

COMBATTING ILLICIT ACTIVITY UTILIZING FINANCIAL TECHNOLOGIES AND CRYPTOCURRENCIES



Abstract

Private and public sector analysts and subject matter experts working in the cyber financial landscape gathered through a series of meetings to examine the use of financial technologies and cryptocurrencies by illicit actors. The key research points investigated include 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 use associated with other emerging blockchain applications (i.e. NFTs). The research gathered from investigating these areas led to the development of suggested, effective changes to reduce illicit activity in this space and identifying the key stakeholders to implement these changes. This paper seeks to provide guidance in navigating cryptocurrencies, emerging digital payment solutions, and other blockchain applications to both consumers and stakeholders to minimize the illicit use of these platforms. While illicit use cannot be eliminated altogether, it can certainly be reduced with better consumer knowledge and better practices/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: Alexander Angert	FBI
Champion: Stephen Deininger	NSA
Kevin Lyons Sec+, CFE	U.S. Secret Service
Chris Kachenko	Federal Reserve Bank of Cleveland
Danie Evariste Saint Cyr, CPA, CFE, CCI	FBI
Kristen Peters	DoD
Mattonna Wahlgren, CFCS	Western Union
Madison Malarkey	Invesco
Kathy Novak	NICB

Table of Contents

Most Common Illicit Finance Activities

Most Exploited Elements of Financial Technology

Legal and Technological Vulnerabilities

Pseudo-Anonymity & Weaknesses in KYC Laws

NFTs and Other Blockchain Applications Risk of Illicit Use

Key Findings and Recommendations

Impact on Government and Private Sector

Future Regulations, Forecast, and Areas for Future Study

Analytic Deliverable Dissemination Plan

Endnotes Separated by Sections

Full Citations Separated by Sections

Appendices

Most Common Illicit Finance Activities

Illicit finance activity continues to grow in value and variation, especially with the use of digital assets and cryptocurrency. Some of the most common illicit activities in this digital space are money laundering, cybercrime, and consumer scams.

Money Laundering

Money laundering traditionally begins with ill-gained fiat currency that criminals wish to make usable. One strategy is to have money mules transfer these funds into bank accounts for later transfer/withdrawal. Cryptocurrency has opened new avenues for money launderers utilizing bank deposits by mules who then purchase cryptocurrency. Bitcoin ATMs are another popular method for money mules to convert fiat currency into cryptocurrency. Bitcoin ATMs are physical machines where people can buy cryptocurrency with cash, requiring varying amounts of personal information to use. Once the fiat currency is converted into cryptocurrency, there are multiple ways it can be laundered, making it difficult for law enforcement to track.

Cryptocurrency mixers, for example, aid in obfuscating the origins of the processed cryptocurrency. This happens by rapidly pooling currency streams into many small transactions across many wallets. Mixers allow illicit actors to launder high amounts very conveniently and are not inherently illegal. The co-founder of Tornado Cash, a popular cryptocurrency mixer, told Bloomberg in March 2022 that their service can be defined as an “anonymizing software provider” which does not subject them to money transmitter regulations in the U.S. Our group examined some of the most popular and common mixers/tumblers used today and our findings are reviewed in the chart below. [1](#)

DeFi, or Decentralized Finance platforms are another common way illicit actors launder their money through cryptocurrency. The defining characteristic of a DeFi service is its lack of a centralized intermediary for transactions or other services. Additionally, most of the DeFi platforms used by illicit actors are outside of the U.S. and are often not subject to or compliant with Know Your Customer (KYC) and Anti-Money Laundering (AML) laws. Some DeFi platforms also allow chain hopping, which allows users to exchange one cryptocurrency for another. Moving to a new blockchain through chain hopping aids in obfuscating transaction history.

Currency	Description
Blender.io	Allows users to determine how much they are willing to pay for service fee. Can access through VPN or TOR. Allows random delay for transactions and can send/receive coins after 3 blockchain confirmations.
Bitcoin Laundry	Does not charge customers a service fee but there is a commission fee for coins withdrawal to a specific address. Customers can choose up to 5 addresses for withdrawal of funds and allocate percentage of total amount to each. Can use time delay as well.
PrivCoin	Combines mixing and swapping services (changing the kind of cryptocurrency). Customers set size of commission fee for transactions.
SmartMix	Offers multiple mixing options including mixing with coins of other participants, with personal reserves of website, and cryptocurrency of investors. Users do not provide registration data and there is a small fee for coin cleaning.
Bitcoin Fog	Coins can be withdrawn to a maximum of 5 addresses. The journal of operations is erased within 7 days.

Case Study: Roman Stirlingov and Bitcoin Fog

In April 2021 Roman Stirlingov, the principal operator of cryptocurrency mixer Bitcoin Fog, was arrested by the FBI. Bitcoin Fog emerged as one of the first cryptocurrency mixers that especially helped illicit actors hide their illegal proceeds. This service particularly aided darknet market and Silk Road users to hide trafficking activity in drugs and other illegal payments. Over 1.2 million Bitcoin equating to approximately \$336 million at the time of transactions were reported to be sent over Bitcoin Fog. Stirlingov was discovered as the operator due to a mix of resources utilized by investigators including bitcoin transactions, financial records, internet service provider records, email records, and additional general records. This case emphasizes that with the right combination of resources, investigators can identify illicit actors utilizing Bitcoin as a cryptocurrency.^{1 2}

Cybercrime

The laundering techniques noted above are regularly used by hackers who have funds originating as cryptocurrency from cybercrime such as ransomware and hacking digital assets from persons or exchanges. The rapid growth of digital assets usage has created a landscape of insecure and often unregulated trading platforms and exchanges, leading to increased consumer risk. Cryptocurrency and blockchain platforms are now targets for hackers due to their large consolidation of assets. In March 2022 the North Korea associated hacking group

Lazarus stole \$620 million of Ethereum from the Ronin Network, a blockchain platform used by the Axie Infinity online game. In addition to these large scale attacks, some consumers' personal digital wallets have been compromised due to unencrypted private keys stored by exchanges, and through social engineering tactics.²

Today's ransomware model is built upon the use of cryptocurrency for payments. Ransomware payments in 2021 and 2022 each totaled over \$600 million according to Chainalysis' 2022 Crypto Crime Report. Most ransomware groups are located outside the U.S. which makes any traditional ransom payment using fiat currency difficult for the victims to pay and the ransomware groups to receive and launder. Global crypto exchanges and DeFi platforms help facilitate the illicit transfers and are typically out of reach to the U.S. and Mutual Legal Assistance Treaty (MLAT) countries. For more information on Ransomware attacks and their impact to critical infrastructure sectors, review the 2022 AEP whitepaper on "Ransomware Attacks on Critical Infrastructure Sectors".³

Consumer Scams

Consumer targeted cryptocurrency crime ranging from investment rug pulls and romance scams to social engineering and account takeovers continues to be the largest subset of illicit transactions. These scams reportedly cost consumers over \$7.7 billion in 2021 according to Chainalysis' 2022 Crypto Crime Report. Rug pulls are investment scams, usually associated with a new token, in which the developers of the project collect investments from consumers and then take the funds and abandon the project. This scam is often tied to romance scams in which victims are pressured or persuaded into an investment. The FBI's 2021 IC3 Report found over \$429 million in losses associated with romance scam victims who reported the use of investments and cryptocurrencies.^{3 4}

