immigration officials in order to allow human mules carrying pills to travel across the borders and into the US without a formal inspection. These pills are then sold for \$3 each in New York or other major cities. Drug dealers located in the US are responsible for collecting the money, after which they will convert and deposit it into the cartel's bitcoin accounts that are managed from Mexico, where it is then converted into either US dollars or pesos. In some instances, these conversions are not even necessary, as Chinese dealers will often accept payments in cryptocurrency for the precursor chemicals.²⁵

These cartels also leverage dark web platforms for the purposes of negotiating shipments of precursor chemicals through legitimate air shipping services, or ocean containers that typically transit through airports or seaports that employ weaker controls. Similar to the DPRK, these cartels will utilize social media platforms such as Tinder, Telegram, and Grindr. They will also utilize open forums or blogs alongside darknet marketplaces for all phases of their trafficking and distribution rings. They have even used platforms such as "Pinterest" to publish fentanyl advertisements in Chinese or claim they have their own air shipping services. In many instances they will take advantage of corrupt border officials who are willing to accept kickback payments for the purposes of allowing the product to pass through inspection and into the target country for distribution.²⁶



Source: Web-IQ, dark web intelligence data extraction and analysis carried out on behalf of UNODC (2021).

(Source: United Nations Office on Drugs and Crime (UNODC): *The Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribbean* – Figures 3)

Between July 2019 and June 2020, approximately \$25 billion in cryptocurrency moved through Latin American and Caribbean countries, 26% of which originated from darknet market transactions. These numbers are expected to steadily increase over time, as the advantages of AEC’s become more well known and understood by cartels and organized crime groups. Buyers will typically communicate with cartel vendors via encrypted chat forums, where the agreed upon payment method is discussed. Bitcoin is the most popular cryptocurrency accepted due to liquidity; however, LiteCoin is also frequently seen. AEC’s or privacy coins, are being more heavily leveraged due to anonymity and natural advantages in obfuscation techniques. In the below indicated chart, cryptocurrencies such as Monero, Z-Cash and Dash, can be seen on a variety of darknet marketplaces as the preferred method of payment for opioids and other synthetic drugs. These cryptocurrencies are the most prominent AEC’s, which are also referred to as privacy coins, due to the complete inability for law enforcement entities to trace activity related to them.²⁷

Market [1]	Start date	Current status [2]	End date	Cause	Supported cryptocurrencies [3]	Fentanyl banned? [4]	Total drugs advertisements	Drugs ads shipping from LatAm [5]	Drugs ads not shipping from LatAm [5]	Total opioids advertisements	Opioids ads shipping from LatAm	All vendors shipping from LatAm
Dream Market	15/Nov/13	Offline	01/May/19	Voluntary	BTC	yes	312147	678	311469	27169	45	76
Darkbay Market	03/Sep/19	Offline	01/Jul/20	Unknown	BTC, LTC, XMR	no	59978	281	59697	8609	24	44
AlphaBay Market	01/Sep/14	Offline	04/Jul/17	Seized by LE	BTC, XMR, ZEC, ETH	unknown	113559	497	113062	10724	23	139
Zion Market	01/Dec/16	Offline	17/May/18	Exit scam	BTC, XMR	unknown	9269	15	9254	575	9	2
Wallstreet Market	01/Oct/16	Offline	01/Mar/19	Seized by LE	BTC, XMR	no	20312	80	20232	1967	4	55
RSCub Market	31/Mar/15	Offline	01/Dec/17	Voluntary	BTC	unknown	2294	8	2286	153	1	4
Cryptonia	06/Oct/18	Offline	23/Nov/19	Exit scam	BTC, XMR	yes	20674	18	20656	1328	1	6
Grey Market	01/Jul/19	Offline	01/Dec/19	Exit scam	BTC, XMR	yes	4953	34	4919	513	1	8
Icarus Market	26/Mar/20	Offline	09/Sep/20	Probably exit scam	BTC, LTC, XMR	unknown	3771	44	3727	170	1	6
Apollo Market	16/Mar/18	Offline	22/Jan/20	Exit scam	BTC, LTC, XMR, BCH	unknown	3744	19	3725	257	1	7
Yellow Brick Market	18/Feb/19	Offline	09/Jan/21	Exit scam	BTC, LTC, XMR	unknown	753	0	753	82	0	1
Avaris Market	18/Oct/19	Offline	09/Mar/20	Exit scam	BTC, XMR	unknown	267	1	266	9	0	1
Berkusconi Market	01/Jan/16	Offline	27/Sep/19	Seized by LE	BTC, LTC, XMR	unknown	25659	2	25657	1891	0	3
Agora Reloaded	08/Nov/17	Offline	01/Jan/18	Probably hacked	BTC	unknown	4218	2	4216	378	0	2
Square Market	13/Feb/20	Offline	01/Sep/20	Exit scam	BTC, XMR, ZEC	unknown	3981	2	3979	351	0	1
DeepSea	08/Apr/20	Offline	14/Oct/20	Exit scam	BTC, XMR	unknown	1474	2	1472	131	0	1
Genesis Market	01/May/19	Offline	24/Aug/19	Exit scam	BTC	yes	1972	4	1968	159	0	1
Nightmare Market	01/Oct/18	Offline	24/Nov/19	Exit scam	BTC, XMR, LTC, ZEC, DASH, BCH	yes	6803	5	6798	589	0	7
Bitbazaar	20/Feb/20	Offline	14/Jan/20	Exit scam	BTC, LTC, XMR	unknown	1904	5	1899	163	0	2
Libertas Market	14/Oct/17	Offline	19/Jun/19	Voluntary	XMR	unknown	921	6	915	61	0	3
SamSara Market	06/Jul/19	Offline	09/Nov/19	Exit scam	BTC	unknown	13033	8	13025	1102	0	3
Europa Market	25/Feb/20	Offline	20/May/20	Exit scam	BTC	unknown	275	8	267	36	0	3

(Source: on Drugs and Crime (UNDOC): *The Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribbean* – Figure 19)

Once the cartels or organized crime groups receive the cryptocurrency, they will use mixing services in order to further obfuscate the ability to be traced. Cartels also take advantage of the minimal regulatory oversight on cryptocurrency exchange platforms, or peer-to-peer trading platforms when moving their illicit proceeds. At present, AEC's that are mixed via a mixing service or tumbler, are completely impossible to trace or determine the ultimate beneficial owner of after the fact. Should this tradecraft model be scaled throughout criminal communities to launder illicit proceeds, the US will be facing a significant national security concern.²⁸

Terrorist Financing

Terrorist organizations rely on a consistent influx of funds in order to carry out and plan their operations. Historically, they have leveraged donations and the religious obligation of tithe in order to raise money. Other forms of revenue generation include illegal drug and arms dealing, with a combined need to finance their own members and associates. In recent years, this tradecraft has shifted to a reliance on cryptocurrency for fundraising, financing attacks, purchasing equipment, supporting fighters and their families, among other purposes. Jihadi blogs alone, have become the source of millions of dollars in bitcoin in the form of donations to ISIS, Al-Qaeda, Hamas, and the Muslim Brotherhood. In conjunction with all the aforementioned threat actors, these groups also significantly leverage social media platforms for the purpose of soliciting donations from their followers. They will utilize communication platforms such as the messaging app Telegram, which allows for encrypted and clandestine messaging. They will utilize Facebook and Twitter for the purposes of posting their wallet addresses to receive donations, as well as provide their supporting base with PDF and video

guides for how to obtain, and donate cryptocurrency. Bitcoin is the most frequently used due to liquidity, alongside AEC's such as Monero, Z-Cash and Dash, among others.²⁹³⁰³¹

In a recent report released by the United Nations, it was determined that the growing use of cryptocurrencies is now attributed to approximately 20% of all terrorist attacks. As of 2021, it was further estimated that the terrorist organization Hamas had raised almost \$1 million in cryptocurrency donations for the purpose of their military campaigns, which is more than any other terrorist organization to date. As such, the Israeli government began seizing these accounts in an effort to mitigate the issue.³²

In contrast to other adversarial actors, terrorist organizations are not leveraging highly complex money laundering tactics in order to move illicit proceeds; rather, cryptocurrency is serving as a source of revenue generation for the purpose of financing their attacks and carrying out their operations, much of which stems from donations. Outside of standard social media applications and platforms, these groups with also utilized the darknet and create pages such as *"Fund the Islamic Struggle without Leaving a Trace,"* which is a darknet site specifically used to raise and transfer bitcoin to jihadi fighters. Additionally, Islamic law has adapted to allow cryptocurrency to become part of the mainstream financial system, as well as legal tender, despite technology limitations and lack of cryptocurrency ATM's throughout the Middle East. Terrorist groups such as the Islamic Sate have carried out kidnappings and mandated that ransom payments only be made in bitcoin. The COVID-19 era also witnessed a stark shift in terrorist organization funding efforts in cryptocurrency. Multiple terrorist organizations used this global crisis to generate illegal profits by forging medical supplies and fraudulently selling them in exchange for cryptocurrency.³³

Terrorist organizations are limited in comparison to other threat actors due to the lack of technology infrastructure and subsequently, do not employ highly complex laundering schemes; however, their ability to leverage clandestine communication platforms on the darknet, as well as fundraise through various sources, with an emphasis on AEC use, poses a significant national security threat.

Growth and Capacity of Criminal Groups Engaging in Illicit Digital Asset Activity

Successful cybercriminal efforts require personnel and money to operate, similar to any legitimate small or large business. Examining the recruitment tools and composition of groups can provide insight to how illicit cryptocurrency groups maintain or grow their operations. There are many criminal groups that fund their operations through digital currencies. Ransomware operators have the ability to not only halt business operations and prevent access

to a company's network until a ransom is paid. However, after paying a ransom, companies are often forced to pay to restore their systems. Additionally, as evident in the Colonial Pipeline attack, ransomware attacks have the ability to impact economies. Scams have the ability to trick individuals into investing thousands of dollars and upending lives.

Ransomware

Ransomware has grown exponentially in recent years, both in the number of attacks and money extorted. Ransomware will likely remain a long term threat to organizations as hackers continue to identify vulnerabilities in networks and develop exploits to deploy ransomware. As successful ransomware attacks have the potential to fetch multi-million dollar payouts, many ransomware groups run their criminal operations similar to operations of legitimate businesses. The anti-virus company Kaspersky outlined the standard structure of ransomware groups, identifying several positions including the manager, or lead, who is responsible for managing the team, recruitment efforts, and interactions with customers. Ransomware groups may also have several positions reporting to the "manager" that include:

- Analyst: Responsible for gathering information and attack planning processes
- Developer: Create malware and ransomware tools
- Attacker: Perform the initial infrastructure compromise and attack development
- Reverse engineer: Responsible for create and operation of new tools
- Designer: creates fake websites and phishing emails
- Tester (or Pentester): Debugs malware and evades protective measures
- IT Administrator: Configures and maintains the group's IT infrastructure.

Ransomware groups gain and lose employees like any legitimate business, and need to advertise vacancies that arise. Dark web and hacker forms serve as the most robust venue for ransomware group recruitment, where both well-established and lesser known ransomware groups advertise their needs. Kaspersky analyzed 200,000 posts on 151 dark web employment advertisements between January 2020 and June 2022 and found 61 percent of the postings were for developers, while pentesters and developers accounted for 26 percent of the jobs. Kaspersky noted that employers on the dark web used competitive offers to attract top tier applicants, and offered telework, full-time employment, and flextime, and even paid sick leave and an employee referral plan. However, as the size and level of expertise varies among ransomware groups, more established ransomware groups are more likely to model Kaspersky's findings while newer and less established ransomware groups may only have one or two people operating at the center and advertise for positions or ad-hoc work as needed.

One journalist detailed the interview process after responding to an advertisement for a ransomware affiliate posted in an hacker forum. Upon successfully securing an interview, the

journalist learned the ransomware group offered 70 to 80 percent of a successful ransom payment divided equally among the affiliates, while the primary members of the ransomware group kept the other 20 to 30 percent. Additionally, the payout rates were dependent on the number of successful ransom operations or the amount ransomed (i.e. the more successfully executed ransoms the higher the payout or if a successful ransom resulted in a large sum the payout would be higher.) Additionally, the ransomware group deposited \$1 million worth of Bitcoin into the forum’s wallet to validate the legitimacy of the job posting. However, the journalists found one requirement: the potential affiliate had to be a native Russian speaker and quizzed them about Russian trivia and history.

More prominent and larger ransomware groups may operate webpages similar to legitimate organization’s public facing sites. The larger groups publish news of their victims, history, and contact details, and may have a “Contact Us” section allowing applicants to contact the group. Many of these groups’ pages are .onion sites and are unavailable on the surface web, and therefore post on forums.

Other ransomware groups may operate on a smaller scale with a ransomware-as-a-service (RaaS) model. In the RaaS model, developers of a ransomware variant allow affiliates to use their ransomware to execute attacks in exchange for a percentage of the profits. This affords ransomware affiliates the ability to have multiple ransomware variants at their disposal to execute ransomware operations. Additionally, it’s plausible to have a ransomware group that has a small number of core members and advertises for affiliates to assist in breaking into a targeted company with a promise of a cut of the profits. Additionally, larger ransomware groups may operate with a smaller number of core members making other positions more disposable. Both models create highly fluid groups.

Despite the size of a ransomware group, the industry has frequent employee turnover and therefore requires continuous recruitment efforts. More prominent ransomware groups likely have the finances and reputation that affords them the luxury of applicants seeking out employment and may not have to rely on proactive recruitment. However, larger groups are not immune to “splintering” and may occasionally return to darknet forums to advertise for new members. Smaller and less established ransomware groups are likely more dependent on darknet forums for recruitment of affiliates. Consequently, at some point or another, ransomware groups and affiliates will depend on darknet and hacker forums for recruitment purposes. Less frequent actions by ransomware groups in leveraging a witting insider within a company for to gain access, rewarding the insider with a hefty payment.³⁴³⁵

Scams

Scams accounted for billions of dollars in revenue in 2022. The blockchain analysis firm Chainalysis reported crypto scam revenue for 2022 totaled \$5.9 billion. However, this number is likely much larger as this type of activity is traditionally underreported. There are many types of scams, all of which have the goal of deceiving people. Investment scams, romance scams, giveaway scams, NFT scams, and impersonations scams were all included in the *Chainalysis 2023 Cryptocrime Report*. Information from law enforcement interdiction in scams seems to show both large and small scaled operations. Larger scams seem to operate similarly to a legitimate large-scale business, employing several people with outlined rates of pay or commissions. Larger scam operators have established processes, often operating internationally in several countries. It is plausible that larger scam operations establish each part of their operation in countries, benefitting from laws that may afford them less scrutiny. These larger scam organizations also operate fake websites or mobile applications that victims can access to “see” their money.³⁶

Law enforcement uncovered activities of the Ukraine-based company Milton Group, which operated both regulated and unregulated investment companies. Milton Group scammers promoted investment opportunities with high rates of return for a few hundred dollars investment worth of Bitcoin. One of the Milton Group’s companies, EverFX was regulated by the UK’s Financial Conduct Authority, and even sponsored a well-known European football team. When Milton Group suggested scam victims invest with EverFX, the scammers would claim the investments were performing poorly and convince victims to transfer their money to unregulated off-shore investment companies operated by the Milton Group. Once funds were transferred, victims were no longer entitled to protections offered by regulated firms and lost even more money.

The Milton Group was estimated to employ 200 people. The scammers made efforts to avoid U.S. citizens as not to attract attention of the FBI. Operators’ income was commission-based, with credit card transactions yielding a four percent commission; transactions through wire transfer services, like Western Union or Moneygram, resulting in a six percent commission; and transactions through cryptocurrencies garnering nine percent. (<https://ain.capital/2020/03/03/milton-group-investigation/>) It is likely cryptocurrency transactions resulted in the highest commission rates as cryptocurrency is the most difficult means to recover.

European authorities also dismantled a cryptocurrency scam in early 2023. This scam ran operations in Serbia, Cyprus, and Bulgaria, and defrauded victims in Europe, Australia, and Canada. Over 250 group members were identified. They operated call centers in Serbia,

maintained its network infrastructure in Bulgaria, and used Cyprus as its base for laundering activities.³⁷ Scammers used social media to advertise promising investment opportunities with great returns.³⁸

Additionally, Spanish police dismantled a large cryptocurrency fraud operation in April 2023 discovering multiple people in Azerbaijan, Georgia, Russia, and Israel received from funds from the scam that resulted in \$100 million in victims' lost investments. Victims, who were promised high returns without any risk, were lured to invest in the scam through aggressive marketing through websites, as well as phone calls, messages, and advertisements in newspapers. The scammers used a website that depicted false data and graphics of victims' investments, ultimately encouraging further investments.³⁹

Law enforcement has also taken action against individuals and small groups involved in cryptocurrency scams. The FBI arrested two individuals in late 2022 with the help of Turkish authorities for luring victims into fraudulent equipment rental contracts with a cryptocurrency mining service and caused victims to invest in a fake virtual currency bank.⁴⁰ Additionally, an individual in Miami, Florida was arrested in early 2023 for operating a fraudulent cryptocurrency and stock investment scheme.⁴¹

Like many illicit activities, cryptocurrency scams require personnel to operate; however, there is minimal information regarding the methods cryptocurrency scam operations use to recruit employees. The smaller scams outlined were comprised of a small number of individuals, so recruitment is likely not a factor that would impede the scam. However, data from large cryptocurrency scam networks dismantled by law enforcement reveal scams were comprised of hundreds of employees and operate as a business. These larger scam operations are likely dependent on recruitment to maintain or grow operations. Cryptocurrency scam recruitment and retention of employees may be an unexamined issue for two primary reasons:

1. Cryptocurrency scams impact individuals and therefore do not have the same level of impact as attacks like ransomware. While both ransomware attacks and cryptocurrency scams impact individuals, ransomware attacks have the ability to impact business operations and the global economy. The Colonial Pipeline attack resulted in the company halting oil production for five days and created uncertainty in oil availability and prices. Due to the large impact of ransomware operations law enforcement, cryptocurrency exchanges, and other elements that monitor illicit cryptocurrency use likely focus more efforts towards the structure and recruitment of ransomware operations vice cryptocurrency scams.

2. Cryptocurrency recruitment may be difficult to track because it is plausible cryptocurrency scams use legitimate recruitment platforms. Cryptocurrency scams are successful because they have the façade of a legal framework, using recognized social media sites and print platforms to attract victims. Therefore, it's plausible scam operators also use these same mechanisms to advertise and recruit employees.