Case study - Zelle Digital Wallet Takeover

Bruce Barth was hospitalized in 2020 with COVID and his phone disappeared from his hospital room. Soon after his Zelle account was used to conduct three transfers totaling \$2,500. They additionally withdrew cash from an ATM and used his credit card with all accounts being at Bank of America. Although he was able to get refunds for his credit card and cash losses after filing a fraud report, Bank of America denied his claims for Zelle refunds. Even though Barth's phone was stolen, since the transactions were validated by authentication codes sent to a phone under the account, they claimed the Zelle transactions were authorized. After filing grievances through a variety of agencies, Barth eventually received refunds for the Zelle transactions after the New York Times contacted Zelle. This case exemplifies how difficult it is for customers to receive refunds on fraudulent Zelle transactions.³

Most Exploited Elements of Financial Technologies

Financial Technology (“FinTech”) is a term used to describe the use of software, mobile applications, and other technological tools to improve and automate the delivery of financial services to business entities and consumers to more efficiently manage their finances. In its infancy, FinTech involved primarily the implementation of technological advances and improvements to update and enhance existing functions and services provided to consumers and businesses without challenging the underlying business models. ¹

In the last decade, FinTech has shifted to become more revolutionary and disruptive to the underlying business models of many different industries including banking and capital markets. Instead of focusing on improvements, FinTech companies are redesigning the process of delivering financial services to customers using cutting edge technologies. FinTech has become so disruptive that it has created new business infrastructure, products, and services.

While Fintech has grown rapidly in the last decades and offers a lot of advantages such as ease, adaptability, faster service, substantial reduction in costs, expanded access to investment opportunities, it also presents a number of challenges and areas that are prone to exploitation. Data privacy, information security, consumer protection, cybersecurity, and financial protection are all areas that are subject to exploitation. First let’s examine the different types of Fintech services available to customers.

Different Types of FinTech

FinTech companies focus on employing technology to enable, enhance, and disrupt financial services. FinTech companies provide a wide range of services such as stock trading, robo-advising, crowdfunding platforms, blockchain technology and cryptocurrencies, as well as mobile payments and P2P services . The increased use of smartphones and ease of conducting transactions electronically, have been central to the adoption and growth of the multitude of FinTech products and services by everyday consumers.

DIFFERENT TYPES OF FINTECH

Type	Description
Stock Trading Solutions	Stock trading has shifted from consumers visiting physical exchanges to trading stocks through services on their smartphones and other devices. This has decreased costs and opened stock trading to a greater market.
Robo-Advising	Robo-advising takes the shift online further by setting up a smart algorithm to provide financial advice and investment management.
Crowdfunding Management	Startup companies and entrepreneurs are increasingly using crowdfunding networks to obtain funding from investors. This has shifted through app based and online based services that everyday individuals have used for projects with Kickstarter and GoFundMe being prime examples.
Blockchain and Cryptocurrencies	Blockchain technology is a decentralized, distributed ledger of all transactions across a peer to peer network. The data on the blockchain cannot be changed once recorded which makes it legitimate.
Mobile Payments/P2P Services	A mobile payment generally refers to payment service performed through a smartphone. The mobile payment service can be used to pay merchants and to send money to friends or family.

Stock Trading Solutions

One of the services offered by FinTech companies is stock trading. The traditional method that investors used to buy or sell stocks was to physically visit an exchange. Stock trading FinTech companies have revolutionized the industry by allowing investors to easily trade stocks using their smartphones or other portable devices. Furthermore, the low cost of these stock trading solutions have made them even more attractive to consumers. According to Bankrate, the top five Stock trading companies in 2022 are Charles Schwab, Fidelity Investments, TD Ameritrade, and Robinhood.²

Robo-Advising

Robo-advisors are digital platforms that provide automated, algorithm-driven financial planning services with little to no human supervision. A typical robo-advisor asks questions about your financial situation and future goals through an online survey; it then uses the data to offer advice and automatically invest for you. Robo Advisors have disrupted the wealth management industry by providing access to investment management at a fraction of the price a typical financial advisor might charge. As such, wealth management has now become accessible to consumers who could not afford it in the past. A Morningstar Inc. analysis of 16 robo-advisors rated the products offered by Vanguard Group and Betterment as the best

overall options to help investors achieve their financial goals. The two rose to the top of the list thanks to their “low cost, transparency, reasonable asset allocation approach and broad range of financial planning tools,” the report said.³

Crowdfunding Management

Fintech has enabled startups, self-employed entrepreneurs, and individuals or groups of individuals to obtain funding from investors through the use of crowdfunding. Crowdfunding networks allow users to receive or send money online or via mobile apps. While crowdfunding is often used by businesses to raise equity, the funds have also been used to fund other projects such as travel, funeral, wedding, medical expenses, and other bills. Kickstarter and GoFundMe have both successfully funded millions of pledges and raised funds.

Blockchain Technology and Cryptocurrencies

A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format, in blocks that are then linked together via cryptography. As new data comes in, it is entered into a fresh block. Once the block is filled with data, it is chained on the previous block, which makes the data chained together in chronological order. Different types of information can be stored on a blockchain, but the most common use so far has been as a ledger for transactions.

Blockchain technology is regarded as one of the biggest innovations of the 21st century as a result of its wide range of application to various sectors from financial to manufacturing, as well as education. Blockchain Technology was first introduced in 1991 by two researchers, Stuart Haber and W. Scott Stornetta who were working on a project that would implement a system where document timestamps could not be tampered with. In 1992, the system was upgraded to incorporate Merkel trees that enhanced efficiency which allowed the collection of more documents on a single block.

In 2009, Blockchain technology gained popularity and relevance by Satoshi Nakamoto, a pseudonymous person or team who outlined the technology in a whitepaper and conceptualized the development of bitcoin, the first application of digital currency. In the Whitepaper, Nakamoto proposed bitcoin as “A purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through another financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network

timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.”

Bitcoin is the first application and most popular type of digital or cryptocurrency built on blockchain technology. Cryptocurrency is decentralized meaning any two people, from anywhere in the world, can send cryptocurrency to each other without the use of a financial institution or government entity. Cryptocurrency transactions are tracked on the blockchain, a distributed ledger that allows the storage of all information in a secure and accurate manner using cryptography. Once the information is stored on the distributed ledger, it cannot be altered, deleted or destroyed.

In addition to monetary transactions such as cryptocurrency, blockchain technology is also used in other sectors and industries. Blockchain technology is used by healthcare providers to store their patients’ medical records. As a result, patients can have proof and confidence that their medical records cannot be changed. Blockchain technology is also utilized to facilitate, verify, and negotiate contract agreements using a computer code referred to as smart contract. Blockchain technology is also used to record and track supply chains as well as facilitate voting systems.

Mobile Payments/P2P Services

FinTech companies offer mobile payment services for both peer to peer and merchant payment transactions. A mobile payment generally refers to payment service performed through the use of a portable electronic device such as a tablet or cell phone. The mobile payment service can be used to pay merchants for goods and services, but to also send money to friends or family through mobile applications such as Paypal, Zelle, and CashApp.

POPULAR PEER TO PEER (P2P) SERVICES

Service	Description
Venmo	Allows users to send money to each other via a linked bank account, balance currently in service, or credit card. Owned by paypal but has some differences including a free, debit card that allows users to expend money directly from their Venmo balance.
CashApp	Created by Block Inc. (formerly Square) that allows users to send money via their Cash App balance, linked bank account, or credit/debit card. Offers users an optional debit card with exclusive discounts known as "cash boosts". Users can also invest in stocks and buy/sell bitcoin.
Paypal	One of the more longterm established platforms that has helped users perform personal money transfers, online purchases, and e-commerce. User can search for other users using name, email, or phone number to send or request money. Has high transfers limits and multiple methods of payments for transfers.
Zelle	Offered through most major banks in the U.S. and allows users to send money to other Zelle users either through their bank account or in the Zelle app. Users can send/request money from someone else by entering their email or phone number. Transfers happen quickly, within a matter of minutes and it is favorable due to being compatible with many financial institutions.
Apple Pay	Allows users to send and receive money in the Messages App. Users link a debit card in the Apple Wallet app and are able to send, request, and accept money from other users. Retailers are increasingly accepting Apple Pay at checkout.

Exploited Elements of FinTech

Data Privacy and Security

Data privacy and information security are the top concerns for consumers of Fintech. The increase of online and phone banking services have provided fintech companies access to tremendous amounts of data about customers and visitors, which can be exploited and analyzed to generate insights about consumer behavior, interests, networks, and personalities, but also makes the data more susceptible to security breaches. According to PwC's Global FinTech Survey 2016, almost 56% of the respondents identified information security and privacy as threats to the rise of fintech.⁴ As more services go online, data privacy and security, are proving to be a major challenge for fintech as consumers are becoming more concerned with how their data are being exploited by enterprises for business and marketing decisions and the security of their data in terms of who ultimately have access to such datam legally or illegally.

Case Study: Equifax Data Breach

In September of 2017, Equifax announced a data breach that exposed the personal information of approximately 150 million people. The company agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement amount was approximately \$425 million to help people affected by the data breach. In February 202, the U.S. government indicted four members of China's military on charges of hacking Equifax to exploit the personal data of 150 million Americans. They allegedly conspired to hack into Equifax's computer networks, maintain unauthorized access to those computers, and steal sensitive, personally identifiable information of nearly half of all American citizens.⁵

Fraud and Money Laundering

While many customers are choosing Fintech banking over traditional banking for the ease of use, competitive prices and better quality of service, others are making the choice because a fintech bank account provides easy access to a bank account and payment card in a matter of minutes with minimal KYC requirements. In fact, the emergence of Fintech banking has allowed individuals to open up multiple bank accounts without proof of residence or salaries providing them greater access to launder illicit funds in countries where KYC regulations are minimal or nonexistent. As a result, Fintech firms have inadvertently facilitated financial crimes by illicit actors and money launderers.

Case Study: Wirecard Money Laundering Scandals

Since June 2020, in Germany, a serious financial scandal involving the online payment company Wirecard is underway, after the discovery of a shortfall of 1.9 billion euros which was thought to be deposited as trust funds in two banks in the Philippines but which never existed. The former Wirecard's CEO has been arrested in Germany on suspicion of fraud, while his former CEO has disappeared after fleeing the country. In addition to this fraud, according to the Financial Times, Wirecard processed payments for a Maltese online casino which was later accused of laundering money for a powerful member of the 'Ndrangheta, one of Europe's most dangerous mafia organizations. Wirecard processed payments for CenturionBet, a Malta-based gaming company that was later found by Italian courts to be an 'Ndrangheta way for moving money out of the country in a sophisticated money laundering operation. Wirecard continued to trade with CenturionBet, which was incorporated in Malta but owned by a Panamanian company, until 2017 when its gambling license was suspended by the Maltese authorities and

ceased trading after an anti-mafia raid that saw the arrest of 68 people. Since then over 30 people have been convicted of mafia related crimes. CenturionBet's revenues included only a fraction of Wirecard's global operations, but the discovery raises further questions about the German company's business model, once deemed to be a pioneer of European fintech. As a regulated payment institution, Wirecard is required to abide by the strict anti-money laundering rules and report suspicious transactions to the competent authorities. Wirecard also processed payments for another larger Maltese gambling company that has been investigated by the Italian authorities for money laundering for organized crime groups. It is possible that Wirecard was unaware of the company's alleged ties to organized crime.⁶

Case Study: Coin Ninja Money Laundering

In February 2020, the U.S. federal government arrested Larry Harmon, CEO of the Coin Ninja media platform and founder of the DropBit cryptocurrency wallet. In particular, Harman was accused of conducting money laundering activities and running a business for the exchange of funds without a specific license from FinCEN. According to the arrest warrant filed in early February 2020, Harmon would have laundered over 354,468 Bitcoin (BTC), equivalent to approximately \$311 million at the time of the transaction, allowing users of Helix and Grams, respectively, a privacy and privacy tool, a dark web search engine, to transact on AlphaBay, a very popular dark market but closed in 2017. In 2021, Harmon pleaded guilty today to a money laundering conspiracy arising from his operation of Helix.

As part of his plea, Harmon also agreed to the forfeiture of more than 4,400 bitcoin, valued at more than \$200 million at the time of his plea deal, and other seized properties that were involved in the money laundering conspiracy. Harmon is expected to be sentenced at later date and faces a maximum penalty of 20 years in prison, a fine of \$500,000 or twice the value of the property involved in the transaction, a term of supervised release of not more than three years, and mandatory restitution.⁷

Hacking and Ransomware

Also, Fintech companies are susceptible to cybercrime such as hacking and ransomware which have become a growing problem for both the private and government sector lately. During ransomware attacks, criminals deploy malicious software that encrypts a victims' files and renders its systems unusable and the data unusable. The attackers then issue a ransom demand, oftentimes in cryptocurrency to allow remote and anonymous payment that cannot be easily traceable to them. The attackers then promise that if they receive the ransom, they will provide the victims with a key to decrypt their systems and data but that is not often guaranteed.

Ransomware has become a major problem as a result of the emergence and acceptance of cryptocurrencies. Ransomware has also become a national security threat of the United States and various other countries around the world. Private companies including Fintech are also subject to becoming victims of hacking and ransomware attacks to steal customers' data and money, and cripple their systems.

Case Study: Binance Ransomware

On August 6, Malta-based cryptocurrency exchange Binance became the victim of ransomware when attackers demanded 300 bitcoin, the equivalent of approximately \$3.5 million at the time in exchange for a Know Your Customer (KYC) database containing the personal information of around 10,000 users. The KYC database allegedly contained personal identification information and photographs of users with documents like passports. The company contested the authenticity of the documents, claiming that they lacked digital watermarks, refused to pay the ransom, and contacted law enforcement for assistance in pursuing the attackers.⁸