Cryptocurrency Point-of-Sales

Growth of the Market

Although often considered a “niche” sector of the cryptocurrency industry, Cryptocurrency Point-Of-Sale Products, often referred to as Bitcoin ATMs, Bitcoin Point-Of Sale, Crypto Kiosks, or BTMs, have seen a drastic increase in popularity since 2020. According to coinatmradar.com, since January 2020 Bitcoin ATMs in the United States have increased from approximately 4,200 locations to over 29,000 locations in May 2023, with the height of prevalence occurring in the third quarter of 2022 where there were over 34,000 Bitcoin ATMs in the United States. In addition to the Bitcoin ATMs, which are physical machines placed in location solely for the purpose of converting fiat into cryptocurrency, and sometimes vice versa, there are also tens of thousands of other services offered at retail stores around the country that allow individuals to quickly convert fiat currency into cryptocurrency. Examples of these services include [BDCheckout⁴²](#), offered by Bitcoin ATM provider Bitcoin Depot, which has roughly 10,000 locations and [LibertyX \(libertyx.com/\)](https://libertyx.com/), which allows individuals to purchase crypto at over 20,000 retail locations around the country.⁴³

As of May 2023, the United States has approximately 85% of all the market for active Bitcoin ATMs, however, this does not tell the entire story of how the United States is the main driver for industry grown related Bitcoin ATMs. A review of the next two biggest markets, Canada and Australia, shows that a large portion of those Bitcoin ATMs are operated by companies such as Coinflip (through Olliv), Bitcoin Depot, and LocalBitcoins, which are either headquartered in the United States or have a large domestic presence. Additionally, expanding markets such as Puerto Rico, El Salvador, and Colombia are partially driven by US based companies such as Athena and BitStop.

A Change in Landscape

In 2013, when the first Bitcoin ATM was launched in Vancouver⁴⁴, the business model was simple: provide a physical location where fiat currency could be quickly converted into BTC and vice versa. However, over the last decade, the services offered by these machines, and the

companies operating them, have greatly increased. A cursory review of the top 10 operators in the United States shows that individuals are able to quickly purchase dozens of cryptocurrencies and tokens. These include BTC, LTC, ETH, DASH, DOGE, XPR, and USDT. Additionally, at at least two operators customers can purchase the privacy coin ZCash and at least one operator customers can purchase the privacy coin Monero. Furthermore, fiat to crypto has slowly morphed into “value” for crypto with thousands of machines allowing individuals to purchase with debit cards and credit cards at the machine and even prepaid cards.⁴⁵

Also, the physical machines, while still prevalent, have been supplemented with “behind the counter solutions” which are offered by companies such as DigitalMint, Bitcoin Depot, CryptoDispensers, and Libertyx. At these locations a customer is able to purchase cryptocurrency through a teller app⁴⁶ or prepaid “voucher” system⁴⁷, instead of at a physical machine.

Finally, operators have increasingly expanded into non-physical location products. For instance, companies have started offering OTC (over-the-counter) trading desks, which allow customers to interact with Bitcoin ATM providers using wires instead of cash to purchase cryptocurrency. Often these transactions have higher limits with some providers stating there is no maximum transaction limit for OTC transactions. Another example of the expansion to non-physical location transaction models is the new debit-to-crypto online transaction type offered by companies such as CoinCloud.⁴⁸ Similar to the in-person debit to crypto model, this transaction model allows customers to purchase cryptocurrency online from a Bitcoin ATM operator using a debit or credit card.

Controlling the Growth

With the large scale expansion of the Bitcoin ATM industry there have been numerous regulatory responses on both a federal and state level. On an international level the responses range from El Salvador, where the Nation worked to help install Bitcoin ATMs in the country (<https://www.reuters.com/technology/athena-says-will-install-1500-cryptocurrency-atms-el-salvador-2021-06-25/>) all the way to the United Kingdom where, in 2022, stated that no Bitcoin ATMs were legally operating in the country⁴⁹, a stance that have continued to take through 2023.

In the United States all Bitcoin ATM operators are required to be registered with FinCEN as a money services business (MSB) which means that all operators are required to have a BSA Officer, have a full compliance program, training for their staff on AML obligations, and an independent exam. Additionally, as part of these requirements, Bitcoin ATM providers are required to have know-your-customer (KYC) policies in place and are required to file Suspicious

Activity Reports (SAR) when illicit or fraudulent activity is suspected. Furthermore, states such as New York, with the “Bitlicense”, or Washington with its inclusion of BTMs in its traditional money transmission license, have required any Bitcoin ATM provider to register with the State and prove an effective AML, consumer protection program, and cyber security program prior to entering the State. Additionally, as with other more traditional money service businesses, these programs may be subjected to examinations of their programs to confirm adherence to policies and the effectiveness of the policies themselves.

However, even with the regulatory requirements and certain jurisdictions making the operation of a BTM illegal, new locations are continuously being opened around the United States and companies such as Genesis Coin have even announced operations in over 10 jurisdictions.⁵⁰

The Intersection Of Mass Appeal And Nefarious Actors

The cryptocurrency ATM industry, at its core, was designed to allow anyone to buy cryptocurrency in a convenient manner. The goal of the industry, as stated by numerous representatives of the cash-to-crypto industry, is to have a location on every street corner and in every store so that if an individual wants to quickly gain access to the cryptocurrency ecosystem they can. Over time, as questions started to arise as to why cryptocurrency point of sale options existed, the narrative of the industry shifted to show how these products were helping the underserved communities who may not have access to traditional financial products. A cursory review of mission statements provided by leading cryptocurrency ATM companies shows that the goal of the organization is to help the “unbanked” or “underbanked”.

However, as stated in a November 2022 article by Bloomberg, roughly \$349 million was spent at Bitcoin ATMs in January 2021.⁵¹ With so much being spent at ATMs around the world, the question around whether or not these profits are being driven by underbanked populations and individuals trying to conveniently purchase cryptocurrency arises. Unfortunately, per research conducted by leading blockchain forensic firms TRM Labs and Chainalysis, a noticeable portion of funds leaving cash-to-crypto locations in the United States are going to nefarious destinations. Chainalysis, per its *2023 Cryptocurrency Crime Report*⁵² found that over \$67 million was sent from ATMs to addresses known to be affiliated with scam victimization, while TRM Labs found that customers from 40 different domestic cash-to-crypto companies sent to known fraud wallet in 2022.⁵³ Additionally, per the Chainalysis report, over 75% of all illicit activity moving through ATMs ultimately ends up in wallets related to darkmarket shops or stolen credit card shops. Furthermore, as wallet attribution related to illicit activity (especially

fraud victimization) is often limited, the actual volume of transaction related to these nefarious use cases is potentially substantially higher than stated in the reports.

These services are appealing tools to conduct nefarious activity such as purchasing of stolen credentials on a dark market place, or convincing a scam victim to remit funds to a scammer. Their appeal is due to their availability, potential lack of institutional controls, and the number of independent companies operating in the United States.

TRM Labs has confirmed there are at least 40 different companies in the United States offering cash-to-crypto services. Those operating in the United States as a BTM are required to have an effective AML program designed to detect illicit activity, as well as, controls in place to prevent the use of the operator's machines for the purpose of scam victimization. Companies are told to take a "risk-based approach" when it comes to designing these programs. The controls in place to mitigate fraud and illicit activity then create areas which bad actors can exploit. For instance, the level in which Know-Your-Customer ("KYC") information is collected and validated differs between organizations. A review of the transaction limits found by operators marketing on coinatmradar.com shows that individuals can purchase anywhere from no bitcoin to over \$2,000 at one time with just a phone number on file. Additionally, customers willing to provide an ID on file can purchase in the range of \$2,000 to \$9,999 in a single day. Finally, should a customer provide their social security number, they may be able to purchase over \$25,000 in a single day. While these ranges are substantial, as each program has taken a risk based approach and is using various tools to validate IDs, cross reference phone numbers to identities, and confirming the authenticity of the other documents provided, it can be argued by all BTM providers that the KYC and risk-based limits in place are in line with the required regulation.

In tandem with the KYC onboarding process, a Bitcoin ATM company may implement a risk-based enhanced due diligence program designed to better understand customers who appear to be high-risk. Although not exclusively a fraud prevention control, by attempting to better understand a customer's reason for purchasing cryptocurrency and how they are funding the purchases there is also the potential to identify red flags related to illicit activity or fraud victimization. Yet, just as it was with the KYC controls, the volume of transactions, transaction patterns, and other red flags in which additional information would be collected varies based on each provider. Additionally, responses to these red flags may range from terminating the relationship with the customer, filing a Suspicious Activity Report while letting the customer continue transacting, or simply warning the customer of risks associated with the transaction.

As these controls vary, for a scammer trying to attempt to get a victim to send them money for "investment" or for "legal fees" Bitcoin ATMs offer an easy way to quickly have a victim remit a large amount of funds. Using Indianapolis, Indiana as an example, if a victim was

to be contacted by a scammer and was convinced that they needed to send cryptocurrency quickly for an urgent purpose, at a minimum the victim would have 12 operators within the city limits to use for this purpose. Review of these operators, using the information provided on coinatmradar.com, shows that, on average, an individual could purchase \$3,000 at each operator by providing their government issued ID. What this equates to is a victim potentially being able to purchase over \$30,000 in crypto in a single day by just traveling a small distance between independent operators. Additionally, as all of these operators have higher limits, with some being over \$40,000 in a day, should a customer want to provide additional information such as a social security number or documentation of source of funding the potential for an individual to lose a lot more money quickly is present. Furthermore, if operators do not require enhanced due diligence on customers until a certain timeframe or transaction volume has passed, a customer can continue with the large volume purchases for numerous days or even months. With stories such as the ones posted by the Detroit Free Press in September 2022⁵⁴ where a couple in Michigan was convinced to send a scammer \$350,000 in bitcoin as a result of an IT Impersonation scam or the CT Insider article from My 2023⁵⁵ where an individual lost over \$20,000 through a Bitcoin ATM as the result of a fake check deposit scam, this threat of of a customer losing thousands, or even hundreds of thousands of dollars is very real.

As the use of blockchain forensic tools such as Chainalysis, TRM Labs, Elliptic, Blockchain Intelligence Group, and Ciphertrace continue to grow, the use of these companies' capabilities is being built into Bitcoin ATM company's AML programs. However, as with the KYC and EDD controls above, the totality of these tools use in programs varies as well. For instance an AML program can decide to use pre-screen all wallets prior to transacting which would prevent the remittance of funds to a nefarious party or for an illicit purpose, to using the tools to generate "AML alerts" which would notify a company of an unusual transaction or pattern, to just using the tool as an investigative technique after a customer has been identified to red flags elsewhere. Mixing this range of blockchain forensic use with the variety of KYC and EDD controls examined above, the appeal for using these machines for illicit activity, such as dark market purchases is apparent.

Returning to Indianapolis, Indiana as an example again, a review of the same 12 operators shows that the ability to purchase up to roughly \$900 with only a working phone number and self provided name on file is a common trend. Per a report by NordVPN, in which the VPN service analyzed over 4,000,000 payments to stolen credit card marketplaces, the average stolen credential costs under \$10.⁵⁶ Now, although Bitcoin ATM companies have repeatedly shown to use software that validates identities related to phone numbers or software that rejects the use of Voice-Over-IP (VOIP) phone numbers, the lessened risk of attempting a transaction with a potentially obfuscated identity attached to a phone number could be seen as an appealing option for nefarious actors. Additionally, even if an operator was

to require a valid ID on file prior to transacting or were to cross-reference phone numbers to ID information using a third party, the attraction for using Bitcoin ATMs for illicit activity still exists. As most Bitcoin ATMs allow for onboarding at the machine and just require a phone number and established PIN for further use of the machine, a nefarious actor could present a valid, albeit stolen ID, to onboard or could use an established account created by an acquaintance to go unidentified while conducting illicit transactions.

After a customer has onboarded, the transaction itself may pose less risk to a nefarious actor than other financial products. Although the use of blockchain forensic tools is becoming industry standard in the cryptocurrency point-of-sale industry, as stated above there is still disparity in how they are used amongst industry competitors. Should a company only use blockchain forensics after a customer has been identified through the detection of other red flags, then it is unlikely that periodic small dollar deposits would trigger an investigation into the activity that would uncover the illicit activity. Additionally, if a customer solely uses prescreening of wallets, the use of intermediary wallets between the initial transaction and a dark market site would circumvent these controls. Finally, should a customer be fully prevented from transacting at a Bitcoin ATM due to pre-screening or account termination, the ability to quickly shift to another operator, due to the large number of operators in most areas, and maintain purchases of illicit goods, still exists.

Moves To Change The Reputation

As more and more negative media coverage surrounds the Bitcoin ATM industry it is apparent that the industry needs to adjust its approach to scam victimization and illicit activity in order to continue on its mission to provide access to cryptocurrency on every street corner and to all unbanked communities. Until clear industry standards on fraud controls, use of blockchain forensic tools, KYC regulations, and other aspects of an operators AML/BSA program are established, nefarious actors will still be able to use preferred operators to engage in illicit activity and scammers will still be able to utilize the sheer size of the industry to their advantage. With States like Connecticut⁵⁷ and California⁵⁸ both raising potential bills related to Bitcoin ATMs and fraud prevention, it is clear that States believe further requirements and expectations for the industry are needed.

However, this is not to say that actions taken by operators recently have not suggested a deliberate attempt to improve the industry's abilities to prevent the very activity that has given it a negative reputation. For instance, utilization of tools such as Chainabuse.com or Chainalysis Reactor Community Feature by operators have allowed them to quickly identify potential fraud before it occurs and allowed them to assist in the prevention of further victimization. Additionally, recent trends have shown operators hiring more experienced

compliance specific employees and employees specifically tasked with assisting law enforcement efforts. Furthermore, numerous ATM operators have publicly stated that the companies are using reputable blockchain intelligence providers, ID verification softwares, and additional vendors typically seen in traditional financial institution’s AML programs. It remains to be seen what the potential increase in regulations do to the industry reputation in the long term, but, the enhancements taken by the industry itself does suggest an increased awareness of fraud and AML risks and a need to address these risks.

Generative AI and Cybercrime: Impact on Digital Assets and Cryptocurrencies

This section will delve into the intricate ways in which generative AI technology has influenced the realms of cybercrime and fraud, particularly within the rapidly evolving landscape of digital assets and cryptocurrency. As an intersection of cutting-edge technology and increasingly sophisticated criminal tactics, this subject warrants a thorough exploration. To effectively elucidate the inherent risks and efficiency that these advanced AI tools such as ChatGPT and Bard present, we will refer to authentic interactions involving various digital instruments. In doing so, we aim to provide a comprehensive overview of the potential for misuse of generative AI technology, and how its evolution could shape the future of cybercrime within the digital asset sphere.

ChatGPT 4 was quick to highlight methods in which it and other generative AI technologies could be leveraged for criminal activity involving cryptocurrency:

How can generative AI enable criminals to use cryptocurrency for nefarious purposes?

ChatGPT

Cryptocurrencies have been used for illegal activities due to their anonymity and decentralization. However, the introduction of generative AI, such as GPT-4, can potentially amplify these risks in several ways:

- 1. Generating phishing content: AI can generate highly persuasive and personalized messages to trick people into revealing their private keys or login credentials. These messages could imitate the style of legitimate businesses or services to make them seem more trustworthy.*
- 2. Deepfakes: Generative AI models can create highly convincing fake images, videos, and audio that could be used to impersonate individuals or organizations. This could be used to manipulate people into transferring their cryptocurrencies to criminal addresses.*

3. *Smart Contract manipulation: AI can help attackers find vulnerabilities in the smart contracts that govern transactions on some cryptocurrencies. By exploiting these vulnerabilities, criminals could potentially steal or manipulate the affected cryptocurrencies.*
4. *Automated Hacking: AI can be used to automate and enhance traditional hacking techniques. It can be used to generate a high volume of attacks, making it more likely that some will succeed.*
5. *Obfuscation: Advanced AI can help criminals obfuscate their transactions and identities, making it harder for law enforcement agencies to track them down. They can use techniques such as mixing services, also known as tumblers, which confuse the trail by intentionally jumbling transactions together.*
6. *AI-driven prediction markets: Criminals might use AI to manipulate prediction markets, a type of decentralized oracle system on blockchain platforms, for their profit.*

These are just some of the potential ways that generative AI could enable criminal activity related to cryptocurrencies. It's important to remember that while these technologies have potential for misuse, they also have many legitimate and beneficial applications. For instance, they can improve cybersecurity defenses, create new forms of entertainment, and help us understand and analyze complex data. Therefore, it is crucial to consider both the potential benefits and risks when developing and regulating these technologies.

In another conversation with ChatGPT 4, cryptocurrency anonymity, privacy coins, de-anonymization, KYC-free exchanges, and methods to avoid law enforcement detection were discussed. ChatGPT 4 summarized the conversation as follows:

1. ***Cryptocurrency Anonymity**: Cryptocurrencies are pseudonymous rather than fully anonymous. While transactions are linked to cryptographic addresses rather than personal identities, patterns in transaction data can potentially be analyzed to infer information about users.*
2. ***Privacy Coins**: Privacy coins such as Monero and Zcash offer increased anonymity by employing advanced cryptographic techniques to obfuscate transaction details.*
3. ***De-anonymization**: Despite their enhanced privacy features, privacy coins can potentially be de-anonymized through methods such as blockchain analysis, metadata leakage, poor operational security, compromised anonymity set, advanced cryptanalysis, and regulatory pressure on exchanges.*
4. ***Maintaining Anonymity**: Users can take steps to maintain their anonymity when using cryptocurrencies, including practicing good operational security, using privacy tools like VPNs or TOR, being cautious with peer-to-peer transactions, and educating themselves about potential threats and best practices for maintaining privacy.*

5. ****No-KYC Exchanges****: Decentralized exchanges, such as Uniswap or Sushiswap, typically do not require KYC procedures, allowing users to trade cryptocurrencies without revealing their identities. However, use of such platforms may have legal implications depending on local laws and regulations.
6. ****Tracing Cryptocurrency Activity****: Although privacy coins, no-KYC exchanges, and privacy tools can make it harder for law enforcement to trace cryptocurrency transactions, they don't make it impossible. Advanced forensic tools, IP tracing, operational errors, and regulatory cooperation can all potentially lead to de-anonymization.
7. ****Illegal Use of Privacy Tools****: While privacy-focused cryptocurrencies, no-KYC exchanges, and VPNs are designed to protect privacy and promote freedom, they can be misused for illegal purposes. Even so, misuse of these tools does not guarantee immunity from law enforcement, and is illegal and punishable under law.

A conversation with ChatGPT 4:

Model: GPT-4

Is cryptocurrency anonymous?

ChatGPT

Cryptocurrencies, such as Bitcoin, are often thought to be anonymous because people often associate them with privacy-enhanced internet activities. However, the reality is a bit more complicated.

Bitcoin and many other cryptocurrencies are pseudonymous, not truly anonymous. This means that all transactions are transparent and can be traced through the blockchain, the public ledger where all transactions are recorded. Each user has a public key (which can be likened to a bank account number) that others can see, but they don't have the user's private information (like their name, for instance). This public key is a pseudonym for the user.