Legal & Technological Vulnerabilities

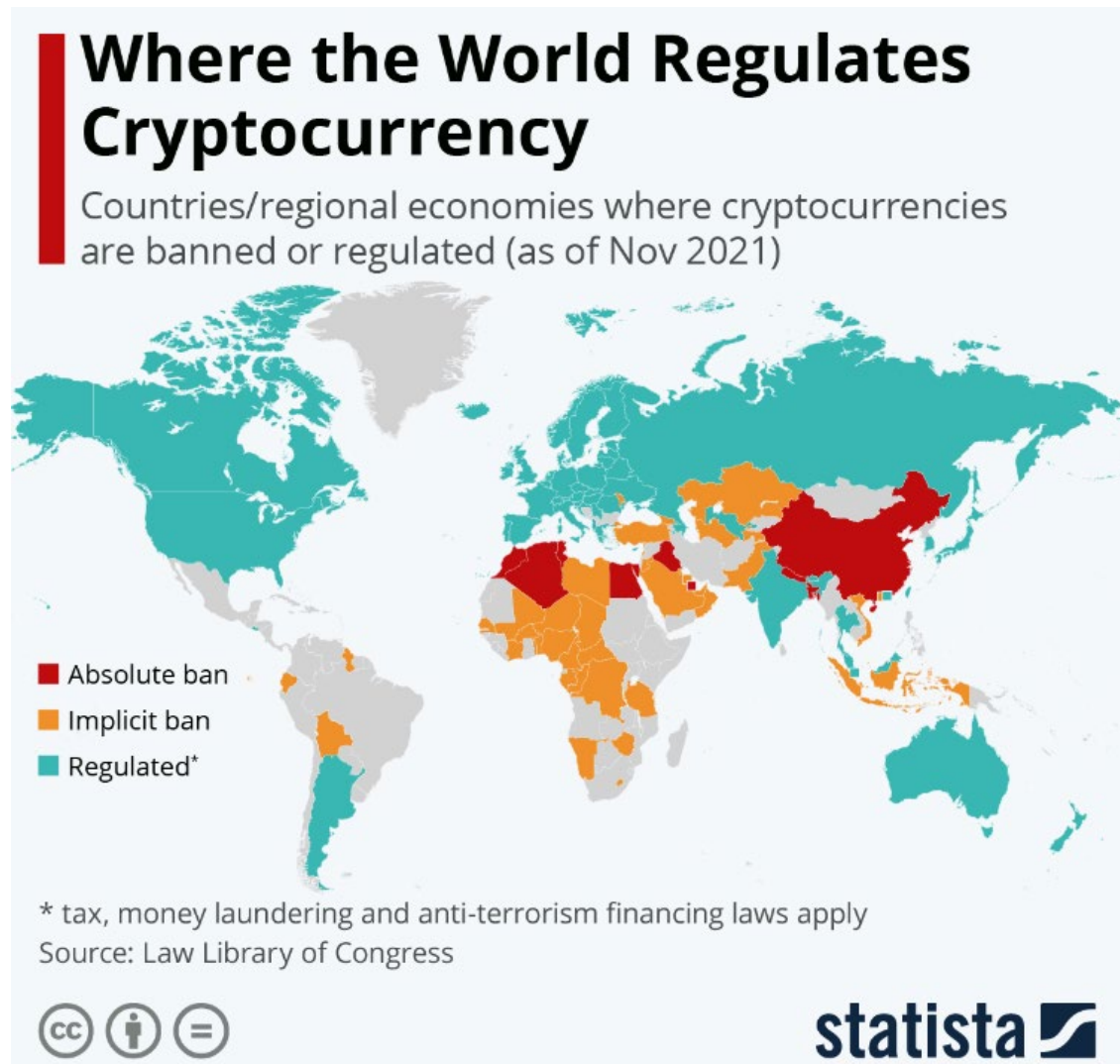
The name cryptocurrency is somewhat of a misnomer. For all intents and purposes, it is not truly a currency, has no inherent value beyond what its investors are willing to pay, and has no government or central agency to back up its value or insure deposits. Eventually, the US government will have to make a determination of how to classify cryptocurrency to establish regulations and enforcement jurisdiction. The Security and Exchange Commission (SEC) considers it a security, the US Commodity Futures Trading Commission (CFTC) considers it a commodity, and the Comptroller's Office of the Currency considers it a currency.^[i] Depending on how cryptocurrency is eventually categorized, this will determine which agency has jurisdiction over this technology, how to regulate it, how to tax it, and how to enforce regulations. Currently, the Department of Justice (Justice) has taken on most of the public responsibility for recovering stolen assets in terms of cryptocurrency while other actors involved in these investigations have been the SEC, the Department of Homeland Security, Cyber Command, the National Security Agency, and the Internal Revenue Service. The main issues that the USG and global law enforcement agencies face are jurisdiction and regulations and reporting requirements. The US Treasury has jurisdiction over any transaction that involves the US dollar because the US government has given the Treasury that power through the Office of the Comptroller of the Currency (Office of the Comptroller).¹ However, cryptocurrencies, because they are decentralized and have no overarching jurisdictional power or issuer with the exception of the miner or the developer, have no such overreaching authority. The

transnational nature of the blockchain and a lack of residency confuse any jurisdictional arguments. However, the SEC has been making steps in the direction of considering cryptocurrencies securities, such as in the case of Ripple (XRP). In December 2020, the SEC brought a lawsuit against XRP stating that the Initial Coin Offering (ICO) was an “unregistered securities offering” raising \$1.3billion through sales. By considering XRP as a security rather than, as Ripple’s issuers argued, a currency, the SEC claimed jurisdiction over the token rather than the Office of the Comptroller under Treasury.² The SEC considers cryptocurrencies as securities and applies securities law to digital wallets and exchanges, while the CFTC considers Bitcoin, specifically, a commodity and allows cryptocurrency derivatives to trade publicly.

In the United States, cryptocurrency exchanges and trading is legal, though inadequately monitored or regulated. Cryptocurrency exchanges fall under the regulatory aegis of the Bank Secrecy Act (BSA) and must register with the Financial Crimes Enforcement Network (FinCEN). Under the BSA, they are considered money service businesses and must implement an Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) regime, maintain records, and submit reports to the proper authorities. However, the US Treasury has no jurisdiction over exchanges that are not registered in the US or those that choose not to comply with AML/CFT practices. The Internal Revenue Service (IRS) wants increased ability to request cryptocurrency transactions at exchanges and brokers, presumably for tax purposes, while FinCEN has proposed reporting requirements for accounts that exchange over \$10,000 per day and KYC requirements on international transactions similar to banking institutions and money service businesses (MSB). Money service businesses like EBay and PayPal come under the jurisdiction of the Treasury because of the type of transactions they enable in the US dollar. One of the main issues authorities face with regulation is how to get exchanges to agree to standardization, anti-money laundering (AML) practices, and oversight. In the United States, several state governments have proposed or passed laws affecting cryptocurrency and blockchain technology, lacking any overarching legislation on the federal level. While there is no uniform definition of cryptocurrency, virtual currency, digital assets, cryptoassets, or crypto, states have largely approached legislation toward a broad definition to encompass the entire asset class.³

Legal regulations worldwide vary and are largely inconsistent between jurisdictions. In the United States, the White House released an Executive Order committing to taking part in research on cryptocurrencies in a “whole-of-government approach to addressing the risks and harnessing the potential benefits of digital assets and their underlying technology.”⁴ On the international level, the Financial Action Task Force (FATF) has made progress releasing guidance on Virtual Asset Service Providers (VASPs). The FATF stated that VASPs are subject to the same relevant standards that cover more traditional financial entities and that countries should

assess and mitigate risks associated with virtual asset financial activities and providers, to include licensing, registering, and monitoring.⁵ In response to FATF guidance, FinCEN clarified that it expected cryptocurrency exchanges to comply with the Travel Rule, proposing that exchanges must collect, retain, and transmit certain information related to funds transfers and transmittals of funds over \$250 for international transactions and \$3000 for domestic transactions. It further stated that these rules apply to convertible virtual currencies, to include any transactions involving digital assets with legal tender status.⁶



Technological Vulnerabilities

Blockchain technology has been advertised as sound but under certain conditions, has specific vulnerabilities mostly due to human error, the economics of the blockchain, or the code. A majority of the weaknesses of blockchain technology comes in the forms of mistakes in account security, fraud, scams, hacking, ransomware, and a lack of resources for adequate security protections. Account Security is a vulnerability for both the individual user and cryptocurrency exchanges and platforms. The most common weaknesses for exchanges and platforms include phishing, missing wallet protections, weak login credential protections in addition to software vulnerabilities and transaction manipulations. For individual users, the most common weaknesses include phishing, poor wallet security, fraud, and scams.

Wallets/Accounts: Inadequate protection of account passwords to include two factor identification, private keys, and seed phrases are one of the most common vulnerabilities to account security. These represent the most common way an individual's account or systems' platform is accessed by an unauthorized entity.

Fraud/Scams: A variety of scams or frauds to induce users to invest money or allow access to their cryptocurrencies have proliferated in recent years. These can run anywhere from 'pump and dump,' fraudulent websites or coins, rug pulls, romance schemes, giveaways, ponzi schemes, or celebrity endorsements.

Social Engineering/Phishing: Social engineering to obtain access to account passwords, keys, seed phrases, or other sensitive data involves inducing victims to download malware onto their computers or networks, allowing outside access. The five types of social engineering methods are phishing, pretexting, baiting, quid pro quo attacks, and tailgating.

Inadequate Resources/Security:

Cross-Blockchain Interoperable Bridge: The bridge that enables users to transfer digital assets from one blockchain to another has recently been the target of several attacks to exploit these technical weaknesses. The Poly Network attack in 2021 resulted in theft of approximately \$610 million in digital assets, locking up nearly \$1 billion across the entire network. The recent attack on the Ronin Network, with a reported loss of over \$625 million in assets attacked the Ethereum-linked bridge the network used to execute transactions for the game, Axie Infinity, to transfer assets in and out of the Ronin network for use in the game. The attackers managed to get control of four of the nine validator signatures needed to access the system held by the parent company, and backdoor access to a centralized server to obtain the final required signature to validate transactions.

51% vulnerability attacks: Blockchains that use proof-of-work as their protocol for verifying transactions are susceptible to manipulation if an individual or pool of miners is able to gain control of a majority of a network’s mining. The miners or pool of miners could potentially change blockchain information by reversing a transaction, allowing double-spending by creating a fork in the blockchain. These types of attacks usually occur on smaller coins where gaining control of the majority of a network is much easier than on larger blockchains such as Bitcoin.

Routing Attacks: Blockchains rely on large real-time data transfers to communicate and execute transactions, which are vulnerable to hacking. Hackers are able to hijack IP prefixes to intercept data transfers, reroute traffic to hacker-controlled destinations, or drop connections to prevent consensus and confirmation of transactions.

[i] SoFi. 27 April 2021. SoFi.Com. “Is Crypto a Commodity or Security.” Accessed 9 February 2022. <https://www.sofi.com/blog/crypto-commodity-vs-security/>

VULNERABILITIES IN DIGITAL ASSETS	
Vulnerabilities	Description
Insider Threats	Most digital asset companies are increasingly employing a zero trust strategy where access rights of all employees are managed and restricted to avoid a large scale attack. This prevents bribing current employees for credentials/access since they lack it themselves and prevents large scale damage in the case their credentials are stolen/discovered.
Site Forgery and Phishing	Illicit actors can create a website that mirrors legitimate websites where users store and trade digital assets. Through these false websites, they can gain access to a user’s credentials and digital assets. This is also a concern if employees of exchanges and digital asset marketplaces fall victim, allowing criminals access to increased information.
Watering Hole Attack	Through this attack illicit actors can gain access to internal/restricted pages of digital asset exchanges and marketplaces. It injects malicious code through a zero day attack into a website an organization and/or particular employee of that organization often uses. This will result in user’s computers being infected with malware allowing actors to gain access to an organization’s internal network.
Lack of Resources	Many companies simply don’t employ robust cybersecurity resources due to budget constraints and the lack of concern that a large scale attack can affect them. It is also a challenge to constantly update systems in both small and large scale organization to prevent attacks. Digital asset exchanges and marketplaces should prioritize cybersecurity in their business model.
Inadequate Security Training/Human Error	It is not uncommon for employees of organization to be lacking in cybersecurity training along with users. Users may not employ 2 factor authentication, strong passwords, VPN, etc. that can help protect their digital assets and online stored locations. Employees conducting a large amount of digital asset trades per day may fall victim to a human error such as typing a deposit address wrong or trading the wrong cryptocurrency.

Pseudo-Anonymity and Weaknesses in KYC

Pseudo-anonymity is a key factor in propelling the use of cryptocurrencies and other emerging digital assets for illicit purposes. Bitcoin is the original catalyst for this element due to its pseudo-anonymous nature. A person's identity is tied to a fake name or pseudonym in using bitcoin which serves as their public key and bitcoin address. Bitcoin has never been truly anonymous because all transactions are available on the public network leaving anyone easily being able to see records of all transactions a bitcoin address has conducted. It is up to the bitcoin address holder to prevent their actual identity from being linked to their pseudonym in bitcoin. As other cryptocurrencies have emerged the same principles have applied in that they provide pseudo-anonymity and a means for people to make transactions that aren't under their true identity. As we're entering a new phase of digital assets, they are taking it a step further by providing complete anonymity or near complete anonymity which is discussed with Monero and NFTs in a later section. However it has largely been a misconception that cryptocurrencies are completely anonymous and even with their pseudo-anonymous nature, illicit actors have not been able to hide from authorities.

Case Study - FBI \$3.6 Billion Bitfinex Seizure

A recent seizure from the FBI that demonstrates the pseudo-anonymous nature of Bitcoin and how it can ultimately be traced back to a person is the \$3.6 billion bitfinex seizure. Married couple Ilya Lichtenstein and Heather Morgan were charged with conspiracy to commit money laundering and conspiracy to defraud the U.S. They were charged after years of investigating by the FBI as to the source of a 119,754 Bitcoin theft from the cryptocurrency exchange Bitfinex where the proceeds were placed into a single crypto wallet. The money remained in that wallet largely untouched for years; however once the currency started to move out of that wallet and into traditional bank accounts, the transactions were able to be traced to Lichtenstein and Morgan. Although the couple was careful to evade authorities for a long time, they were ultimately caught due to the public nature of the blockchain and any errors in hiding their identities being a permanent feature on the blockchain. The couple did utilize a few different dark web currency exchanges including Hydra and Alphabay that allowed them to still conceal their identities while moving funds. However these services has since been shut down by law enforcement and in this case Alphabay's internal logs allowed law enforcement to link the wallet in the Bitfinex hack to the laundered accounts. Ultimately once law enforcement was granted access to Lichtenstein's cloud storage account, they found a list of wallet addresses linked to the hack and were able to seize the funds. This case exemplifies how most cryptocurrencies aren't truly anonymous and the difficulty in concealing a large amount of illicit funds generated in illicit activity. Criminals will likely use these illegal exchanges

and make large scale purchases through traditional accounts allowing them to be discovered by law enforcement. ⁴