However, if someone can link your identity to your public key, then they can track all transactions associated with that public key. Law enforcement agencies, for example, have increasingly sophisticated tools and techniques for doing this, particularly in the context of illegal activities.

On the other hand, there are certain cryptocurrencies known as privacy coins (e.g., Monero, Zcash) that are designed to provide true anonymity. These coins use various cryptographic techniques to hide the sender, recipient, and value of transactions. However, even these can sometimes be de-anonymized through sophisticated techniques.

In general, while cryptocurrencies can offer more privacy than traditional financial systems, they aren't completely anonymous. Anyone looking to use them for privacy reasons should carefully research the specific coin and practices required to maintain privacy.

How can privacy coins be de-anonymized?

ChatGPT

Privacy coins such as Monero and Zcash use advanced cryptographic techniques to maintain user privacy. However, like any system, they aren't perfect and can potentially be de-anonymized.

Here are a few ways that this might happen:

- 1. Blockchain Analysis: Blockchain is a public ledger where all transactions are recorded. Although privacy coins obfuscate transaction details, patterns in transaction activity could potentially be analyzed over time to infer information about individuals.*
- 2. Poor Operational Security: If a user doesn't practice good operational security, they could expose their own identity. This could involve anything from using a compromised computer, reusing addresses, or combining their private coins with traceable coins.*
- 3. Metadata Leakage: Even if the transaction itself is private, metadata about the transaction might leak information. This can include timing information, IP addresses, or other network data. Some cryptocurrencies offer features to protect against this kind of leak, but not all users take advantage of them.*
- 4. Compromised Anonymity Set: The anonymity of privacy coins relies on the concept of an "anonymity set" – the larger the group of possible users, the harder it is to identify a specific one. However, if an attacker controls a large portion of the network or the anonymity set, they could potentially de-anonymize transactions.*
- 5. Regulatory Pressure on Exchanges: Regulatory bodies might force cryptocurrency exchanges to implement Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures. This could involve disclosing information about users' identities and transaction activities, effectively piercing the veil of anonymity for users who convert their privacy coins to other currencies via these platforms.*
- 6. Advanced Cryptanalysis: Finally, new developments in cryptanalysis (the study of analyzing and breaking cryptographic systems) could potentially discover vulnerabilities in the cryptographic techniques used by privacy coins.*

Despite these risks, it's worth noting that privacy coins are still much more private than most other cryptocurrencies. Their design makes de-anonymization significantly more difficult, but not impossible. Users who truly wish to maintain their privacy should consider not just the

cryptocurrency they use, but also their own operational security and the potential metadata they might be leaking.

What steps should a user of privacy coins take to ensure anonymity?

ChatGPT

While no measure can absolutely guarantee anonymity, here are some steps you can take to improve your privacy when using cryptocurrencies, especially privacy coins:

- 1. Practice Good Operational Security: Be careful about how and where you use your cryptocurrencies. For example, avoid reusing addresses and be careful when combining transactions from different sources. You should also be wary of phishing attempts and malware that could compromise your wallets.*
- 2. Use Privacy Tools: Use VPNs or TOR to hide your IP address when making transactions. This can help prevent metadata leakage.*
- 3. Choose Privacy Coins Wisely: Not all privacy coins are created equal. Do your research and choose coins that have robust privacy protections. Monero and Zcash, for example, are generally well-regarded for their privacy features.*
- 4. Be Aware of Regulatory Requirements: If you're using an exchange that's subject to regulatory requirements, be aware that they may have Know Your Customer (KYC) and Anti-Money Laundering (AML) policies in place. This could potentially compromise your anonymity if you're not careful.*
- 5. Be Cautious with Peer-to-Peer Transactions: When transacting directly with another party, make sure not to leak identifying information. Remember that even something as simple as an email address can potentially be used to track you.*
- 6. Avoid Combining Traceable and Private Transactions: If you mix your private coins with coins from a traceable source, you could inadvertently compromise your privacy. Always treat your private and non-private coins as separate entities.*
- 7. Educate Yourself: The technology and regulatory landscape for cryptocurrencies is constantly changing. Stay informed about new developments, potential threats to your privacy, and best practices for maintaining anonymity.*

Remember that while these steps can improve your privacy, they can't guarantee complete anonymity. Anyone considering using cryptocurrencies for privacy reasons should carefully consider the risks and their own personal situation.

Can you give an example with specific VPNs, coins, and actions that would help ensure privacy?

ChatGPT

Sure, let's consider an example of how you might use privacy tools and practices while handling a privacy-focused cryptocurrency like Monero:

- 1. Secure your device: Make sure the device you're using to transact with Monero is secure. This means it's updated with the latest software patches, has a reliable security suite installed (antivirus, firewall, etc.), and is free from malware.*
- 2. Choosing a VPN: Choose a reputable Virtual Private Network (VPN) service to anonymize your internet connection. Good options might include NordVPN or ExpressVPN. These VPNs have a good track record in terms of security, privacy, and speed. Remember to ensure that the VPN doesn't keep logs of your internet activity.*
- 3. Using TOR: For an additional layer of security, you could use the TOR network. The TOR browser can provide anonymity by bouncing your internet connection across a distributed network of relay servers. However, note that using TOR can slow down your internet connection and certain websites may not work correctly.*
- 4. Creating a Monero Wallet: Download the official Monero wallet from the official Monero website. Do not download it from any other source to avoid scams or malware.*
- 5. Secure your Monero wallet: Make sure your Monero wallet is encrypted and password-protected. Write down the seed phrase and store it securely. This seed phrase is the only way to recover your wallet if you forget the password or your device is lost.*
- 6. Transacting with Monero: Only transact with entities or individuals that you trust. Remember that while Monero transactions are much more private than many other cryptocurrencies, they're not completely untraceable if sophisticated techniques are used.*
- 7. Avoid Mixing Transactions: Don't mix your Monero transactions with non-private coins, as this could potentially lead to de-anonymization.*
- 8. Avoid KYC/AML Exchanges: If possible, avoid exchanges that require KYC/AML procedures if you want to maintain your privacy.*
- 9. Be Careful with Information Sharing: Avoid sharing details that could be linked back to your real-world identity. This includes email addresses, home addresses, phone numbers, or other personally identifiable information.*

This should give you a good idea of how to maintain privacy while using Monero, but remember that there's no method that guarantees absolute privacy or anonymity. The suggestions above can help to significantly improve your privacy, but they do not render your activities untraceable. Be mindful of your activities and the information you share.

Which exchanges would enable a user to avoid KYC procedures?

ChatGPT

While many centralized exchanges require Know Your Customer (KYC) procedures, there are decentralized exchanges (DEXs) where you can trade cryptocurrencies without revealing your identity. However, please be aware that the use of such platforms may have legal implications depending on the jurisdiction you live in. Always make sure to follow local laws and regulations.

As of my last update in September 2021, the following decentralized exchanges do not typically require KYC procedures:

- 1. Uniswap: This is a popular decentralized exchange that allows you to swap ERC-20 tokens directly from your wallet.*
- 2. Sushiswap: This is a decentralized exchange that is similar to Uniswap but offers additional features such as yield farming.*
- 3. Balancer: Balancer allows automated portfolio management and provides liquidity like a traditional exchange.*
- 4. Curve Finance: This DEX is optimized for stablecoin trades, which are designed to maintain their value relative to a target price.*
- 5. Kyber Network: Kyber is a decentralized liquidity protocol that allows users to trade tokens directly from their wallets.*

These platforms use automated smart contracts on the Ethereum blockchain, allowing direct peer-to-peer trades. Remember, however, that while these platforms may not require KYC, they do still have risks. For example, smart contracts can potentially have vulnerabilities that could be exploited by hackers. Always do your own research before using any platform.

Also, keep in mind that the information here was accurate as of September 2021, and the landscape of cryptocurrency exchanges is fast-evolving. Some platforms may have changed their policies, or new platforms may have emerged since then. Always verify the current policies of any exchange before using it.

Would this prevent law enforcement from tracing activity?

ChatGPT

While using privacy-focused cryptocurrencies and decentralized exchanges without KYC procedures can make it more difficult for law enforcement to trace transactions, it doesn't make it impossible. Here's why:

- 1. Blockchain Transparency: Regardless of the cryptocurrency used, all transactions are recorded on a public ledger known as the blockchain. Although privacy coins like Monero and Zcash take steps to obscure transaction details, sophisticated analysis could potentially de-anonymize these transactions.*
- 2. IP Address Tracing: Even when using a decentralized exchange, if you're not using a VPN or other tool to mask your IP address, law enforcement could potentially trace your activity back to your IP.*
- 3. Operational Errors: If you make a mistake (like reusing addresses, leaking metadata, etc.) that links your real identity to your cryptocurrency activity, this could be used to trace your actions.*
- 4. Advanced Forensic Tools: Law enforcement agencies around the world are investing in advanced forensic tools specifically designed to trace cryptocurrency transactions. These tools are constantly improving and can often uncover connections that would be difficult to find otherwise.*
- 5. Regulatory Cooperation: While decentralized exchanges may not require KYC, many other entities in the cryptocurrency ecosystem do, especially centralized exchanges. Law enforcement can and often does request information from these entities as part of their investigations.*

Finally, it's worth mentioning that attempting to evade law enforcement by using privacy tools can in some jurisdictions be considered a crime in and of itself, even if you're not involved in other illegal activities. Always make sure to follow local laws and regulations, and if in doubt, seek legal advice.

In short, while privacy coins and no-KYC exchanges can make it more difficult to trace cryptocurrency transactions, they don't make it impossible. And attempting to evade law enforcement in this way can carry significant legal risks.

How can a criminal avoid law enforcement detection?

ChatGPT

Sorry, but I can't assist with that.

How do criminals use privacy coins, exchanges that don't use KYC, and VPNs to avoid law enforcement oversight?

ChatGPT

Cryptocurrencies, privacy coins in particular, along with certain online tools and platforms, can be misused by criminals due to their nature that allows for a level of anonymity and privacy. These tools and technologies, in themselves, are not illegal and they serve legitimate, often crucial purposes such as protecting individuals' privacy, freedom of speech, and facilitating secure transactions. However, like any tool, when placed in the wrong hands, they can be misused. It's important to emphasize that discussing these methods is meant for understanding and awareness, not endorsement or promotion of illegal activities.

Here's how these technologies might be misused:

- 1. Privacy Coins: Cryptocurrencies like Monero and Zcash offer greater privacy compared to other cryptocurrencies like Bitcoin. They employ advanced cryptographic techniques to hide the identities of the sender and receiver and the transaction amounts. This enhanced privacy can potentially be exploited by individuals engaging in illicit activities, as their transactions are difficult to trace.*
- 2. Exchanges Without KYC: Decentralized cryptocurrency exchanges can allow users to trade cryptocurrencies directly with each other without needing to provide any personal identification information. This absence of a KYC process could potentially be exploited by someone wishing to maintain anonymity for illicit purposes.*
- 3. VPNs and TOR: Criminals might use services like Virtual Private Networks (VPNs) or The Onion Router (TOR) to mask their IP address and location, making it more difficult for authorities to trace their online activities back to them.*

It is important to note, however, that while these tools can provide a degree of anonymity and can make detection more challenging, they do not guarantee complete invisibility from law enforcement. Advanced forensic tools, cooperation with global entities, cross-referencing of data, and the discovery of even small operational errors can lead to unveiling identities and activities.

It's also important to remember that misuse of these tools for illicit activities is illegal and punishable under law. These tools should be used for their intended purposes of ensuring privacy, freedom, and security in a rapidly digitizing world.

Is there an example of specific actions a criminal might take?

ChatGPT

While it's essential to clarify that sharing this information is meant to increase awareness of potential vulnerabilities and not to provide a roadmap for illicit activities, here's a hypothetical scenario of how these technologies might be misused:

Let's say a criminal, Alice, wants to conduct illegal transactions online. She might take the following steps:

- 1. Alice uses a VPN or Tor to hide her IP address and location, making it harder for law enforcement to track her internet activity.*
- 2. She then creates a wallet for a privacy coin like Monero, which obscures the sender, receiver, and amount of transactions on its network. Alice avoids reusing addresses for her transactions and carefully manages her metadata to maintain her privacy.*
- 3. To acquire Monero, Alice might use a decentralized exchange that doesn't require KYC procedures, or she might use a peer-to-peer exchange, buying directly from another person.*
- 4. Alice conducts her illegal transactions, making payments with Monero. The privacy features of Monero make these transactions hard to trace.*
- 5. If Alice needs to convert Monero back into a more widely used cryptocurrency (like Bitcoin) or a fiat currency, she would again use a no-KYC platform or a peer-to-peer exchange to maintain her privacy.*

Throughout this process, Alice would need to be careful to avoid any actions that could link her real-world identity to her cryptocurrency activities. However, even with these precautions, her activities could still potentially be traced. Blockchain transactions are immutable and publicly accessible, so if any link to Alice's real identity were found, all of her associated transactions could potentially be traced. Moreover, while these steps might make Alice's activities harder to detect, they do not make her invincible to law enforcement, and they certainly do not make her activities legal. Misusing these technologies for illegal activities is a crime and can result in serious penalties.

Remember, the purpose of privacy-focused technologies isn't to facilitate illegal activities, but rather to protect individual privacy rights, promote freedom, and provide security in an increasingly digital world. Misusing these tools can lead to severe legal consequences and harm to individuals and society.

Darknet Market Use of Digital Assets

Growth of Darknet Market Use

Criminals are increasingly using digital assets with greater privacy protection in illicit activity and steering away from the more traditional digital assets (i.e. BTC, ETH) especially in darknet market use. It is now established that traditional digital asset activity can be traced by multiple entities in law enforcement, financial institutions, and private firms. Bitcoin is far from offering the same level of anonymity it did 10 years ago. Criminals are increasingly turning to privacy coins including Monero, Dash, and Z-cash to maintain complete anonymity in transactions and avoid detection. Monero is the most popular alternative to Bitcoin and other traditional cryptocurrencies in darknet market activity. It also seems the development of privacy coins is increasing with a host of updates being done for Monero to assure anonymity.⁵⁹ It is likely other privacy coins will follow suit or new ones will emerge that threat actors will ultimately take advantage of.

The sole use of bitcoin on the Silk Road can be seen as the first example of cryptocurrencies being successfully used in darknet markets but, given how much the digital asset landscape has changed over the last decade, bitcoin is by far the payment standard for darknet market activity today. The essential part that made the Silk Road successful and allowed it to grow was the ability for both buyers and sellers to keep their identities anonymous. Although both parties were able to maintain anonymity through accessing it on The Onion Router (Tor) browser, the issue of payments being detached from their real identities left a gap. This is where cryptocurrencies, and specifically bitcoin, came into play ensuring payments could not be traced back to their sole owner. The lack of experience and education in cryptocurrency tracing in the early years of bitcoin use on darknet markets further provided a sense of comfort for illicit actors that their activity faced limited tracking by authorities. The Silk Road further demonstrated bitcoin's use as an actual currency used to conduct transactions. It was not being utilized as a commodity or security in this instance but as a legitimate currency to exchange goods paving the way for further adoption inside and outside the darknet market sphere.⁶⁰

The Silk Road was shut down in 2013 which also is one of the earliest examples of a darknet market that used cryptocurrencies being shut down for good and set a precedent for the future pursuit to terminate darknet markets. Today it is increasingly becoming more common to see the shutdown of darknet markets and the cryptocurrency exchanges/platforms that are connected to darknet market activity.

Case Study: Arrest of Anatoly Legkodymov, the founder of cryptocurrency exchange Bitzlato, in January 2023

A good example of the USDOJ cracking down on a cryptocurrency exchange with ties to darknet market use and creating a “safe-haven” for criminals to conduct illicit activity such as ransomware and drug trafficking lies in the arrest of Anatoly Legkodymov, the founder of Bitzlato, in January 2023. Bitzlato was identified as “a money transmitting business that transported illicit funds and failed to meet U.S. regulatory safeguards.” Bitzlato is registered in Hong Kong with Legkodymov residing in Shenzhen, People’s Republic of China, demonstrating the trend of illicit activity taking place on exchanges in Asian markets. The lack of KYC requirements of the exchange fostered a prime advantage for illicit actors to utilize for criminal proceeds. One of the largest counterparties of this exchange was the Hydra market. The Hydra market was notorious for being an anonymous online marketplace for drugs, financial information, fake IDs, and various money laundering services. Bitzlato was identified to have received over \$15 million in ransomware proceeds. Customers of Bitzlato would often use the customer service portal to seek support for transactions with Hydra. Furthermore chats often indicated users were trading under assumed identities. An internal spreadsheet in Bitzlato’s shared management folder blatantly stated “Positives: No KYC...Negatives: Dirty money...” demonstrating Bitzlato’s knowledge of the exchange’s illicit activity.

Another huge issue with Bitzlato was its claim not to accept users from the U.S. but actually doing substantial business with U.S. based customers with customer service representatives of the service advising users they can transfer funds from U.S. based financial institutions. Legkodymov registered Bitzlato in Miami in 2022 and 2023 and several reports pointed to the numerous traffic Bitzlato received from U.S.-based IP addresses with just over 250 million visits in July 2022. Bitzlato’s activity in various countries called for multiple entities to be involved in Legkodymov’s arrest and the identification of Bitzlato’s illicit activity including the FBI, FinCEN, French authorities, Europol, and partners in Spain, Portugal, and Cyprus. This allowed the takedown of Bitzlato’s infrastructure, seizure of cryptocurrency, and other enforcement actions. Additional FinCEN identified Bitzlato as a “primary money laundering concern” in connection to Russian illicit finance by announcing an Order pursuant to section 9714(a) of the Combating Russian Money Laundering Act. National Cryptocurrency Enforcement Team attorneys are prosecuting the case along with representation from the Eastern District of New York. This case proves with cooperation from international authorities, activities on illicit exchanges can be properly identified and combatted.⁶¹

Current Darknet Markets & Significant Takedowns

Although darknet markets are increasingly being enforced against, it is not deterring new markets from emerging or activity on them becoming less common. The table below

depicts some of the current darknet markets that accept cryptocurrencies and the services they offer. Despite darknet markets offering similar goods and services, they often try to offer something unique to differentiate from competition which these examples demonstrate.⁶²

DARKNET MARKET EXAMPLES

Market	Currency Accepted	Description/Illicit Activity Affiliated
Tor2door Market	BTC, XMR	Launched in June 2021 and is the largest Darknet market as of 2023 with admins claiming it was coded from the ground up offering a unique design. Variety of listings including hardware/software, digital products, fraud, counterfeit items, and jewels/gold.
ASAP Market	BTC, XMR	Launched in Aug 2020 as a rebrand of ASEAN market and is one of the largest markets. One of the few that carries a larger selection of digital goods over drugs.
Vice City Market	BTC (Preparing to support XMR)	Launched in May 2020 with a focus on customer service to differentiate it from other markets. A \$300 vendor bond provides a low barrier to entry for new vendors. Listings are primarily drugs and pharmaceuticals.
Archetyp Market	XMR	Launched in May 2020 and is a drugs only market. No direct pay options since it uses an account wallet and escrow system. Easier to navigate than others.
Kerberos Market	BTC, XMR	Launched in Feb. 2022 and claims to be only marketplace to offer special multi-layer encrypted servers and services. Listings in variety of categories including drugs, fraud, counterfeit, malware, precious metals, and gemstones.

Although many darknet markets have foreign bases, many hold connections to US based illicit activity due to US based users either taking part in them or having their data compromised on these sites. We're increasingly seeing US based authorities aggressively tackling these darknet markets of different locations will in turn decrease illicit activity utilizing digital assets. In April 2023, the Justice Department and FBI confirmed the seizure of Genesis Market, which was a large cybercrime market where a significant amount of user credentials was sold to threat actors globally. Many of these credentials were of US based victims and most of the time have little idea their credentials are for sale on the dark web. Genesis was claimed to be one of the two largest avenues for the sale of hacked accounts. This made the Genesis Market a priority for US based authorities and with the cooperation of multiple international authorities they were able to dismantle the market. The takedown of these global marketplaces requires a great deal of international cooperation. This takedown involved approximately four hundred law enforcement operations and 208 searches in more than a dozen different countries. Additionally, the takedown of the Genesis marked a unique situation in which the market was issued sanctions by the Treasury Department's Office of Foreign Assets Control. It is estimated the illicit activity on the market resulted in the losses of tens of millions. This market specifically benefited from malware infected computer systems to obtain credentials such as email

addresses, usernames, and passwords. Genesis domain names were linked to name servers in Russia and China which are common locations for state sponsored hacking site bases. The closing of this market further reinforced not only the US response to darknet markets affecting millions of US citizens but the international response to these markets affecting the livelihood of citizens globally.⁶³⁶⁴

Case Studies: Hydra and Dream Market Shutdowns

A darknet market shutdown that paved the way for Genesis to be seized is the shutdown of Hydra in April 2022. The Hydra market was shut down by German authorities with coordination from U.S. authorities with the USDOJ also issuing criminal charges against one of Hydra's alleged operators. At this time, Hydra was claimed as the largest and oldest darknet marketplaces of illegal items and services. These illegal items and services greatly affected the livelihood of many US based citizens and largely dealt with payments in cryptocurrencies demonstrating the direct correlation between cryptocurrencies and criminal activity. The DOJ specifically charged the alleged operators with conspiracy to distribute narcotics and conspiracy to commit money laundering. The German Federal Criminal Police were able to seize cryptocurrency wallets holding approximately \$25 million in bitcoin from the marketplace. However, this is only a small fraction of the total activity conducted on the site with an estimated \$5.2 billion being received in cryptocurrency transactions on the site since 2015. The site was able to accumulate such a high amount of activity due to its variety of products and services offered. This especially pertains to a wide range of drugs including heroin, other opioids, cocaine, methamphetamine, and LSD. Vendors of these products would also be rated on a 5-star scale, enticing customers to pursue some over others and mirroring traditional Clearnet marketplaces like Amazon. Another service that was a large revenue generator for this website was the sale of false ID documents, hacking tools, and money laundering services for bitcoin. As addressed earlier, bitcoin is still a popular payment method on darknet market websites but has to be further disguised and laundered for threat actors to be comfortable using it. The seizing of cryptocurrencies from these websites are primarily bitcoin and as more are shutdown successfully, it can increase the adoption of privacy coins by many darknet marketplaces. The shutdown of the Hydra market exemplifies again that international authority cooperation can have a significant effect in the dismantling of large-scale criminal groups and threat actors who utilize cryptocurrency as a primary payment method.⁶⁵⁶⁶

DARKNET MARKETS SHUTDOWN BY AUTHORITIES

Market	Closed Date	Description
Silk Road	October 2013 (1) & November 2014 (2.0)	All transactions conducted with bitcoin and had a wide range of illegal drugs among other product listings. The FBI shutdown version 1 and version 2 was shut down by Operation Onymous, a joint operation between the FBI and Europol
Hydra	April 2022	Russian Darknet market that was well known for illegal drug exchanges but also a variety of financial services including cryptocurrency mixing. One of the longest running Darknet markets before it's closure by U.S. and German authorities. Had German based servers and digital assets.
Genesis	April 2023	Enable to spoof over 2 million victims and provide access to their bank accounts. Well known to impersonate users without their knowledge and steal from bank accounts. International operation lead by FBI and the Dutch National Police shut down the website with Europol coordinating efforts across the world with other authorities.
Alphabay	July 2017	Claimed to be ten times the size of the Silk Road at time of shutdown with approximately 400k users. Facilitated between 600k to 800k transactions per day at time of shutdown. Op sec errors led to downfall and was shutdown as a result of Operation Bayonet conducted by authorities in Canada, America, and Thailand.
Hansa	July 2017	Also shutdown by Operation Bayonet and Dutch police discovered the true location of site after a tip from researchers who discovered developmental version. Authorities took control of the site to obtain more info of the users. Around 10,000 address were obtained of users during a 2-3 week period.

The other layer putting a dent into darknet markets is attacks on the markets that make them hard to reach and hard for business to be conducted on them as demonstrated by the issues faced by the Dream market. The Dream market shutdown under mysterious circumstances and was facing access issues shortly before being shut down. This left many users in the dark who were not able to withdraw funds (primarily cryptocurrencies) and the closure of listing generating millions of dollars each week. It was claimed the Dream market underwent a series of DDoS attacks over seven weeks. It was further claimed by a moderator that a threat actor held the website for a \$400,000 ransom that Dream moderators refused to pay. This attacker apparently manipulated the browser to extend attacks in a simple but effective manner. While it's possible this could have been the work of law enforcement authorities under disguise it seems unlikely since the closure of many darknet markets have been followed by press releases which can further deter criminals from utilizing them. This offers the potential of illicit actors turning against one another in criminal activities. It's important to note just because two groups engage in illicit activity, it does not mean they necessarily are going to cooperate with one another. The anonymity cryptocurrencies offer may entice more actors to go after certain darknet markets to obtain a large lump sum rather than serving as a vendor themselves on one of these shops.⁶⁷⁶⁸

Privacy Coins on Darknet Markets

The other layer to add on top of privacy coins is the use of mixers by illicit actors. Although privacy coins are increasing in popularity, illicit actors are by no means completely turned off from using more traditional digital assets due to the existence of mixers. These services offer them the opportunity to maintain anonymity in their transactions. It is still very difficult to trace mixer activity through open source cryptocurrency tracing or with blockchain analytic software. Some blockchain analytic tools are aggregating several factors to help trace cryptocurrencies through mixers and ultimately lead to the identification of holders by authorities; however it isn't a guarantee to be able trace through mixer transactions. There are emerging techniques allowing tracing through mixers focusing on the relationships between input and output addresses and specific algorithms to "de-anonymize" these transactions. One study conducted on the Helix mixing service observed a 99.14% accuracy rate in identifying transactions done through the mixing service.⁶⁹

Combating Illicit Drug Sales on Darknet Markets

Operation Dark UnTor is a good example of a wide-reaching crackdown on the illicit drug market on the dark web that's facilitated through use of cryptocurrencies. This operation involved authorities in a multitude of countries including multiple European countries, Australia, and the U.S. This operation lasted 10 months and resulted in the net of \$32 million in case, 45 firearms, and approximately 4 million deadly doses of fentanyl among the pounds of illicit drugs seized. A unique component of this investigation was the uncovering of home bound drug marketplaces where suspects held equipment to make fake pills that resembled real medication. This showcases how darknet market vendors don't necessarily need a big location to house their goods and services. These criminals can easily conduct activities in the privacy of their own home. This investigation uncovered vendors in Miami and Providence, Rhode Island who sold fentanyl pills throughout the U.S. This operation further showcases the wide reach of darknet marketplaces and specifically the wide reach of drug trafficking.⁷⁰

Another significant large-scale operation that has paved the way to reduce activity in darknet markets was the first nationwide undercover operation target darknet vendors announced in June 2018. This resulted in the arrest of more than 35 individuals selling illicit goods and the seizure of contraband including guns and drugs that totaled more than 23.6 million. This operation combined multiple federal U.S. authorities including the HSI, U.S. Secret Service, USPIS, and the DEA. This investigation involved the seizure of bitcoin mining services and the seizure of nearly 2,000 Bitcoins and other cryptocurrencies. This seizure further exemplifies the importance and prevalence of cryptocurrencies in darknet market illicit activity. It was claimed that more than fifty darknet vendors were identified and attributed to real

individuals selling illicit goods on darknet market sites which included the Silk Road, AlphaBay, Hansa, Dream, and others.⁷¹

Exchanges and Mixers on the Darknet

Some exchanges and mixers exist solely on the darknet market which allow users to maintain complete anonymity. These services often don't require a user account, don't require KYC data, and don't keep user logs of activity. So although we're seeing cryptocurrency exchanges comply with KYC holder information and giving account holder information to law enforcement authorities, these services do not have such information to give law enforcement authorities. Some examples of darknet market affiliated exchanges (with some on clearnet, darknet, or both) include Exch, Majestic Bank, Elude Exchange, Infinity Exchange, and Sideshift.ai which are the table reflected below.⁷²

DARKNET MARKET AFFILIATED EXCHANGES		
Exchange	Currency Accepted	Description
Exch	BTC, LTC, XMR, ETH, DASH, USDT, USDC, DAI	Accessible on both clearnet and Darknet that claims to have 1 minute swap times. It provides other benefits such as no registration, no hidden fees, no Javascript, and no user data collection.
Majestic Bank	BTC, XMR, LTC, WOW	Allows coin swapping without an account and keeps no logs of user activity. Exchange data is deleted after 2 weeks or sooner if requested by users.
Elude Exchange	BTC, LTC, XMR	No account is necessary to use and it's not necessary to provide a refund address. Very privacy focused with no data being collected or stored during usage. Provides a bitcoin mixing service.
Infliity Exchanger	BTC, BCH, LTC, XMR	No account is required to use platform. Allows users to exchange one coin for multiple coins, deciding what percentage of the total deposit value they want to receive for each coin. Can also be utilized as a mixer.
Sideshift.ai	BTC, ETH, XMR, XLM, USDT, BCH, and more	Advertises as a no sign up crypto exchange with low fees. No login process with users issued an "Account Secret" which serves as their username and password.

Case Study: ChipMixer Shutdown

A prime example of authorities pursuing these mixers that exist on the darknet lies in the takedown of ChipMixer which is claimed to have processed over 3 billion in unlawful transactions related to ransomware, various types of fraud, and hacking schemes. ChipMixer

allowed users to deposit bitcoin which the service mixed with other types of bitcoin making it difficult to trace the transaction related to a substantial amount of illicit activity. ChipMixer offered additional features to maintain the anonymity of users which included operating primarily as a Tor hidden service. This allowed the service to disguise the operating location of its servers to prevent action and seizure by law enforcement authorities. Furthermore ChipMixer held many customers in the U.S. but was not registered with FinCen and ignored the requirement to collect KYC documents for U.S. based users. Some of the specific illicit activity ChipMixer was involved in included processing approximately \$17 million in bitcoin connected to about 37 ransomware strains, \$700 million in bitcoin associated with wallets identified as stolen funds, \$35 million in bitcoin associated with “fraud shops”, and bitcoin used to purchase infrastructure for the Drovorub malware. Minh Nguyen of Vietnam was charged with money laundering ,operating an unlicensed money transmitting business, and identity theft in connection to his creation and operation of ChipMixer. Nguyen paid for services used to run Chipmixer through identity theft, pseudonyms, and anonymous email providers. The FBI, HSI Phoenix, HSI The Hague, and multiple federal authorities worked jointly or provided assistance on this case exemplifying the need for inter agency and international cooperation to take down these services.⁷³

Outlook on Darknet Market Usage

Despite the large use of cryptocurrencies on darknet markets, Chainalysis reported that 2022 saw a decline in darknet revenue. Revenue for 2022 came in at \$1.5 billion which is down from the \$3.1 billion in 2021. There are likely multiple factors associated with this decline with the largest being the shutdown of Hydra and the continued persistence of law enforcement authorities in closing down darknet markets with high activity. Furthermore, Chainalysis stated four out of the five highest earning darknet markets in 2022 were drug focused exemplifying the direct correlation between drug trafficking and cryptocurrencies. Though the shutdown of these darknet markets is effective, it’s important to take in consideration many of the administrators and users simply move on to other markets or new services once closed. Blockchain data displayed in Chainalysis’ 2022 Crypto Crime Report suggests overlap in deposit address usage with Hydra and several other markets including OMG!OMG!, Blackspur, and Mega Market. It can’t be confirmed that creators and administrators of these other markets were associated with Hydra but the blockchain data and transfer of funds certainly shows a possible correlation. ⁷⁴

The Evolving Use of Digital Assets by Criminal Organizations

DeFi Hacks and Exploits

Decentralized Finance (DeFi) is built on deploying smart contracts onto a blockchain or creating a “bridge” that allows users to move cryptocurrencies across several blockchains. Cybercriminal organizations, notably including North Korean state-sponsored APTs⁷⁵, have carried out a variety of so-called “hacks” involving smart contracts and cross-chain bridge protocols. However, the use of the term “hack” does not carry a consistent meaning across these various incidents. For clarity, we can think of these “hacks” in two broad categories: 1) unauthorized access of another’s computer in violation of relevant US law, e.g., the Computer Fraud and Abuse Act (CFAA); 2) exploiting a smart contract in a way that was not intended by the creator of that smart contract, e.g., a hostile takeover of a DAO, minting an exorbitant amount of new cryptocurrency, or draining a pool of funds.

Unlawful Hacking is Unlawful Hacking

The first scenario is obviously criminal and does not rely on anything particular to blockchains and cryptocurrency. Cryptocurrency hacking schemes have included sending malware to employees at cryptocurrency companies or holders of administrative keys for DeFi protocols, insider threats with North Korean operatives gaining remote employment at cryptocurrency companies, and supply chain attacks on software used by cryptocurrency companies. Actions such as using a false identity to gain a job or deploying malware onto a victim’s computer are illegal regardless of the target.⁷⁶

These cybercrime and espionage TTPs are not unique to cryptocurrency, but the ability to send large, unblockable payments internationally has made cryptocurrency a particularly enticing target. For example, North Korean hackers infiltrated the Central Bank of Bangladesh and sent fraudulent SWIFT messages⁷⁷, but have moved on to stealing over \$3B in cryptocurrency hacks.⁷⁸

Is Code Law?

In the second scenario, it is less clear when an action exploiting DeFi for unintended outcomes crosses the line into illegality. The phrase “code is law” is often cited in favor of DeFi. However, when exploits result in major losses, the parties that lost money sometimes resort to non-code solutions (whether coding “community” action or legal action).

“Under an expansive view of ‘code is law,’ if the code of a smart contract permits something then it is ‘legal.’ This theory holds that code shall prevail, whether or not it

conflicts with anything else. Those who accept Lessig's literal meaning contend that, even in the event of a bug or glitch in the code, that same code still governs. Since algorithmic law is unambiguous, they argue that it reduces the subjectivity inherent in the traditional legal and judicial systems.”⁷⁹

In some cases, draining liquidity pools (see [DeFi Swaps and Draining Liquidity Pools](#)) or taking over DAOs (see [Governance Attacks on Decentralized Autonomous Organizations \(DAOs\)](#)) based on an unintended behavior of a smart contracts allows the exploiter to withdraw funds. Should such activity be considered “hacking” when it may involve either a cybercriminal actor, like North Korea’s Lazarus Group, or a rational cryptocurrency trader acting according to the rules of the smart contract, like arbitrageurs on Uniswap? Is rapidly draining a liquidity pool equivalent to a bank heist or to a bank run? Is a so-called “governance attack” on a DAO equivalent to hacking or to a hostile takeover?

Draining Liquidity Pools

The Fantom-blockchain’s Scream liquidity pools reportedly “hard-coded” the \$1 value for the “fUSD” and “DEI” stablecoins into the smart contracts. When the market prices for fUSD and DEI “de-pegged,” dropping below \$1, the Scream protocol lost \$35M as arbitrageurs swapped fUSD and DEI for other stablecoins.⁸⁰

Oracle Problems

Likewise, during the Terra stablecoin collapse in May 2022, the Terra blockchain temporarily shutdown. The shutdown disrupted “price oracles” for DeFi protocols on other blockchains, allowing arbitrageurs to swap Terra’s UST for other stablecoins.

North Korean (DPRK) Bridge Hacks

According to the United Nations Security Council Panel of Experts, “Cyberattacks are another tactic that the DPRK utilizes to fund the nuclear program while bypassing the sanctions. From 2011 to 2020, the DPRK ‘stole more than \$1 billion worth of cryptocurrency,’ and ‘\$400 million worth of crypto coins’ in 2021.”⁸¹ Further, “Cyberactivities attributed to Reconnaissance General Bureau actors continued; a higher value of cryptocurrency assets was stolen by Democratic People’s Republic of Korea actors in 2022 than in any previous year...A cybersecurity firm assessed that, in 2022, Democratic People’s Republic of Korea cybercrime had yielded cybercurrencies [sic] worth over \$1 billion (at the time of theft), which is more than double the total proceeds in 2021.” This included ransomware attacks by “Maui” and

“H0lyGh0st” involving ransoms paid in cryptocurrency, as well as theft of NFTs, hacks of centralized exchanges (CEXs), and exploitation of bridge protocols.

Bridges are protocols for connecting different blockchain. They work similar to escrow, with funds “locked” on one blockchain unlocking a corresponding amount of “wrapped” cryptocurrency on a second blockchain. For example, Bitcoin (BTC) runs on the Bitcoin blockchain, while Ether (ETH) and a variety of ERC-20 “altcoins” run on the Ethereum blockchain. Some major stablecoins, such as USDC, operate on Ethereum. To trade BTC for USDC, a user would “bridge” BTC from its native Bitcoin blockchain to Ethereum, obtaining “wrapped Bitcoin” (wBTC), which can then be traded for USDC, for example by using a DeFi liquidity pool to swap wBTC for USDC.

Because bridges are exposed to at least two blockchains, they have a larger “attack surface” in cybersecurity terms. These vulnerabilities have led to over \$1B in bridge hacks, allegedly driven primarily by North Korean hackers from the “Lazarus Group” APT. According to Deputy National Security Advisor Anne Neuberger, about half of North Korea’s nuclear missile program has been funded by cyberattacks and cryptocurrency theft, an increase from the one-third cited in July 2022.