Case Study - Miami Feds \$34 Million Crypto Seizure

Another recent bitcoin seizure which demonstrates the pseudo-anonymous nature of the currency but ultimately how it can be tied to someone's true identity is the joint federal seizure between the FBI, IRS, and HSI of \$34 million from a Miami resident. The unnamed Miami resident is accused of using numerous anonymous identities on the dark web to carry out fraudulent online transactions between 2015 and 2017. The accused person is suspected of selling people's account information that had been hacked from popular services such as HBO, Netflix, and Uber. Authorities did not have enough evidence to pursue a criminal case so they pursued a civil case to seize his cryptocurrency. The suspect additionally used tumblers to conceal the movement of his funds. This seizure and civil case illustrates that bitcoin and other cryptocurrencies do not provide a complete anonymous nature. ⁵

Group Research Task: Privacy Coins & How They Maintain Anonymity

Pseudo-anonymity is becoming harder to maintain due to the emergence of privacy coins. There are a variety of privacy coins available to consumers to maintain complete anonymity in online transactions. Our group looked into some of the most popular privacy coins that are expected to continue to grow and that open the door for further illicit activity by criminals.

PRIVACY COINS

Currency	Description
Monero	One of the top coins chosen to remain anonymous. Difficult to trace due to use of ring signatures and stealth addresses. Ring Confidential Transactions help conceal the transaction amount.
DASH	Allows users to choose whether their transactions are anonymous or not using PrivateSend feature. This employs a mixing protocol using master nodes.
Zcash	Allows users to shield transactions and employs a cryptographic tool called Zero-Knowledge Proof. Hides transaction amount and addresses don't have to be revealed.
Verge	Relies on TOR and I2P to protect users' identities. Locations and IP addresses of users remain hidden.
Horizen	Offers privacy shielded Z-address and public T-addresses that work similarly to Bitcoin. Has a vast node network which helps maintain anonymity.

Know Your Customer requirements are another important aspect to consider in cryptocurrency exchanges and digital asset marketplaces that ties directly with the element of pseudo-anonymity. Although KYC requirements are strongly guarded in the financial institution industry, when it comes to the emerging digital asset realm there are vast differences among marketplaces. Some contain the same KYC requirements as traditional financial institutions including proof of identity with a photograph and proof of address while some just require an email address upon registration and nothing more. The lack of KYC requirements in cryptocurrency exchanges and digital asset marketplaces has attracted more illicit actors over traditional financial institutions. Although the US Treasury is declaring all US crypto exchanges must register with FinCEN as a Money Service Business, not all have registered yet. This also only applies to US based exchanges which is only a fraction of the exchanges that exist worldwide. This will continue to be an obstacle for directly tying someone as an owner of an account or wallet if the exchange is based in another country and does not require any KYC upon account registration. It is also important to keep in mind that even though crypto exchanges are becoming more regulated and more attention is being focused on them, other digital assets like NFTs remain largely unregulated. FinCen has only released some guidance that NFTs may be subject to FinCen regulations however there are no concrete regulations yet. This will likely change as they become more commonly used but it will still be an uphill battle in attaching regulations to the assets and ensuring that customers are submitting the right

identification when purchasing these assets. CipherTrace released a report that 1/3 of the top 120 exchanges have weak KYC requirements.⁶

There are multiple obstacles towards implementing KYC requirements in crypto exchanges and online marketplaces. Firstly, they add increased expenses to these emerging institutions. It is costly to add increased verification processes, registering with regulatory bodies, and adding large compliance teams to adhere towards more KYC policies. Secondly, customers would prefer to use exchanges and marketplaces they can quickly register on rather than waiting a week or longer for their verification process to be complete. This makes it more enticing for exchanges to not have a comprehensive verification process so they don't lose out on customers who want to register quickly. Another factor are the security implications that come with storing personal information of users. Over the last decade we've seen numerous large scale data breaches where customer PII has been leaked. It is common for exchanges to use third party verifiers and there is precedent for these verifiers being leaked, PII being compromised, and hackers demanding ransom for the "safe" return of the PII. The more KYC collected, the more responsibility is placed on exchanges and marketplaces. Overall given current regulations and the promise of more regulations in the future, marketplaces will likely struggle to properly meet KYC demands. Current and emerging digital asset marketplaces in the US should all at least have the baseline KYC of photo identification and proof of address to prevent illicit activity.⁷

Improper KYC directly ties in with pseudo-anonymity because anonymous user accounts are more likely to be used for money laundering and terrorist financing. It also increases the risk of identity theft crimes and false identities being used as owners of digital assets. One of our group's original research tasks included registering under different exchanges and seeing what kind of KYC factors they implemented. This allowed us to compare and contrast how exchanges were adhering to KYC protocols and which ones consumers should feel comfortable using.

Group Research Task: Registering Under Different Cryptocurrency Exchanges

Coinbase - Types of verification required include phone number, photo I.D., SSN, and other personal details. Founded and based in the U.S., Coinbase is one of the longest standing exchanges so it has well adapted to regulations over time. Contains different account limits based on types of verifications tied to accounts.

Kraken - Verification required includes email address, full name, DOB, physical address, employment info, and SSN. Similarly to Coinbase, this exchange was also founded and based in the U.S. Contains different account tiers with different verification requirements.

Binance- Basic verification required includes name, address, and DOB with other tiers requiring picture ID and proof of address. Regarded as the largest exchange by trading volume and has its headquarters in the Cayman Islands. Originally it was based in China however due to China’s increased regulation of cryptocurrency, it moved its headquarters to a less regulated location. This exchange provides a great demonstration as to how increased regulations in the U.S. may drive exchanges outside of the country and into locations with less regulations.

FTX- International exchange that has 3 levels of restrictions. Tier 1 does not require legal documents but users must provide email, full name, DOB, phone jurisdiction ,country of residence, and optional SSN. Tier 2 requires government ID, proof of address, description of source assets, and facial verification which gives access to unlimited withdrawals. Specifically in the US FTX unverified users can only explore the site, Tier 1 users are subject to \$10,000 per day, and Tier 2 users have full access

Kucoin- This exchange just required email and no other identifiers at sign up. However users can partake in full ID verification through presenting a valid ID which will allow them to increase withdrawal limits. This exchange is headquartered in the Seychelles (an island up north from Madagascar) which, similar to Binance, gives them more freedom when it comes to following exchange related regulations and compliance.