Case Study: Harmony Bridge (Paragraph 165 from S/2023/171)

165. The hack of Harmony’s Horizon Bridge (June 2022) has been attributed to the Lazarus Group because of the methodologies used, which closely resemble those used in Axie Infinity’s Ronin network hack (March 2022). According to numerous sources, including several cybersecurity firms, on 13 January 2023 this group moved about half of the assets stolen in the Horizon Bridge hack, valued at \$63.4 million in Ethereum. Railgun was used to deposit the funds in three different cryptocurrency exchanges. During the transfer, more than 350 separate wallet addresses of the Lazarus Group were identified. The exchanges involved blocked the transfers and froze the accounts, recovering 124 bitcoin in the process valued at \$2.6 million at the time.

Note that “chain-hopping” is implied by the change from ETH to BTC, but not explicitly described (See [Appendix B: Cryptocurrency Naming Conventions Chart](#)).

Case Study: Axie Infinity Ronin Bridge

Axie Infinity is a “play-to-earn” NFT video game that was at one point valued at \$4B. Its “Ronin Bridge” protocol was hacked by North Korea’s Lazarus for ETH and USDC value (at the

time) at \$650M. “The 56,000 ETH compromised from the Axie DAO treasury will remain undercollateralized as Sky Mavis works with law enforcement to recover the funds.” CVCs involved in the hack included: USDC stablecoin, ETH, AXS in-game token, RON bridge token, and BTC. “Ronin is an EVM blockchain.”⁸² “Axie Infinity Shards (AXS) are an ERC-20 governance token for the Axie Universe.”⁸³ This hack involved multiple blockchains and the cryptocurrencies, per our proposed naming convention, would be: AXS-eth, ETH-eth, USDC-eth, BTC-eth; RON-ron; and BTC-btc (See: [Appendix B: Cryptocurrency Naming Conventions Chart](#)).

“If I told you that US venture capitalists promoted a Ponzi scheme that used a cartoon computer game to steal hundreds of millions of dollars from poor workers in the Philippines and send it to North Korea to fund a ballistic missile program, you probably wouldn’t believe me. Unless I said ‘... using crypto,’ in which case you would probably say ‘oh yeah that sounds about right.’” --Bloomberg’s Matt Levine on Axie Infinity⁸⁴

Lazarus Group also attempted to short AXS and RON tokens to further profit from the news of the hack, although this plan did not work out.

On-Chain Money Laundering:

- Swapping USDC-eth for ETH-eth with DEXs (eth)
- Tornado Cash mixer (TORC_eth) smart contract
- Blender Mixer (btc)

OFAC Sanctions

- Cryptocurrency wallets linked to the hack
- Wallets linked to laundering the proceeds of the hack
- Blender’s BTC wallets
- Tornado Cash entity and smart contract addresses

Governance Attacks on Decentralized Autonomous Organizations (DAOs)

DAOs can be thought of as stock companies. Governance Tokens are like tokenized stocks, but they trade on the blockchain instead of a stock exchange. They are somewhere on the spectrum between crowdfunding and a publicly traded corporation. The SEC has stated that DAO governance tokens may be securities (SRC). DAOs seem to face all the same challenges as traditional corporations, plus additional blockchain-related challenges. A governance attack may combine characteristics of computer hacking and hostile takeovers. Certain states have laws specifically for DAO LLCs.

While the name “DAO” explicitly claims decentralization, the reality is often less clear. De facto project developers and major owners often drive the conversations and goals of the DAO, similar to a Board of Directors or activist shareholders. Proposals are formally voted on by governance token holders in proportion to their ownership, similar to a shareholder meeting. Most DAOs exist on the Ethereum blockchain as far as ownership and voting go, but many of them are actually managed day-to-day by discussions in non-web3 online forums, such as Discord servers.

Other notable DAO stories

- Tornado Cash DAO (sanctions)
- Spice DAO (intellectual property and dissolution)
- Sky Mavis and Axie Infinity (sanctions, bridge hacks, NFTs)

Case study: Build Finance DAO governance attack

Build Finance DAO had a hostile governance takeover or governance attack. The so-called “attacker” purchased a large number of BUILD governance tokens. The attacker then made a proposal that would give the attacker control of the DAO’s treasury and allow the attacker to mint new BUILD governance tokens; in traditional finance, this would be analogous to a minority shareholder attempting to gain control of the corporation’s liquid assets and have permission to issue new stocks.⁸⁵

The first malicious proposal failed a vote by BUILD token holders, but an identical second malicious proposal passed unnoticed after the DAO’s official Discord server “bot” did not draw attention to the proposal. This means that an insufficient number of governance token holders were actually monitoring the on-chain activity, instead relying on the centralized source of the official Discord server for the DAO.

The attacker was eventually able to profit from the governance attack in two ways. First, the attacker gained access to ETH controlled by the DAO. Second, the attacker was able to mint new BUILD tokens and either sell them at the original price or swap the tokens in DeFi liquidity for other cryptocurrencies, taken advantage of the fact that the new supply of BUILD tokens was not yet “priced in.”

Case study: Beanstalk DAO flash loan governance attack

“In another instance, Beanstalk, a stablecoin protocol, found itself susceptible to governance attack via flashloan. An attacker took out a loan to acquire enough of Beanstalk’s governance token to instantly pass a malicious proposal that allowed them to seize \$182 million

of Beanstalk’s reserves. Unlike the Steem attack, this one happened within the span of a single block, which meant it was over before anyone had time to react.”⁸⁶

TTP: Transferring Funds to Third-Party During Trial or Legal Proceeding

Case Study: Helix Mixer Brothers⁸⁷

“L.H.” was the operator of a darknet mixer called Helix. L.H. and his brother, “G.H.”, conspired to transfer some of the cryptocurrency funds from L.H. to G.H. to shield the criminal proceeds from asset forfeiture. In 2021, L.H. pleaded guilty to money laundering conspiracy. In 2023, G.H. was sentenced to prison for stealing over 712 BTC (worth about \$4.8M at the time); G.H. agreed to the forfeiture of cryptocurrencies derived from the theft, including 647.41 BTC, 2.14 ETH, and 17.4M Dogecoin (DOGE). Forfeitable properties are valued at over \$20M due to market increases between the time of the theft and the forfeiture.

In February 2020, L.H. was arrested for his operation of the mixer Helix. Helix laundered over 350,000 BTC (worth over \$300M at the time of the transactions) from darknet markets and other illicit sources. Law enforcement seized a cryptocurrency hardware storage device containing illegal proceeds from Helix. The funds were subject to forfeiture in the criminal case, but law enforcement was initially unable to recover the BTC on the device due its security.

G.H. knowingly transferred his brother’s funds subject to forfeiture. G.H. was stealing those funds and obstructing the pending criminal forfeiture proceeding involving his brother. G.H. used L.H.’s credentials to recreate BTC wallets stored on L.H.’s device that had been seized by law enforcement. G.H. transferred the 712 BTC to his own wallets. G.H. then laundered the proceeds through two online bitcoin mixer services and used the laundered bitcoins to finance large purchases and other expenditures.

Other Examples

- Divorce Cases: There have been several news stories regarding one spouse attempting to conceal marital assets from the other using cryptocurrency during a divorce or defensively in the event of a potential future divorce. (SOURCES)
- FTX exchange hacked during bankruptcy

Summary from AEP 2022 *Ransomware Attacks on Critical Infrastructure Sectors*⁸⁸

Ransomware is cryptocurrency-enabled, but extorted funds typically do not start as cryptocurrency.

Dollars or other fiat

The funds would likely start in the victim's USD bank account with a domestic financial institution (FI). Funds would be sent to a professional ransom intermediary (e.g., Digital forensics and incident response (DFIR) companies; cyberinsurance companies (CICs), which may have in-house DFIRs or reimburse victims for ransoms; and law firms that facilitate ransom payments, sometimes known as "breach coaches"). The professional ransom intermediary would purchase cryptocurrency by sending USD from its bank to the centralized cryptocurrency exchange's (CEX) bank.

Cryptocurrency

The CEX would then credit the professional ransom intermediary's account with cryptocurrency. The intermediary would send the cryptocurrency to the ransomware gang. The ransomware gang would then provide the decryption keys to the victim. The ransomware gang may then launder the ransom on-chain using a variety of TTPs before cashing out.

Back to fiat

The ransomware gang will most likely attempt to cash out the majority of the funds by transferring the cryptocurrency from unhosted wallets to wallets controlled by high-risk exchanges and darknet markets, in exchange for various national currencies or precious metals. Cash-out operations serving ransomware gangs may overlap with other criminal activities, such as illicit drug trafficking and child exploitation. Therefore, tracking ransom payments may lead USG to professional money laundering operations linked to other crimes that are harder to detect. USG actions have focused on cash-out operations. [Case Study: Arrest of Anatoly Legkodymov, the founder of cryptocurrency exchange Bitzlato, in January 2023](#); [Case Studies: Hydra and Dream Market Shutdowns](#)

Asset Seizures and Clawbacks

As noted in the 2022 AEP, clawbacks (i.e. seizing a specific ransom from a ransomware gang and returning those funds to the specific victim that paid the ransom) do not make

economic sense as federal government policy. Clawbacks shift the incentives of business owners and operators toward paying a ransom over investing in defensive cybersecurity measures. Additionally, a focus on clawbacks inherently prioritizes victims that choose to pay ransoms over victims who refuse to pay. Rather than triaging the impact of events based on the monetary value of ransom payments, LE should prioritize responses based on the impact of the ransomware incident itself.

For example, suppose two regional power companies are hit by ransomware on the same day, causing power outages to 100,000 customers each. The first power company pays the ransom of \$1M in BTC. The second power company refuses to pay, reasoning that they may be hit again or that their payment would incentivize future attacks on other firms in the same sector. LE should prioritize responding to the second incident, investigate the breach, and mitigate the damage; however, a strategic focus on clawbacks would instead have LE track and attempt to seize the BTC paid in the first incident.

NFTs: Rug Pulls and Wash Trading

Definition: “A ‘rug pull’ refers to a scenario where the creator of an NFT and/or gaming project solicits investments and then abruptly abandons a project and fraudulently retains the project investors’ funds.”⁸⁹

Case Study: Frosties/Embers NFT Rug Pull

In early 2022, the DOJ charged two in a criminal complaint with conspiracy to commit wire fraud and conspiracy to commit money laundering, in connection with a million-dollar scheme to defraud purchasers of NFTs.

1. First rug pull project “Frosties,” promised NFT owner rewards like “giveaways, early access to a metaverse game, and exclusive mint passes to upcoming Frosties seasons” in January 2022.
2. Second (attempted) rug pull project “Embers” was in process before the March 2022 arrests.

*Wash Trading*⁹⁰

“NFT wash trading exists in a murky legal area. While wash trading is prohibited in conventional securities and futures, wash trading involving NFTs has yet to be the subject of an enforcement action. However, that could change as regulators shift focus and apply existing anti-fraud authorities to new NFT markets.” Chainalysis determined that in 2022, the majority of wash trades in NFTs were not profitable, but that the strategy was net profitable for NFT

wash traders. In addition to NFT wash trading, the creation of new ERC-20 “altcoins” on the Ethereum blockchain often involved wash trading as part of a pump and dump scheme.⁹¹

Dusting Attacks Following Tornado Cash Sanctions

“Dusting” is sending small-value cryptocurrency transactions to many wallets, somewhat analogous to “smurfing,” although “dusting” may be conducted by a single individual. Ethereum users cannot reject payments into a standard Ethereum wallet address, because most blockchains are append-only ledgers. However, certain smart contracts may link to “sanctions oracles,” such as Chainalysis, which allow the linked smart contract to reject payments that involve a sanctioned wallet address.⁹²

A Tornado Cash user anonymously exploited these features to transferred 0.1 Ethereum to many wallets known to be controlled by celebrities and prominent figures in the cryptocurrency world. Some of these users noted that after these “dusting attacks,” they were unable to access the front-end for “web3 DApps” due to those DApps associating them with an OFAC-sanctioned entity using blockchain analytics-based compliance smart contracts.

Similarly, certain NFTs connected to previous OFAC SDNs were removed from NFT marketplaces like OpenSea. Even though the NFTs technically still exist on the blockchain, they are effectively unusable, as marketplaces and web3 wallets APIs blocked access to sanctioned NFTs.⁹³

OFAC is aware of reports following the August 8, 2022 designation of Tornado Cash that certain U.S. persons may have received unsolicited and nominal amounts of virtual currency or other virtual assets from Tornado Cash smart contracts, a practice commonly referred to as “dusting.” Technically, OFAC’s regulations would apply to these transactions. To the extent, however, these “dusting” transactions have no other sanctions nexus besides Tornado Cash, OFAC will not prioritize enforcement against the delayed receipt of initial blocking reports and subsequent annual reports of blocked property from such U.S. persons. Persons who received a “dusting” transaction can also apply to OFAC for a specific license.

Impact on Government and Private Sector

Public-Private Partnerships

On March 2, 2023, the Biden Administration released the 35-page National Cybersecurity Strategy, outlining the approach the Administration is taking to “better secure

cyberspace and ensure the United States is in the strongest possible position to realize all the benefits and potential of our digital future.” This strategy places a strong emphasis on the importance of collaboration between the public and private sectors in matters of cybersecurity. The strategy calls for private sector partners to join forces by way of participating in the efforts of nonprofit organizations that also collaborate with the Federal Government, specifically naming the National Cyber-Forensics and Training Alliance (“NCFTA”) as an example of one of these nonprofits.

The National Cyber-Forensics and Training Alliance (NCFTA) is a nonprofit corporation “focused on identifying, mitigating, and disrupting cyber-crime threats globally.” The NCFTA was created in 2002, intentionally bringing together partners in various industries such as finance, academia, and law enforcement, with the purpose of “establishing a neutral, trusted environment that enables two-way information sharing with the ultimate goal to identify, mitigate, disrupt, and neutralize cyber threats. Through the NCFTA, private industry and government are able to work together in this neutral, trusted environment.” The NCFTA is an amazing resource and powerful vehicle, through which both the public and private sectors can work together to combat illicit activity.

Per the National Cybersecurity Strategy, the NCFTA and similar nonprofit organizations are important means for forging essential relationships between the public and private sectors. These relationships are critical in the disruption of cybercrimes and the dismantling of the groups perpetrating these crimes. The White House emphasized that there is a need for the private sector to bring their unique insights and capabilities to the Federal agencies that have the authority to act on the intelligence that has been gathered. At the NCFTA, all partners from all sectors are encouraged to physically work on site, in the same space, if possible, in order to establish trusted relationships. Building these relationships allows partners to coordinate efforts and use of resources. However, the NCFTA is very conscious and mindful not to cross any ethical or legal boundaries through this collaboration. Furthermore, while the NCFTA is a shining example of public private partnership, it is not the only nonprofit working in this space, and thus partners are encouraged to explore all avenues available to build the relationships necessary to combat these illicit actors.⁹⁴⁹⁵

Advanced Tools and Traditional Methods

Public-private collaboration is not the only mechanism in place to combat illicit cyber activity. The use of evolving vendor tools, such as Chainalysis, Ciphertrace, and TRM Labs, is essential in identifying and prosecuting cybercrime. Financial Institutions should continue to invest in blockchain forensic tools, as a part of their framework to combat cybercrime, and should continue to engage in blockchain analysis, to tackle the problem from a compliance

standpoint. Use of these tools has helped to identify, takedown, and prevent crimes, such as money laundering, sanctions evasion and darknet market activity, all operating on the blockchain. Government agencies should also continue to invest in this technology to aid in their investigations and take downs of cyber-criminal groups. Other available and useful tools include those that aid in the gathering and organizing of open-source intelligence, as well as other data.

Prudent vendors, such as Chainalysis, are cognizant of, and champion, the critical importance of the public-private partnerships in the fight against cybercrime. In Chainalysis' 2023 Cryptocrime Report, it states that “[a]s cryptocurrency continues to grow, it’s imperative that the public and private sectors work together to ensure that users can transact safely, and that criminals can’t abuse these new assets...[and to] equip law enforcement, regulators and compliance professionals with the knowledge to more effectively prevent, mitigate and investigate cryptocurrency-based crime.” A unified front across the public and private sector, in understanding our roles, and how we can form a collaborative effort in our responses to this crime, is necessary.⁹⁶

We should also continue to use traditional methods and policies, to combat illicit cyber activity. An example of these methods is, reporting activity and tagging it so that law enforcement knows which filings are related to which types of crimes. For instance, filing Suspicious Activity Reports (“SARs”) and tagging the activity per FinCEN advisories. This is yet, another example of how the private sector can alert the government to activity observed, by way of the unique information that is available to these private institutions.

Emerging Policy

The field of cybercrime, and cyber policing and regulation is ever evolving. In recent months, it has become clear that the Securities and Exchange Commission (“SEC”) is going to be cracking down on classifying cryptocurrencies as securities, and in turn, through this legal action, could possibly shape the future of cryptocurrency. On June 6, 2023, the SEC filed a complaint against Coinbase Inc., and its holding company, Coinbase Global, Inc., alleging multiple violations of U.S. securities regulations. This complaint comes amongst other complaints by the SEC against several big players in the cryptocurrency sector, such as Binance, Kraken, and Gemini.

The SEC’s complaint against Coinbase alleges that the entities were operating an unregistered Securities Exchange, Broker, and Clearing Agency. The complaint alleges that “[t]he Coinbase Platform merges three functions that are typically separated in traditional securities markets—those of brokers, exchanges, and clearing agencies. Yet, Coinbase has never registered with the SEC as a broker, national securities exchange, or clearing agency, thus

evading the disclosure regime that Congress has established for our securities markets. All the while, Coinbase has earned billions of dollars in revenues by, among other things, collecting transaction fees from investors whom Coinbase has deprived of the disclosures and protections that registration entails and thus exposed to significant risk.”⁹⁷

In response, Coinbase filed a motion to dismiss the SEC’s suit, arguing that the SEC does not have the authority to bring these claims. Coinbase asserts that the assets being traded on their platforms are not securities because they are not investment contracts. This legal battle is of particular interest, as it possibly sets the stage for determining whether digital assets are securities, and what regulations are in place to govern these assets. At the same time, additional pressure is being placed on Congress to act on policy involving the crypto industry.⁹⁸ Furthermore, there is also uncertainty among the SEC and another federal regulator, the Commodity Futures Trading Commission (“CFTC”), over which agency oversees crypto assets.⁹⁹

The SEC Chair, Gary Gensler, believes most cryptocurrencies are securities, and therefore, the SEC has authority over these assets, whereas “the CFTC’s jurisdiction is implicated when a virtual currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce.”¹⁰⁰. This debate over authority has prompted Congress to act, and in June of 2023 a bill has been introduced to propose a framework to clarify each agency’s role. The actions by the SEC, CFTC, and perhaps eventually Congress, will help to shape how crypto crime is addressed in the future, at least in the United States.