CRYPTO EXCHANGE COMPARISON

Exchange	Headquarters/ Founded	KYC	AML
Coinbase	San Francisco, USA June 2012	Yes	Yes
Kraken	San Francisco, USA July 2011	Yes	Yes
Binance	San Francisco, USA Sept. 2013	Yes	Yes
Remitano	St Vincent and the Grenadines 2016	Yes	Yes
KuCoin	Hong Kong 2017	Yes	Yes
FTX	The Bahamas May 2019	Yes	Yes

A key thing in common with the exchanges we investigated were that exchanges vary on requirements depending on the location of the customer. US based users are subject to some of the heaviest KYC requirements when comparing other requirements worldwide. Exchanges have adapted to fit US requirements while still maintaining less restrictions in other locations. Other exchanges we looked into included LocalBitcoins and Local Monero which are unique in that they provide direct transactions between parties, essentially cutting out the “middle man”. These local services provide another unique avenue for illicit actors to engage in money laundering and other criminal activity without leaving a trail to trace back to them. As KYC factors become more enforced by US based exchanges, illicit actors will continue to use other means bypassing typical exchanges to avoid being identified.⁸

NFTs and Other Blockchain Applications Risk of Illicit Use

Other, emerging blockchain applications such as NFTs and digital payment services such as gaming currency and P2P services present a great risk of illicit use. While these forms are just starting to emerge in criminal cases, they have the potential for large-scale mis-use by illicit actors. The first U.S. federal criminal case involving NFTs occurred in March 2022 and provides a great case study into how this class of digital assets can be misused.

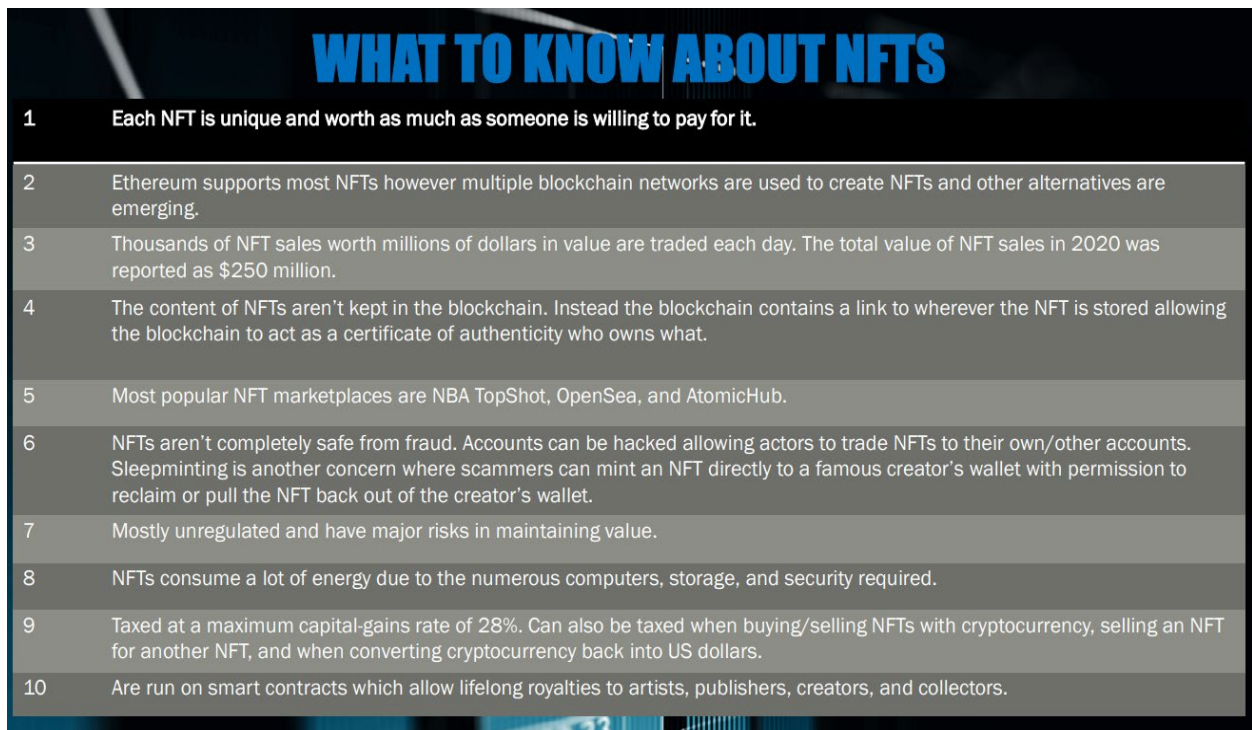
Case Study - NFT “Rug Pull Scheme”

Ethan Vinh Nguyen and Andre Marcus Quiddaeon were both arrested in Los Angeles in March 2022 after they were charged with conning buyers of NFTs worth 1.1 million. They were charged with both wire fraud and conspiracy to commit money laundering after issuing a set of NFTs known as “Frosties”. The purchasers of “Frosties” were supposed to be eligible for exclusive hodler rewards including early access to a meta verse game and giveaways. These types of NFTs which offer special bonuses are specifically known as utility NFTs. Nguyen and Quiddaeon subsequently ditched the project after selling out just hours after launching and transferred the money earned from the sales of the NFTs to multiple cryptocurrency wallets under their control. They started their project under pseudonyms which further demonstrates the pseudo-anonymity involved in online blockchain applications. Criminals can hide behind online identities while promoting their NFTs and ultimately perform a “rug pull” leaving any investors defrauded.⁹

Another interesting case study that exemplifies the volatility of NFT rates and exactly what they could go for is the sale of an NFT of the first tweet from Jack Dorsey, who is a co-founder and former CEO of twitter.

Case Study - NFT Sale of Jack Dorsey’s First Tweet

NFTs have the value of whatever the public is willing to pay for them which makes them a volatile investment and an investment anyone should be cautious about. A prime example of this is how crypto entrepreneur Sina Estavi bought the first tweet by Twitter founder Jack Dorsey as an NFT for \$2.9 million in March 2021. At face value that is already an enormous amount for an NFT let alone an NFT of just a tweet. In March 2022 Estavi announced that he would list the NFT for sale by auction and donate fifty percent of the proceeds to charity. Like any investment, Estavi assumed the NFT appreciated in some value over the year. He expected the NFT to at least net \$25 million especially with the explosion of interest in NFTs. However once the auction ended for the NFT the highest bid was only 0.09ETH which equates to approximately \$277 market rate at that time. Estavi told CoinDesk afterwards he may never sell it but if he does eventually get a good offer, he may accept it. This serves as a cautionary tale for all members of the general public interested in buying an NFT to take into consideration the long term appreciation of the piece. This is still fairly new territory and although artwork has shown a history of appreciating in value, it too has its volatile investment risks and NFTs can’t be directly correlated to physical art. The amount of NFTs that can be produced is almost limitless so it is likely we will see trends in the coming years of popular ones, such as the Bored Ape Yacht Club, peaking to a high price and then decline. ¹⁰



WHAT TO KNOW ABOUT NFTS

- 1 Each NFT is unique and worth as much as someone is willing to pay for it.
- 2 Ethereum supports most NFTs however multiple blockchain networks are used to create NFTs and other alternatives are emerging.
- 3 Thousands of NFT sales worth millions of dollars in value are traded each day. The total value of NFT sales in 2020 was reported as \$250 million.
- 4 The content of NFTs aren’t kept in the blockchain. Instead the blockchain contains a link to wherever the NFT is stored allowing the blockchain to act as a certificate of authenticity who owns what.
- 5 Most popular NFT marketplaces are NBA TopShot, OpenSea, and AtomicHub.
- 6 NFTs aren’t completely safe from fraud. Accounts can be hacked allowing actors to trade NFTs to their own/other accounts. Sleepminting is another concern where scammers can mint an NFT directly to a famous creator’s wallet with permission to reclaim or pull the NFT back out of the creator’s wallet.
- 7 Mostly unregulated and have major risks in maintaining value.
- 8 NFTs consume a lot of energy due to the numerous computers, storage, and security required.
- 9 Taxed at a maximum capital-gains rate of 28%. Can also be taxed when buying/selling NFTs with cryptocurrency, selling an NFT for another NFT, and when converting cryptocurrency back into US dollars.
- 10 Are run on smart contracts which allow lifelong royalties to artists, publishers, creators, and collectors.