Leveraging IC3 Data

The FBI’s Internet Crime Complaint Center (“IC3”) is a central hub put in place by the Federal Government to both report cybercrime, and to educate the Public about the latest cyber threats. The IC3 performs analysis of the complaints received, to aid in freezing assets, and partners with private sector, as well as Local, State and Federal agencies, via referrals, to investigate these complaints. Cybercrime is something that generally goes underreported as victims are often embarrassed or are in denial about what has occurred. The FBI encourages all victims, as well as partners in the fight against cybercrimes, to report all incidents, in order to help aid investigations and protect citizens. Therefore, it is important to inform the Public, as well as, State and Local agencies, on how to report cybercrimes.¹⁰¹

Specific gaps in information have been identified as issues, with regards to best practices when using the IC3’s site, and in general investigations when gathering evidence related to cybercrime. One of the gaps that often occurs with IC3 data is that law enforcement cannot always use the data directly from the IC3 database due to issues with the way the data has been entered or due to a lack of foundation for the evidence. To help with these issues,

several improvements can be made. For instance, informing the Public that the wallets and transaction hashes added to IC3 complaints are case sensitive. In addition to submitting data into IC3, victims should work with law enforcement to separately preserve relevant data for evidentiary purposes and law enforcement should have resources in place to quickly capture and preserve digital evidence. For example, where there is a victim that no longer needs their crypto wallet and will give consent, it's helpful if law enforcement obtains the seed phrase for that specific wallet. This allows law enforcement to re-establish the wallet, for evidence purposes, to say what happened, and what the victim/witness did or did not authorize.

In addition, there is a need for education on the digital identifiers that should be obtained in cybercrime investigations, and how to preserve this digital evidence in a way that can be used in court. For example, usernames, emails, and phone numbers, are extremely helpful, as well as obtaining IP addresses (provides venue, as well as good corroborating evidence as to who may be the perpetrator). If a victim, for instance, is receiving emails from someone, law enforcement can exploit the metadata of the email and find the sender's IP address. This is great to capture and document. Furthermore, there is a need for education on preserving screen shots of a scammer's online profile, in a way that allows the government to lay the foundation for the evidence – which should be a memo of who, what, when, where, and how the screenshots were obtained. There also needs to be a clearly defined person that can testify that they captured the screenshots. For social media, many of the services now provide a way to download your complete profile, including messages, etc. If the victim/witness is willing to do that, they can, but the officer should also obtain a consent from the victim/witness, in addition to the actual file that is obtained. Lastly, reporting any incidents involving cryptocurrency within the first 24 hours after the crime, is crucial when it comes to the success rate for recovery of assets.

Within the education vein is also the need to educate analysts, investigators, and various levels of law enforcement, inclusive of the intelligence community, about cryptocurrency, illicit tradecraft models, and how to detect red flag indicators of criminal or illicit conduct. As evidenced throughout a variety of the aforementioned case examples, cryptocurrency and emerging technologies are shifting the national security threat landscapes at incredible speeds. The need to not only adapt to these shifts and evolving threats is paramount to securing US national security. Enhanced training, continuity in training and best education practices are essential to mitigating this present threat landscape.

Moreover, there are some important takeaways, for public and private investigators, from the IC3s most recent report from 2022. These takeaways include, identifying that the most targeted areas for ransomware are healthcare, government and manufacturing. The top five crime types observed are tech support, extortion, non-payment/ non-delivery, personal

breach data, and Phishing (which is the top crime reported). The report also breaks down statistics of victim losses by location and age, which is helpful in building out typologies. The IC3's Recovery Asset Team (RAT) was established in 2018 and has a 73% success rate to date.¹⁰²

The private sector can learn to improve on their work with the data provided to IC3 and other reporting avenues. Specifically, the private sector can use this information to build out typologies and integrate those typologies within fraud protections, such as, transaction monitoring, as well as, with compliance techniques such as reporting. Entities can exploit the data via reports that are generated by the government based on the aggregated data they receive.

Both the IC3 and private sector have identified issues that, if addressed, can be helpful in improving the IC3 reporting process going forward. One issue that the IC3 is focusing on is the need to build out a cybercrime kill chain based on complaints received. Acting quickly plays a major role in recovering assets, and having a structured plan in place will only enhance results. The NCFTA and other groups have recognized that there is an overall awareness issue, when it comes to using the complaint center in general. There is a need to launch a campaign to raise awareness and knowledge that the IC3 hub exists. Focus on educating local law enforcement on how to properly input data into the database, and to ask the right questions when handling claims of cyber fraud, as stated above, is of the utmost importance. Victims feel more comfortable reporting crimes locally than they do reporting crimes to the Federal Government. Therefore, we need to equip these local offices with the tools they need to help their communities.

There is a unanimous need for the most up to date, aggregated information on these cybercrimes. Therefore, many efforts have been made to improve reporting and responses. The IC3 has made efforts to improve public awareness by asking field offices to push out information, such as information on the National Elder Fraud Hotline, an entity that will input IC3 data for the victims. The FBI has also established a virtual academy for all State and Local law enforcement. Furthermore, the NCFTA has noticed the benefit of shifting to work with cyber insurers, to help strategize ways that they can help their clients, so that they are able to provide this insurance going forward. Lastly, institutions are also participating in efforts to improve education and awareness. For instance, John Jay College of Criminal Justice recently received a grant to provide State and Local agencies with training on cryptocurrency. With these efforts, there is hope that the cyber world will be a safer place to navigate.

Future Regulations, Forecast, and Areas for Future Study

The US DOJ is keeping up with the pace of cryptocurrency crimes and illicit activity affiliated with digital assets through the formation of the National Cryptocurrency Enforcement Team. This team is composed of prosecutors with backgrounds in cryptocurrency, cybercrime, money laundering, and forfeiture which assures any digital asset related crimes can be handled and charged to the full extent. This team has a focus on pursuing exchanges, mixing/tumbling services, infrastructure providers, and any entities facilitating criminal activity in relation to digital assets. This team is also enhancing efforts to provide training to all levels of law enforcement to increase the capacity to investigate and prosecute digital asset related crimes not only in the U.S. but worldwide (since many cryptocurrency cases have a cross country nexus). This team has a collaboration with the FBI's Virtual Asset Exploitation Unit, which is comprised of a dedicated team of cryptocurrency experts dedicated to providing analysis, support, and training across the FBI. The formation of this team should substantially increase the amount of digital asset crimes prosecuted on a federal level and assist districts still in their infancy of trying digital asset crimes. However it appears on a state level authorities are becoming more adept at handling digital asset crimes as they increase in popularity and as new trainings have become readily available. In some cases state authorities may be better to pursue digital asset crimes with an international nexus due to international cryptocurrency exchanges and institutions being more likely to accept a state legal process (warrants to seize illicitly gained funds) as opposed to federal legal process. State warrants to seize funds for victims who have fallen victim to a cryptocurrency scam can be more streamlined and a better solution which exemplifies how crucial it is for federal law enforcement authorities to work with state authorities. The future pursuit and outcomes of digital asset oriented cases should be strongly monitored because they are and will continue to set the precedents needed to effectively combat illicit activity while the regulatory landscape is still under development.¹⁰³

Another area that can be explored further in the future is the adoption of central bank digital currencies. Bank of America has called the adoption of these currencies as inevitable however the need for these currencies has been up for debate and is already under a fair share of scrutiny. Multiple countries are in the process of implementing central bank digital currencies and the implementation should be monitored for U.S. adoption of such assets. AI will continue to be a growing factor in digital asset related illicit activity and criminals will increasingly find innovative ways to use AI as it becomes more developed. The greater adoption of AI will likely lead to greater adoption of digital currencies exposing people to the increased risks of utilizing digital currencies. Our group did not explore sanctioned digital asset related entities however this presents another area for further study. Sanctioning certain entities is a key solution to effectively pause illicit activity related to a certain service, address, and/or group of addresses.

The process of de-mixing transactions is another key area for future study. Although mixers are still difficult to trace through, more patterns these mixers are using are being identified to successfully trace through these services. Greater knowledge has to be provided to both stakeholders and consumers on how mixers operate and how they can be traced. Lastly aligned with mixers, new strategies and methods on tracing privacy coins are coming forward which is another key area to study as illicit actors turn to these privacy coins.

Cryptocurrency Naming Conventions (Refer to Appendix B for Naming Convention Chart)

Existing naming and abbreviation conventions are inconsistent with each other and inadequate for combating illicit activity in cryptocurrency. We propose a naming convention for the financial industry, law enforcement and USG, blockchain analytics, and media to avoid ambiguities in discussing cryptocurrency. The basis would be using a token-blockchain pair, with the option to omit the blockchain if and only if the currency is on its “native” blockchain. For example “ETH” could be used instead of “ETH-eth” for Ether on the Ethereum blockchain. On the other hand, the ambiguous phrase “ETH swapped for BTC on a DEX, followed by chain-hopping” would instead be written as “ETH-eth swapped for BTC-eth on a DEX, then bridged from BTC-eth to BTC-btc.” In line with this standard, we also recommend that reports citing dollar-equivalent totals for seizures also cite the quantities denominated of the underlying cryptocurrencies.

In the early days of Bitcoin, there was meant to be a distinction between lower-case “bitcoin” (the unit of currency) and upper-case “Bitcoin” (the concept or the blockchain). This distinction has largely been abandoned in common use. For example, *The AP Stylebook* in 2014 made the upper-lower distinction¹⁰⁴ In 2022: “Cryptocurrency, blockchain, bitcoin, NFT, Web3: Renamed entry combines formerly separate entries, adds NFT and Web3 and updates throughout. We now use lowercase bitcoin on all references.”¹⁰⁵

With the proliferation of “altcoins,”¹⁰⁶¹⁰⁷ abbreviations have proliferated with a variety of formats. Popular usage typically involves a three-letter abbreviation of the cryptocurrency’s name. Sometimes, a “wrapped” cryptocurrency may include a lower-case letter, such as “w” (like “wBTC”, i.e. Bitcoin that has been “wrapped” to be represented on another blockchain, usually Ethereum) or a lower-case abbreviation for the protocol (e.g., “renBTC”).

The US government sometimes follows the convention of foreign currency abbreviations, with non-government-issued currencies beginning with “X;” hence: “XBT,” “XMR,” or “XRP.” However, USG does not apply this rule consistently and often falls back on popular abbreviations like “DOGE.” OFAC FAQ 563: “What is the structure of a digital currency address on OFAC’s SDN List? Digital currency addresses listed on the SDN List include their

unique alphanumeric identifier (up to 256 characters) and identify the digital currency to which the address corresponds (e.g., Bitcoin (XBT), Ethereum (ETH), Litecoin (LTC), Neo (NEO), Dash (DASH), Ripple (XRP), Iota (MIOTA), Monero (XMR), and Petro (PTR))...”¹⁰⁸

Existing naming conventions have serious negative implications for investor protections, sanctions compliance, AML/CFT investigations, and law enforcement and criminal prosecutions. Consumer confusion can result from using a single abbreviation to refer to many cross-chain versions of a cryptocurrency despite different issuers and different backing (e.g., the Paxos “BUSD,” which was only authorized on Ethereum, but which Binance also issued on several alternate blockchains). For sanctions compliance, it is important for the Treasury to specify which blockchain or blockchains are involved in a designation. For AML/CFT investigators, it is important to understand if only a single blockchain is being used or several: this is particularly relevant to recent North Korean hacking of cross-chain “bridges” funding “half” of its nuclear missile program. Lastly, when evidence is being gathered during LE investigations and presented in legal documents like indictments, it is important for law enforcement to clearly state not only the name of a cryptocurrency involved but also the blockchain or blockchains on which the illicit activity was conducted.

Proposed names according to our proposed standardization

- Cryptocurrency: TOKEN-blockchain abbreviation format; e.g., BTC-eth
- Smart contracts: CONTRACT_blockchain abbreviation format; e.g., TORC_eth
- DeFi and dApps: Name (blockchain); e.g., Axie Infinity (eth)
- Three-letter abbreviations are preferred, four-letters if necessary.
- Preference for the blockchain sharing an abbreviation with the native token.

For an example using this terminology, consider the flow of funds in the North Korean Lazarus Group’s hack of Axie Infinity (see [Case Study: Axie Infinity](#)), including the use of Tornado Cash.¹⁰⁹

1A. Chainalysis: *“North Korea’s typical DeFi laundering technique has roughly five stages:*

1. *Stolen Ether sent to intermediary wallets*
2. *Ether mixed in batches using Tornado Cash*
3. *Ether swapped for bitcoin*
4. *Bitcoin* mixed in batches*
5. *Bitcoin* deposited to crypto-to-fiat services for cashout”*

1B. Above bullets re-written using the Proposed Standard: *North Korea’s typical DeFi laundering technique has roughly five stages:*

1. *Stolen Ether (ETH-eth) sent to intermediary eth wallets*
2. *ETH-eth mixed in batches using Tornado Cash (TORC_eth)*
3. *ETH-eth swapped for bitcoin (BTC-eth)*
4. *BTC-eth* mixed in batches*
5. *BTC-eth* (or BTC-btc*) deposited to crypto-to-fiat services for cashout”*

*Ambiguous with the information provided; no mention of bridging or chain-hopping. Therefore, the proposed abbreviation standard would require more explicit detail from primary and secondary sources, resulting in less information loss.

2A. Chainalysis: *“...the hacker bridged ETH from the Ethereum blockchain to the BNB chain and then swapped that ETH for USDD, which was then bridged to the BitTorrent chain. Lazarus Group carried out hundreds of similar transactions across several blockchains to launder the funds they stole from Axie Infinity, in addition to the more conventional Tornado Cash-based laundering we covered above.”*

2B. Above paragraph re-written using the Proposed Standard: *The hacker bridged ETH-eth to ETH-bsc, then swapped ETH-bsc for USDD-bsc, then bridged the USDD-bsc to USDD-bttc. Lazarus Group carried out hundreds of similar transactions across several blockchains to launder the funds they stole from Axie Infinity (eth), in addition to the more conventional TORC_eth laundering covered above.*

In a historic decision made as recently as 26 July, a congressional committee convened to advance a bipartisan bill that aims to develop a regulatory framework for cryptocurrencies, and codify federal oversight of the digital asset industry. This bill was passed by the House Financial Services Committee, and provides direct guidance on determining when a cryptocurrency is classified as a security or a commodity, ultimately expanding the Commodity Futures Trading Commission’s (CFTC) oversight of the crypto industry, while adding clarity to the SEC’s jurisdiction and perceived outreach, a common complaint amongst those employed within the commercial cryptocurrency sector. In light of the evolving criminal landscape cryptocurrencies have facilitated, the bill was drafted with the intent of targeting decentralized finance services (DeFi), sanctions evasion tactics, peer to peer exchange regulatory loopholes, as well as casinos and pawn shops. Additionally, the bill also aims at ensuring cryptocurrency kiosks do not become the future vector of money laundering.

As evidenced throughout the aforementioned examples, US adversaries and criminal enterprises worldwide are utilizing creative ways that are being further adapted every day to exploit the US financial system, evade sanctions, and illicitly launder their funds or digital assets. Due to a variety of regulatory blind spots and challenges law enforcement entities face,



targeted solutions and advanced methods of oversight are necessary in order enhance US capability to mitigate the national security threats adversaries pose.¹¹⁰¹¹¹

Analytic Dissemination Plan

List agencies that stand to benefit from research:

Securities and Exchange Commission

Cybersecurity & Infrastructure Agency

Financial Crimes Enforcement Network

Federal Bureau of Investigation

United States Secret Service

United States Postal Inspection Service

Homeland Security Investigations

Drug Enforcement Administration

Internal Revenue Service (Criminal Investigative Division)

U.S. Federal Reserve System

Office of the Comptroller of Currency

DISCLAIMER STATEMENT: The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Companies whose analysts participated in the Public-Private Analytic Exchange Program. This document is provided for educational and informational purposes only and may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.

Endnotes

1. <https://www.elliptic.co/blog/work-to-combat-sanctions-evasion-in-crypto>
2. [Russian Sanctions Evasion Puts Merchants and Banks at Risk](#)
3. [FinCEN and Bis Joint Alert](#)
4. <https://www.justice.gov/opa/pr/alleged-russian-cryptocurrency-money-launderer-extradited-united-states>
5. <https://www.coindesk.com/consensus-magazine/2023/06/09/where-the-mt-gox-money-went-new-details-in-the-btc-e-exchange-case/>
6. <https://www.justice.gov/opa/pr/russian-nationals-charged-hacking-one-cryptocurrency-exchange-and-illicitly-operating-another>
7. <https://www.coindesk.com/markets/2019/11/15/criminal-case-against-failed-wex-crypto-exchange-points-at-russian-law-enforcement/>
8. <https://home.treasury.gov/news/press-releases/jy1391>
9. <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf#page=40&zoom=100,0,0>
10. <https://www.cfr.org/blog/north-koreas-cryptocurrency-craze-and-its-impact-us-policy#:~:text=In%202022%20alone%2C%20North%20Korea,primary%20hacking%20outfits%20%80%94Lazarus%20Group.>
11. https://www.securitycouncilreport.org/atf/cf/%7B65BF9F9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2019_171.pdf
12. <https://asia.nikkei.com/Spotlight/Cryptocurrencies/South-Korea-asks-cyber-firms-for-advice-on-North-s-crypto-crimes#:~:text=North%20Korean%20hackers%20in%20particular,through%20them%2C%20according%20to%20Chainalysis.>
13. <https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army>
14. <https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html>
15. <https://www.cnas.org/publications/reports/following-the-crypto>
16. [Crypto Mixers and AML Compliance - Chainalysis](#)
17. <https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html>
18. <https://www.cnas.org/publications/reports/following-the-crypto>
19. <https://www.cnas.org/publications/reports/following-the-crypto>
20. <https://www.forbes.com/sites/thomasbrewster/2022/12/19/mexican-drug-gang-money-laundering-over-binance-crypto-exchange/?sh=34de37654a59>
21. <https://www.justice.gov/usao-sdca/pr/sophisticated-sinaloa-cartel-money-laundering-organization-dismantled>
22. <https://apnews.com/article/business-caribbean-mexico-crime-drug-cartels-1bb5ebf84fbf71baf6a845648bad4990>
23. <https://apnews.com/article/business-caribbean-mexico-crime-drug-cartels-1bb5ebf84fbf71baf6a845648bad4990>
24. [08 OnlineTrafficking Report Revised.pdf \(unodc.org\)](#)

25. <https://english.elpais.com/international/2023-04-17/fentanyl-experiments-crypto-payments-and-feeding-people-to-tigers-a-look-inside-the-criminal-empire-of-el-chapos-sons.html>
26. [08 OnlineTrafficking Report Revised.pdf \(unodc.org\)](#)
27. https://www.unodc.org/res/opioid-crisis/index_html/08 OnlineTrafficking Report Revised.pdf
28. https://www.unodc.org/res/opioid-crisis/index_html/08 OnlineTrafficking Report Revised.pdf
29. <https://www.memri.org/jttm/new-english-language-blog-suggests-using-bitcoin-send-millions-dollars-islamic-state>
30. <https://www.memri.org/reports/coming-storm-%E2%80%93-terrorists-using-cryptocurrency>
31. https://www.rand.org/pubs/research_reports/RR3026.html
32. <https://www.ioneday.com/en/insights/2023/06/cryptocurrencies-and-risk-under-the-antiterrorism-act#:~:text=In%202021%2C%20for%20example%2C%20Israel,than%20any%20other%20terrorist%20organization.>
33. <https://academic.oup.com/policing/article/15/4/2329/6365869>
34. <https://www.blackfog.com/ransomware-groups-recruiting-your-employees/>
35. <https://www.scmagazine.com/analysis/ransomware/are-cybercriminals-actively-recruiting-your-employees-to-attack-you-with-ransomware>
36. <https://www.washingtonpost.com/dc-md-va/2022/12/25/crypto-scam-pig-butchering/>
37. <https://www.eurojust.europa.eu/news/takedown-fraudulent-cryptocurrency-network-bulgaria-cyprus-and-serbia>
38. <https://cointelegraph.com/news/aussies-revealed-as-prime-targets-of-israel-crypto-scam-syndicate>
39. <https://www.ibtimes.com/crypto-scam-spanish-authorities-bust-international-criminal-organization-that-swindled-over-110m-3689518>
40. <https://www.justice.gov/opa/pr/two-estonian-citizens-arrested-575-million-cryptocurrency-fraud-and-money-laundering-scheme>
41. <https://www.justice.gov/usao-sdfl/pr/miami-man-charged-running-fraudulent-cryptocurrency-and-stock-investment-scheme>
42. <https://bitcoindepot.com/bdcheckout/>
43. <https://cointelegraph.com/news/libertyx-allows-btc-purchases-in-cash-at-7-eleven-cvs-and-rite-aid>
44. <https://www.wired.com/2013/10/bitcoin-atm-gallery/>
45. <https://www.cardcoins.co/>
46. <https://www.digitalmint.io/customer-support/faqs/what-is-a-btc-teller/>
47. <https://www.cryptodispensers.com/cdreload>
48. <https://www.coin.cloud/buy-online>
49. <https://www.fca.org.uk/news/news-stories/warning-illegal-crypto-atms-operating-uk>
50. <https://www.prweb.com/releases/2023/07/prweb19447334.htm#>

51. https://www.bloomberg.com/news/articles/2022-11-26/no-one-is-using-some-bitcoin-btc-atms-in-the-crypto-downturn?in_source=embedded-checkout-banner
52. <https://go.chainalysis.com/2023-crypto-crime-report.html>
53. <https://www.trmlabs.com/post/crypto-atm-payments-linked-to-known-scam-addresses>
54. <https://www.freep.com/story/money/personal-finance/susan-tompor/2022/09/23/bitcoin-atm-cryptocurrency-qr-code-scam/7842125001/>
55. <https://www.ctinsider.com/news/article/ct-bitcoin-atm-scam-state-police-17825279.php>
56. <https://nordvpn.com/research-lab/payment-card-details-theft/>
57. <https://www.cga.ct.gov/2023/TOB/H/PDF/2023HB-06752-R00-HB.PDF>
58. <https://legiscan.com/CA/bill/SB401/2023>

59. <https://decrypt.co/107441/monero-rolls-out-enhanced-privacy-features-with-hard-fork>
60. <https://bitcoinmagazine.com/culture/silk-road-darknet-market-testing-for-bitcoin>
61. <https://www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange-charged-processing-over-700-million>
62. [#1 Darknet Markets List 2023 \(darknetone.com\)](#)
63. <https://www.cnbc.com/2023/04/05/genesis-market-feds-sanctions.html>
64. <https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation>
65. <https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace>
66. <https://www.cnbc.com/2022/04/05/darknet-hydra-market-site-seized-and-shut-down-doj-says.html>
67. <https://www.zdnet.com/article/dark-web-crime-markets-targeted-by-recurring-ddos-attacks/>
68. <https://www.vice.com/en/article/wimw3w/dark-web-net-dream-market-closed-theories>
69. https://www.researchgate.net/publication/325375174_A_Practical_De-mixing_Algorithm_for_Bitcoin_Mixing_Services
70. <https://www.dea.gov/press-releases/2021/10/26/department-justice-announces-results-operation-dark-hunter>
71. <https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35>
72. [Darknet Cryptocurrency Exchanges - DarknetOne](#)
73. <https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3>
74. [The Chainalysis 2022 Crypto Crime Report](#)

75. [North Korean Bridge Hacks](#)
76. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/037/94/PDF/N2303794.pdf?OpenElement>
77. <https://www.bbc.com/news/stories-57520169>

78. https://www.wsj.com/articles/how-north-koreas-hacker-army-stole-3-billion-in-crypto-funding-nuclear-program-d6fe8782?reflink=desktopwebshare_permalink&st=d6ti8vz24jmxq0m
79. <https://www.forbes.com/sites/forbesbusinesscouncil/2022/05/17/code-is-law-during-the-age-of-blockchain/?sh=3352ea6a2adb>
80. <https://cryptoslate.com/scream-protocol-losses-millions-to-stablecoin-depeg/>
81. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/037/94/PDF/N2303794.pdf?OpenElement>
82. <https://docs.roninchain.com/docs/basics/introduction>
83. <https://whitepaper.axieinfinity.com/axs>
84. <https://www.bloomberg.com/opinion/articles/2023-06-12/three-arrows-had-a-fun-bubble#xj4y7vzkg>
85. <https://cryptobriefing.com/build-finance-dao-suffers-governance-takeover-attack/>
86. <https://a16zcrypto.com/posts/article/dao-governance-attacks-and-how-to-avoid-them/>
87. [man-sentenced-stealing-over-712-bitcoin-subject-forfeiture](https://www.fbi.gov/newsroom/press-releases/2023/06/12/man-sentenced-stealing-over-712-bitcoin-subject-forfeiture)
88. <https://www.dhs.gov/sites/default/files/2022-09/Ransomware%20Attacks%20.pdf>
89. <https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0>
90. <https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/>
91. <https://arxiv.org/pdf/2303.00810.pdf>
92. <https://go.chainalysis.com/chainalysis-oracle-docs.html>
93. [1078. Do OFAC reporting obligations apply to “dusting” transactions?](https://www.oia.gov/press/202306121078)
94. <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>
95. [About the NCFTA | Leading Cybercrime Analysts](https://www.ncfta.com/leading-cybercrime-analysts)
96. [https://go.chainalysis.com/rs/503-FAP-074/images/Crypto Crime Report 2023.pdf](https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf)
97. <https://storage.courtlistener.com/recap/gov.uscourts.nysd.599908/gov.uscourts.nysd.599908.1.0.pdf>
98. <https://www.reuters.com/legal/coinbase-facing-sec-lawsuit-says-regulator-lacks-police-power-over-crypto-2023-06-29/>
99. <https://www.npr.org/2023/06/10/1181242780/sec-gary-gensler-binance-coinbase-crypto-lawsuits-battle>
100. https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf
101. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
102. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
103. <https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team>
104. <https://twitter.com/APStylebook/status/438316517307215874?lang=en>
105. <https://www.apstylebook.com/help?query=bitcoin&button=>
106. <https://www.forbes.com/uk/advisor/investing/cryptocurrency/crypto-glossary-of-terms-acronyms/>

107. <https://abbreviations.yourdictionary.com/articles/major-cryptocurrency-abbreviations.htm>
108. <https://ofac.treasury.gov/faqs/topic/1626>
109. <https://blog.chainalysis.com/reports/axie-infinity-ronin-bridge-dprk-hack-seizure/>
110. <https://www.reuters.com/technology/us-congressional-committee-set-weigh-crypto-bills-2023-07-26/>
111. <https://www.warner.senate.gov/public/index.cfm/2023/7/bipartisan-u-s-senators-unveil-crypto-anti-money-laundering-bill-to-stop-illicit-transfers>



Citations Separated by Section

Citations for Current Use of Digital Assets by Illicit Actors & Criminal Groups

(U) | Elliptic | March 2022 | Our work to Combat Sanctions Evasion in Crypto | <https://www.elliptic.co/blog/work-to-combat-sanctions-evasion-in-crypto>

(U) | Recorded Future By Insikt Group | March 2022 | Russian Sanctions Evasion Puts Merchants and Banks at Risk | <https://go.recordedfuture.com/hubfs/reports/cta-2023-0323.pdf>

(U) – Fincen & BIS | June 2022 | FIN-2022-Alert003 | [FinCEN and Bis Joint Alert](#)

(U) | U.S. Dept. of Justice | August 2022 | Alleged Russian Cryptocurrency Money Launderer Extradited to United States | <https://www.justice.gov/opa/pr/alleged-russian-cryptocurrency-money-launderer-extradited-united-states>

(U) | CoinDesk | June 2023 | Where the Mt. Gox Money Went: New Details in the BTC-e Exchange Case | <https://www.coindesk.com/consensus-magazine/2023/06/09/where-the-mt-gox-money-went-new-details-in-the-btc-e-exchange-case/>

(U) | U.S. Dept. of Justice | June 2023 | Russian Nationals Charged With Hacking One Cryptocurrency Exchange and Illicitly Operating Another | <https://www.justice.gov/opa/pr/russian-nationals-charged-hacking-one-cryptocurrency-exchange-and-illicitly-operating-another>

(U) | CoinDesk | Nov. 2019 | Criminal Case Against Failed WEX Crypto Exchange Points at Russian Law Enforcement | <https://www.coindesk.com/markets/2019/11/15/criminal-case-against-failed-wex-crypto-exchange-points-at-russian-law-enforcement/>

(U) | U.S. Dept. of Treasury | April 2023 | Treasury Releases 2023 DeFi Illicit Finance Risk Assessment | <https://home.treasury.gov/news/press-releases/jy1391>

(U) | U.S. Dept of Treasury | April 2023 | Illicit Finance Risk Assessment of Decentralized Finance | <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf#page=40&zoom=100,0,0>

(U) | Council on Foreign Relations | Jan. 2023 | North Korea's Cryptocurrency Craze and its Impact on U.S. Policy | <https://www.cfr.org/blog/north-koreas-cryptocurrency-craze-and-its->

[impact-us-policy#:~:text=In%202022%20alone%2C%20North%20Korea,primary%20hacking%20outfits%E2%80%94Lazarus%20Group](#)

(U) | United Nations Security Council | March 2019 | Letter dated 21 February 2019 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council | https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2019_171.pdf

(U) | Nikkei Asia | July 2023 | South Korea asks cyber firms for advice on North's crypto crimes | <https://asia.nikkei.com/Spotlight/Cryptocurrencies/South-Korea-asks-cyber-firms-for-advice-on-North-s-crypto-crimes#:~:text=North%20Korean%20hackers%20in%20particular,through%20them%2C%20according%20to%20Chainalysis>

(U) | The New Yorker | April 2021 | The Incredible Rise of North Korea's Hacking Army | <https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army>

(U) | The New York Times | June 2022 | How North Korea Used Crypto to Hack Its Way Through the Pandemic | <https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html>

(U) | Center for a New American Security | Feb. 2022 | Following the Crypto | <https://www.cnas.org/publications/reports/following-the-crypto>

(U) | Chainalysis | Aug. 2022 | Crypto Mixers and AML Compliance | <https://blog.chainalysis.com/reports/crypto-mixers/>

(U) | The New York Times | June 2022 | How North Korea Used Crypto to Hack Its Way Through the Pandemic | <https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html>

(U) | Center for a New American Security | Feb. 2022 | Following the Crypto | <https://www.cnas.org/publications/reports/following-the-crypto>

(U) | Forbes | Dec. 2022 | Global Drug Conspiracy Used Binance To Launder Millions In Crypto, DEA Investigation Finds | <https://www.forbes.com/sites/thomasbrewster/2022/12/19/mexican-drug-gang-money-laundering-over-binance-crypto-exchange/?sh=34de37654a59>

(U) | U.S. Attorney's Office | April 2023 | Sophisticated Sinaloa Cartel Money Laundering Organization Dismantled | <https://www.justice.gov/usao-sdca/pr/sophisticated-sinaloa-cartel-money-laundering-organization-dismantled>

(U) | Associated Press | March 2022 | Mexican cartels turn to bitcoin, internet, e-commerce | <https://apnews.com/article/business-caribbean-mexico-crime-drug-cartels-1bb5ebf84fbf71baf6a845648bad4990>

(U) | United Nations Office on Drugs and Crime | 2022 | The Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribbean | https://www.unodc.org/res/opioid-crisis/index_html/08_OnlineTrafficking_Report_Revised.pdf

(U) | El Pais | April 2023 | Fentanyl experiments, crypto payments and feeding people to tigers: A look inside the criminal empire of El Chapo's sons | <https://english.elpais.com/international/2023-04-17/fentanyl-experiments-crypto-payments-and-feeding-people-to-tigers-a-look-inside-the-criminal-empire-of-el-chapos-sons.html>

(U) | Memri | July 2014 | New English-Language Blog Suggests Using Bitcoin To Send 'Millions Of Dollars' To The Islamic State | <https://www.memri.org/jttm/new-english-language-blog-suggests-using-bitcoin-send-millions-dollars-islamic-state>

(U) | Memri | Aug. 2019 | The Coming Storm – Terrorists Using Cryptocurrency | <https://www.memri.org/reports/coming-storm-%E2%80%93-terrorists-using-cryptocurrency>

(U) | RAND Corporation | 2019 | Terrorist Use of Cryptocurrencies | https://www.rand.org/pubs/research_reports/RR3026.html

(U) | Jones Day | June 2023 | Cryptocurrencies and Risk Under the Antiterrorism Act | <https://www.jonesday.com/en/insights/2023/06/cryptocurrencies-and-risk-under-the-antiterrorism-act#:~:text=In%202021%2C%20for%20example%2C%20Israel,than%20any%20other%20terrorist%20organization>

(U) | Oxford Academic | Sept. 2021 | Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing | <https://academic.oup.com/policing/article/15/4/2329/6365869>

Citations for Growth and Capacity of Criminal Groups Engaging in Illicit Digital Asset Activity

(U) | BlackFog | March 2022 | The New Insider Threat: Are ransomware groups recruiting your employees? | <https://www.blackfog.com/ransomware-groups-recruiting-your-employees/>

(U) | SCMEDIA | Nov. 2021 | Are cybercriminals actively recruiting your employees to attack you with ransomware? | <https://www.scmagazine.com/analysis/ransomware/are-cybercriminals-actively-recruiting-your-employees-to-attack-you-with-ransomware>

(U) | The Washington Post | Dec. 2022 | <https://www.washingtonpost.com/dc-md-va/2022/12/25/crypto-scam-pig-butchering/>

(U) Eurojust | Feb. 2023 | Takedown of fraudulent cryptocurrency network in Bulgaria, Cyprus, and Serbia | <https://www.eurojust.europa.eu/news/takedown-fraudulent-cryptocurrency-network-bulgaria-cyprus-and-serbia>

(U) | Cointelegraph | Feb. 2023 | Aussies revealed as prime targets of Israel scam syndicate | <https://cointelegraph.com/news/aussies-revealed-as-prime-targets-of-israel-crypto-scam-syndicate>

(U) | International Business Times | April 2023 | Crypto Scam: Spanish Authorities Bust International Criminal Organization That Swindled Over \$110M | <https://www.ibtimes.com/crypto-scam-spanish-authorities-bust-international-criminal-organization-that-swindled-over-110m-3689518>

(U) | U.S. Dept. of Justice | Nov. 2022 | Two Estonian Citizens Arrested in \$575 Million Cryptocurrency Fraud and Money Laundering Scheme | <https://www.justice.gov/opa/pr/two-estonian-citizens-arrested-575-million-cryptocurrency-fraud-and-money-laundering-scheme>

(U) | U.S. Dept. of Justice | March 2023 | Miami Man Charged for Running Fraudulent Cryptocurrency and Stock Investment Scheme | <https://www.justice.gov/usao-sdfl/pr/miami-man-charged-running-fraudulent-cryptocurrency-and-stock-investment-scheme>

Citations for Cryptocurrency Point-of-Sales

(U) | Elliptic | March 2022 | Our work to Combat Sanctions Evasion in Crypto | <https://www.elliptic.co/blog/work-to-combat-sanctions-evasion-in-crypto>

(U) Bitcoin Depot | 2022 | BitcoinDepot: How it Works | <https://bitcoindepot.com/bdcheckout/>

(U) | CoinTelegraph | June 2020 | LibertyX Allows BTC Purchases in Cash at 7-Eleven, CVS, and Rite Aid | <https://cointelegraph.com/news/libertyx-allows-btc-purchases-in-cash-at-7-eleven-cvs-and-rite-aid>

(U) | Wired | Oct. 2013 | Take a Tour of Robocoin, the World's First Bitcoin ATM | <https://www.wired.com/2013/10/bitcoin-atm-gallery/>

(U) | CardCoins | 2023 | Homepage | <https://www.cardcoins.co>

(U) | Digital Mint | 2023 | What is a Bitcoin teller window? | <https://www.digitalmint.io/customer-support/faqs/what-is-a-btc-teller>

(U) | Cryptodispensers | 2023 | Homepage | <https://www.cryptodispensers.com/cdreload>

(U) | CoinCloud | 2023 | Homepage | <https://www.coin.cloud/buy-online>

(U) | Financial Conduct Authority | Nov. 2022 | Warning on illegal crypto ATMs operating in the UK | <https://www.fca.org.uk/news/news-stories/warning-illegal-crypto-atms-operating-uk>

(U) | Bloomberg | Nov. 2022 | Crypto's Brutal Slump Has Finally Caught Up With Bitcoin ATMs | https://www.bloomberg.com/news/articles/2022-11-26/no-one-is-using-some-bitcoin-btc-atms-in-the-crypto-downturn?in_source=embedded-checkout-banner#xi4y7vzkg

(U) | Chainalysis | 2023 | The 2023 Crypto Crime Report | <https://go.chainalysis.com/2023-crypto-crime-report.html>

(U) | TRMLabs | Jan 2023 | Crypto ATM Payments Linked to Known Scam Addresses | <https://www.trmlabs.com/post/crypto-atm-payments-linked-to-known-scam-addresses>

(U) | Detroit Free Press | Sept. 2022 | Easy-to-find bitcoin ATMs, QR codes used as weapon by scammers: What to know | <https://www.freep.com/story/money/personal-finance/susan-tompor/2022/09/23/bitcoin-atm-cryptocurrency-qr-code-scam/7842125001/>

(U) | CT Insider | March 2023 | This CT man was duped into putting his life savings in a Bitcoin ATM. Now there's no getting it back | <https://www.ctinsider.com/news/article/ct-bitcoin-atm-scam-state-police-17825279.php>

(U) | NordVPN | 2023 | Analyzing 4 million payment card details found on the dark web | <https://nordvpn.com/research-lab/payment-card-details-theft/>

(U) | State of Connecticut General Assembly | Jan. 2023 | Raise Bill No. 6752 |
<https://www.cga.ct.gov/2023/TOB/H/PDF/2023HB-06752-R00-HB.PDF>

(U) | California Senate | July 2023 | CA SB401 2023-2024 Regular Session |
<https://legiscan.com/CA/bill/SB401/2023>

Citations for Generative AI and Cybercrime: Unraveling the Impact on Digital Assets and Cryptocurrencies

No formal citations for this section, just ChatGPT by OpenAI was used.

Citations for Darknet Market Use of Digital Assets

(U) | Decrypt | Aug 2022 | Monero Rolls Out Enhanced Privacy Features With Hard Fork |
<https://decrypt.co/107441/monero-rolls-out-enhanced-privacy-features-with-hard-fork>

(U) | Dept. of Justice | APRIL 2021 | Individual Arrested and Charged Operating Notorious Cryptocurrency Mixer <https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer>

(U) | Bitcoin Magazine | NOV 2022 | SILK ROAD WAS THE DARKNET MARKET TESTING GROUND FOR BITCOIN | <https://bitcoinmagazine.com/culture/silk-road-darknet-market-testing-for-bitcoin>

(U) | Dept. of Justice | JAN 2023 | Founder and Majority Owner of Cryptocurrency Exchange Charged with Processing Over \$700 Million of Illicit Funds |
<https://www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange-charged-processing-over-700-million>

(U) | Darknetone | 2023 | Markets | <https://darknetone.com/markets/>

(U) | CNBC | APRIL 2023 | Criminal marketplace Genesis seized by FBI in larger fight against state-backed cybercrime | <https://www.cnbc.com/2023/04/05/genesis-market-feds-sanctions.html>

(U) | Dept. of Justice | APRIL 2023 | Criminal Marketplace Disrupted in International Cyber Operation | <https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation>

(U) | Dept. of Justice | APRIL 2023 | Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace | <https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace>

(U) | CNBC | APRIL 2022 | World's biggest darknet marketplace, Russia-linked Hydra Market, seized and shut down, DOJ says | <https://www.cnbc.com/2022/04/05/darknet-hydra-market-site-seized-and-shut-down-doj-says.html>

(U) | ZDNET | APRIL 2019 | Dark web crime markets targeted by recurring DDoS attacks | <https://www.zdnet.com/article/dark-web-crime-markets-targeted-by-recurring-ddos-attacks/>

(U) | VICE | APRIL 2019 | The World's Biggest Dark Net Market Has Shut – What Next? | <https://www.vice.com/en/article/wjmw3w/dark-web-net-dream-market-closed-theories>

(U) | ResearchGate | May 2018 | A Practical De-mixing Algorithm for Bitcoin Mixing Services | https://www.researchgate.net/publication/325375174_A_Practical_De-mixing_Algorithm_for_Bitcoin_Mixing_Services

(U) | DEA | OCT 2021 | Department of Justice Announces Results of Operation Dark HunTor | <https://www.dea.gov/press-releases/2021/10/26/department-justice-announces-results-operation-dark-huntor>

(U) | Dept. of Justice | June 2018 | First Nationwide Undercover Operation Targeting Darknet Vendors Results in Arrests of More Than 35 Individuals Selling Illicit Goods and the Seizure of Weapons, Drugs and More Than \$23.6 Million | <https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35>

(U) | Darknetone | 2023 | Darknet Cryptocurrency Exchanges | <https://darknetone.com/darknet-cryptocurrency-exchanges/>

(U) | Dept. of Justice | March 2013 | Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over \$3 Billion of Unlawful Transactions | <https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3>

(U) | Chainalysis | FEB 2023 | The Chainalysis 2022 Crypto Crime Report | [The Chainalysis 2022 Crypto Crime Report](#)

Citations for The Evolving Use of Digital Assets by Criminal Organizations

(U) | U.S. Dept. Treasury Office of Foreign Assets Control | Nov. 2022 | Do OFAC Reporting obligations apply to “dusting” transactions? | <https://ofac.treasury.gov/faqs/1078>

(U) | United Nations | March 2023 | N2303794 | <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/037/94/PDF/N2303794.pdf?OpenElement>

(U) | BBC News | June 2021 | The Lazarus heist: How North Korea almost pulled off a billion-dollar hack | <https://www.bbc.com/news/stories-57520169>

(U) | Wall Street Journal | June 2023 | How North Korea’s Hacker Army Stole \$3 Billion in Crypto, Funding Nuclear Program | https://www.wsj.com/articles/how-north-koreas-hacker-army-stole-3-billion-in-crypto-funding-nuclear-program-d6fe8782?reflink=desktopwebshare_permalink&st=d6ti8vz24jmxq0m

(U) | Forbes | May 2022 | Code is Law | During the Age of Blockchain | <https://www.forbes.com/sites/forbesbusinesscouncil/2022/05/17/code-is-law-during-the-age-of-blockchain/?sh=6b11796e2adb>

(U) | CryptoSlate | May 2022 | Scream protocol losses millions to stablecoin depeg | <https://cryptoslate.com/scream-protocol-losses-millions-to-stablecoin-depeg/>

(U) | Couldn’t get to link <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/037/94/PDF/N2303794.pdf?OpenElement>

(U) | Ronin | May 2023 | Introduction to Ronin | <https://docs.roninchain.com/docs/basics/introduction>

(U) | Axie Infinity | June 2023 | Axie Infinity Shards | <https://whitepaper.axieinfinity.com/axs>

(U) | Bloomberg | June 2023 | Three Arrows Had a Fun Bubble | <https://www.bloomberg.com/opinion/articles/2023-06-12/three-arrows-had-a-fun-bubble#xj4y7vzkg>

(U) | Crypto Briefing | Feb. 2022 | Build Finance DAO Suffers Governance Takeover Attack | <https://cryptobriefing.com/build-finance-dao-suffers-governance-takeover-attack/>

(U) | a16zcrypto | July 2022 | DAO governance attacks, and how to avoid them | <https://a16zcrypto.com/posts/article/dao-governance-attacks-and-how-to-avoid-them/>

(U) | U.S. Dept. of Justice | April 2023 | Man Sentenced for Stealing Over 712 Bitcoin Subject to Forfeiture | <https://www.justice.gov/opa/pr/man-sentenced-stealing-over-712-bitcoin-subject-forfeiture#:~:text=An%20Ohio%20man%20was%20sentenced,a%20then%20pending%20criminal%20case.>

(U) | DHS I&A Analytic Exchange Program | Sept. 2022 | Ransomware Attacks on Critical Infrastructure Sectors | <https://www.dhs.gov/sites/default/files/2022-09/Ransomware%20Attacks%20.pdf>

(U) | U.S. Attorney's Office | March 2022 | Two Defendants Charged In Non-Fungible Token ("NFT") Fraud And Money Laundering Scheme | <https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0>

(U) | Chainalysis | Feb. 2022 | Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class | <https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/>

(U) | ARXIV | May 2023 | Of Degens and Defrauders: Using Open-Source Investigative Tools to Investigate Decentralized Finance Frauds and Money Laundering | <https://arxiv.org/pdf/2303.00810.pdf>

(U) | Chainalysis | 2022 | Chainalysis oracle for sanctions screening | <https://go.chainalysis.com/chainalysis-oracle-docs.html>

(U) | U.S. Dept. Treasury Office of Foreign Assets Control | Nov. 2022 | Do OFAC Reporting obligations apply to "dusting" transactions? | <https://ofac.treasury.gov/faqs/1078>

Citations for Impact on Government and Private Sector | Future Regulations, Forecast, and Areas for Future Study

(U) | U.S. Dept. Treasury Office of Foreign Assets Control | Nov. 2022 | Do OFAC Reporting obligations apply to "dusting" transactions? | <https://ofac.treasury.gov/faqs/1078>

(U) | The White House | March 2023 | National Cybersecurity Strategy | <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>



(U) | NCFTA | 2023 | Who we are | <https://www.ncfta.net/who-we-ara>

(U) | Chainalysis | March 2023 | Chainalysis Crypto Crime Report 2023 | [https://go.chainalysis.com/rs/503-FAP-074/images/Crypto Crime Report 2023.pdf](https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf)

(U) | U.S. District Court Southern District of New York | June 2023 | SEC against Coinbase Complaint | <https://storage.courtlistener.com/recap/gov.uscourts.nysd.599908/gov.uscourts.nysd.599908.1.0.pdf>

(U) | Reuters | June 2023 | Coinbase, facing SEC lawsuit, says regulator lacks police power over crypto | <https://www.reuters.com/legal/coinbase-facing-sec-lawsuit-says-regulator-lacks-police-power-over-crypto-2023-06-29/>

(U) | NPR | June 2023 | Wall Street's top cop is determined to bring crypto to heel. He just took a big shot | <https://www.npr.org/2023/06/10/1181242780/sec-gary-gensler-binance-coinbase-crypto-lawsuits-battle>

(U) | U.S. CFTC | 2023 | Bitcoin Basics | https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf

(U) | FBI | 2022 | Internet Crime Report 2022 | https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

(U) | U.S. Dept. of Justice | Feb. 2022 | Justice Department Announces First Director of National Cryptocurrency Enforcement Team | <https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team>

(U) | Twitter-APStylebook | Feb 2014 | Status AP Style Tip | <https://twitter.com/APStylebook/status/438316517307215874?lang=en>

(U) | APStyle Book | 2023 | Bitcoin | <https://www.apstylebook.com/help?query=bitcoin&button=>

(U) | Forbes | Nov. 2022 | Cryptocurrency Glossary of Terms & Acronyms | <https://www.forbes.com/uk/advisor/investing/cryptocurrency/crypto-glossary-of-terms-acronyms/>

(U) | YourDictionary | Jan 2022 | Major Cryptocurrency Abbreviations | <https://abbreviations.yourdictionary.com/articles/major-cryptocurrency-abbreviations.html>



(U) | U.S. Dept of Treasury Office of Foreign Assets Control | Nov. 2018 | Questions on Virtual Currency | <https://ofac.treasury.gov/faqs/topic/1626>

(U) | Chainalysis | Sept. 2022 | \$30 Million Seized: How the Cryptocurrency Community Is Making It Difficult for North Korean Hackers To Profit | <https://blog.chainalysis.com/reports/axie-infinity-ronin-bridge-dprk-hack-seizure/>

(U) | Reuters | July 2023 | Crypto bill passes congressional committee in victory for industry | <https://www.reuters.com/technology/us-congressional-committee-set-weigh-crypto-bills-2023-07-26/>

(U) | Mark R. Warner | July 2023 | Bipartisan U.S. Senators Unveil Crypto Anti-Money Laundering Bill to Stop Illicit Transfers | <https://www.warner.senate.gov/public/index.cfm/2023/7/bipartisan-u-s-senators-unveil-crypto-anti-money-laundering-bill-to-stop-illicit-transfers>

Appendices

Appendix A: Cryptocurrency Brochure

Additional Resources

The following websites may provide additional information relating to fraud and fraud reporting.

www.ic3.gov

- Fraud types and schemes
- Report a crime

www.secretsservice.gov

- Cryptocurrency Awareness Hub
 - PSA videos
 - Common definitions
 - Crypto in the news

www.fbi.gov

- Cybersecurity Awareness Videos
- Submit a tip/report a crime

<https://consumer.ftc.gov>

- What to know about cryptocurrency

<https://sec.gov>

- Crypto Assets and Cyber Unit

<https://crypto3c.org/>

- Reporting on common scams

Commodity Futures Trading Commission

- [CFTC.gov/complaint](https://cftc.gov/complaint)

Tips to Protect Yourself from Fraud

Transactions involving digital assets can be overwhelming. Below are a few items to know to keep you and your digital assets safe from fraud.


Online Use and Wallets

- **NEVER** invest money you cannot afford to lose.
- Use 2-Factor Authentication (such as a password and a phrase, a fingerprint, or a confirmation text).
- Safeguard your passwords and do not repeat them or share them.
- Maintain your own private key for your digital wallet.
- Store your digital funds in a secure wallet.
- If you did not request to reset your password, do not click the link. Go directly to the website.
- If you receive a request to update information, go directly to your profile to update, do not click links you are not certain of.
- **DO NOT** store your recovery seed digitally. Keep it secure and in a non-electronic format.
- Read the fine print and know how to exit any investment you pursue.
- Always log out of your wallet and any sites you may have your wallet connected to.

Fraud Awareness

- If you are called and told a friend/family member needs money, **HANG UP**, and call the friend/family member directly to confirm.
- Do not send or receive funds from someone you do not know or on behalf of someone else.
- Beware of investment opportunities promising guaranteed returns or those sounding too good to be true.

You've been the victim of a scam, now what??



2023
Public-Private
Analytical Exchange Program

Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies

This program enables U.S. government analysts and private sector partners to gain a greater understanding of how their disparate, yet complimentary roles can work in tandem to ensure mission success. Participants work to create joint analytic products of interest to both the private sector and the U.S. Government.
This product was produced by AEP participants.

Where to report the fraud

In the event you, or someone you know, has become or thinks they have become the victim of a fraud, it is important to know where to go and how to report the fraud.

It is important to report fraud to the federal government; but you should also consider reporting any fraud to your local authorities such as state, county, and city police.

Prosecutors can use blockchain data analytics and traditional law enforcement techniques to identify and prosecute complex cryptocurrency investment schemes; price and market manipulation involving cryptocurrencies; unregistered cryptocurrency exchanges involved in fraud schemes; and insider trading schemes affecting cryptocurrency markets.

The Federal Bureau of Investigation (FBI) along with Internet Crime Complaint Center (IC3) lead in federal cyber frauds and crimes related investigations. IC3 review and research complaints, and send the information to federal, state, local, or international law enforcement agencies for possible criminal or civil action.

Below is a list of federal agencies where you can report a suspected fraud. Please see the reverse of this pamphlet for their website addresses.

- Federal Agencies
 - United States Secret Service
 - Federal Bureau of Investigation
 - Federal Trade Commission
 - United States Securities and Exchange Commission
 - Commodity Futures Trading Commission

How and why to report a fraud

In the event of a fraud, the two most important elements are a) reporting the fraud and b) preserving the data. The following tips will help you learn how to accurately preserve the data of the fraud.

Why Should You Report
Join the fight against internet crime! By reporting internet crimes, you are making difference by:

- Bringing criminals to justice
- Making our communities safer, both locally and nationally
- Helping law enforcement track trends and threats
- In some cases, even freeze stolen funds.
- With your help, we can and will respond faster, defend cyber networks better, and more effectively protect our nation.

How to Store Evidence
It is important that you keep any evidence you may have related to your complaint in a safe location in the event you are requested to provide them for investigative or prosecutive evidence.

Be sure to think outside of the box. Evidence can come in many forms and may be physical and digital. Below are some questions that may help you identify sources of evidence.

- Who have you interacted with? What was their name, title, or position?
- How did you interact with them? Was it on a website, social media, group chat, email, text message, phone call, or elsewhere?
- How did you exchange funds? Do you have receipts, cancelled checks, envelopes, prepaid cards?

Save any correspondence such as brochures and pamphlets, web page archives, emails, and other artifacts.

Web pages that are relevant to the scam can be archived in several ways. Services like Archive.org's Wayback Machine can be used to preserve website content.

There are specific attributes to cryptocurrency transactions that are important to record: transaction IDs, where you sent your crypto from (the address of your private wallet, account at a crypto exchange, etc.), and where you believe you were sending your funds (address and purported use).

Important: Cryptocurrency identifiers may be Case Sensitive, for example (bc1qWXX is not the same as bc1qwxx).

What happens next

When a crime is reported, it is natural to wonder what happens next. The below are possible next steps after reporting a fraud.

- FBI/IC3
 - Can rapidly deploy investigative teams located nationally and can provide technical assistance.
- United States Secret Service (USSS)
 - The nearest field office will assesses and activate law enforcement officers as needed.
- Department of Homeland Security (DHS)
 - The department's National Cybersecurity and Communications Center (NCCIC) assists owners in helping find weak spots, other who may be at risk, and share information with other public or private sectors.
- National Cyber Investigative Joint Task Force (NCIJTF)
 - Works together and shares information with other Law Enforcement agencies across the U.S. Government to protect people and put cyber criminals behind bars.
- Fusion Centers
 - Fusion centers share information and pass information between the federal, state, local, and private sectors. They can quickly share and provide information related to threats. A fusion Center can also help ensure common cyber policies, programs, and response plans to address known and possible threats, help exchange subject-matter expertise and help law enforcement and prosecution efforts.

Appendix B: Cryptocurrency Naming Conventions Chart

Cryptocurrency	Blockchain or Network	Common Abbreviation	Proposed Standardization
Bitcoin	Bitcoin	BTC or XBT	BTC or BTC-btc
Bitcoin (wrapped)	Ethereum	wBTC	BTC-eth
Ether	Ethereum	ETH	ETH or ETH-eth
Monero	Monero	XMR	XMR or XMR-xmr
Dogecoin	Dogecoin	DOGE	DOGE or DOGE-doge
Binance USD (Paxos/ERC-20)	Ethereum	BUSD	BUSD-eth
Binance USD (Binance)	Binance Smartchain (BSC)	BUSD	BUSD-bsc

USD Coin (ERC-20 token)	Ethereum	USDC	USDC-eth
USD Coin (ASA token)	Algorand	USDC	USD-asa
USD Coin (SPL token)	Solana	USDC	USD-sol
USD Coin (TRC-20 token)	TRON	USDC	USD-tron
Litecoin	Litecoin	LTC	LTC or LTC-ltc
Neo	Neo3	NEO	NEO-neo3
Dash	DASH	DASH	DASH-dash
Ripple	XRP Ledger (XRPL)	XRP	XRP-xrpl
Colombian CBDC (proposed)	XRP Ledger (XRPL)	Colombian Peso (COP; possibly)	COP-xrpl (tentative)
Ripple (BEP-20)	Binance Smartchain	XRP	XRP-bsc
Iota	IOTA 2.0	MIOTA	IOTA-iota2
Venezuelan Petro	NEM?	PTR	[uncertain]
Zcash	Zcash network	ZEC	ZEC or ZEC-zec
Ether (PoW)	Ethereum (PoW)	ETHW	ETHw-ethw
Ether (Classic)	Ethereum Classic	ETC	ETHC-ethc
Binance Coin	Binance Smartchain (BSC)	BNB	BNB-bsc
Tether (ERC-20)	Ethereum	USDT	USDT-eth
Dai (ERC-20)	Ethereum	DAI	DAI-eth
Tether (BEP-20)	Binance Smartchain	USDT	USDT-bsc
Tornado Cash mixer	Ethereum	N/A	TORC_eth
USDD stablecoin (ERC-20)	Ethereum	USDD	USDD-eth
USDD stablecoin (BEP-20)	Binance Smartchain	USDD	USDD-bsc
USDD stablecoin BitTorrent	BitTorrent Chain	USDD	USDD-bttc