Apart from trying to avoid any blatant NFT scams done by creators, hackers are increasingly becoming skilled at exploiting vulnerabilities in these platforms. This is exemplified by someone posting an NFT to OpenSea that contained malicious code. Users who clicked on the NFT and accepted a gift from the hackers who had designed it would immediately have their user balance cleaned out. OpenSea investigated this claim and did not find any victims and claimed victims would have to provide a digital signature before someone would have access to their funds. Although OpenSea updated its security warning and this vulnerability was “patched”, crypto users soon reported on a similar scam. Hackers were able to discover another vulnerability after this one was fixed. Consumers have to be careful with what NFTs they purchase. They can easily be conned into purchasing a worthless NFT.¹¹

NFTs are currently not addressed by FinCEN due to their fairly new emergence on the market. This follows the general art trend where art work has largely been unregulated and has opened the door to a wide range of illicit activity, in particular money laundering. Although sites like OpenSea can be registered as money service businesses and large sales can generate SARs in the future, not all sites permitting the purchase of NFTs will likely ever be covered. FinCen has only published guidance on how BSA and general regulations that apply to virtual currency apply to NFTs. (citation) The “underground” art dealing community will always exist in both physical and digital forms. ¹²

Another type of digital currency that has the potential for misuse is gaming currency. One of the most popular games on the market today, Fortnite, has been discovered to be used for money laundering in some capacity. Fortnite uses a currency known as V-bucks which serves as in-game currency for players. A joint report issued by the Independent and Sixgill, a cybersecurity firm, discovered Fortnite money laundering operations on a worldwide scale. Criminals were using stolen cards to purchase V-bucks and would sell them discounted on the dark web and auction websites such as Ebay. Sixgill discovered in 2018 there was more than \$250,000 raked in by Fortnite items on Ebay over a 60 day period alone. Epic Games has been criticized for not doing enough to crack down on suspicious transactions within the game. This raises the question and discussion of what risk indicators should gaming companies have in place to monitor transfers of high value goods and players with a large amount of in game currency. ¹³

Case Study - Squid Tokens and Smart Contracts

After the success of Netflix’s Squid Games, one scam arose as a play to earn game modeled after the show. Squid tokens were sold by project leaders and rose nearly 23 million percent in less than a week. However these tokens were governed by a smart contract which

every NFT is governed by. These smart contracts contain code which developers use to build mini applets in. This code opens the door and potential for scams and malware. The smart contract for Squid tokens forbade the sale of Squid tokens without burning a number of Marbles tokens, which players earn in the game. This project was short-lived and fell apart after a week, before the game launched, with the creators disappearing with the money and the Squid tokens becoming worthless. Squid tokens remain to be unsold even as a novelty since Marble tokens can't be earned. These tokens will most likely remain in wallets of purchasers forever. This case demonstrates the uncertainty and investment risks that come with purchasing game related currency. These currencies will not always maintain their value and the games could one day disappear leaving any in game currency worthless. [14](#)

Case Study - Second Life and Linden Dollars

Second Life provides what can be arguably one of the first examples of widely used gaming currency and how it can be potentially used illicitly. I was first launched in 2003 and had around 1 million users at its peak with approximately 800,000 active users in 2017. This game contained and largely revolved around the 'Linden dollar' which served as an in-game currency to buy items, land, and even use at in-game casinos. Approximately \$65 million was paid out to Second Life users in 2018 for a variety of goods and services. This high amount of users and money involved in the game obviously leads to the opportunity for illicit use to occur. A former employee Pearlman spoke up about the issues plaguing the game and company claiming compliance with anti-money laundering rules were not being properly followed. No KYC information was being collected on any operators of the game while she was employed. Second Life later added anti money laundering regulations but for well over a decade it allowed users to remain pseudo-anonymous and move around money freely. Another concern of gaming currencies that pertain to general consumers is the possibility for their in game currency to be stolen and hacked. In 2007 the virtual banks of Second Life experienced multiple bank heists which gave hackers a reported \$3.2million in Linden Dollars. Although there have been advancements in cybersecurity science then and games are generally more protected, there is always the chance a vulnerability can be found and exploited by hackers. This is another concern the general public should have when investing in virtual game currency. The game might not always have the strongest security in place to prevent funds from being stolen and unable to be recovered. [15](#)

In addition to gaming currency, there is currently the development and implementation of metaverses where people can live a virtual existence and by way conduct digital transactions. This opens the door to a wide range of fraud and illicit activity purposes. Since this is such a new space, there is not a current case study to analyze illicit activity that can potentially be

conducted. However this should be a concern for those developing these mataverses and they should keep in mind the security implications when developing currency. Another rising concern with NFTs and other emerging blockchain technologies is the idea to use them for records including home ownership, medical, and general social media. Wallets in these areas could open the door for personal data to be leaked and even deleted from the blockchain by criminals.

P2P platforms such as Zelle and Square that provide digital payments solutions directly between customers also host the opportunity for an increase in illicit use. These platforms provide fast transactions directly between parties and the immediacy of transactions opposed to a day or more wait at banks is very enticing to illicit actors. Although many banks employ Zelle as a transaction solution, banks say returning money to defrauded customers is not their responsibility. Regulation E, the federal law for electronic transfers, requires banks to only cover unauthorized transactions. Most scams will trick people into making the transfers themselves which loses them the opportunity to claim their money back. [16](#)

Cash App is an emerging financial payment service that is seeing an increase in several fraud schemes and illicit activity that can be expected from P2P services. Firstly multiple fake cash app support schemes have emerged in which scammers are imitating customer support to obtain PII and gain access to accounts. These support lines will ask customers to share their screens or directly ask for account information to gain access. Secondly, Cash App does an official sweepstakes called Cash App Friday which is often imitated. Fake accounts are created on social media sites tricking people into thinking they won the sweepstakes and in turn asking them to send a small amount of money to verify their identity. In turn they take the money, block the user, and the user has no way of recovering their funds. Thirdly, Cash App does not provide complete buyer protection which allows people to sell fake items through the app. Consumers should use caution when making a purchase over Cash App for items like tickets because once they send the money, the seller can vanish with the money.

Case Study - Cash App Phone and Sweepstake Scams

Charee Mobley fell victim to the customer support Cash App scam after using the service during the covid pandemic as a quick means to pay bills and do online banking. After noticing an online shopping charge on her account, she looked up a cash app support number for assistance with her account. However this support number was fake and asked her to download software which allowed them to take control of the app and drain her account. Mobley was depending on the last \$166 in her account to get her through the last two weeks of August 2020. Another victim, Emily Bradford, fell for the sweepstakes scam. She received a

direct message through Twitter informing her that if she sent a clearance payment of \$75 she would receive a prize of \$3,000. However as soon as she sent the money, the receiver disappeared leaving her money gone. This demonstrates the small amount many lose due to cash app sweepstake scams and how easily people can fall for it across multiple social media platforms. It was reported by Sixgill that Cash App received about 10,577 posts on the DarkNet, up 450 percent over the previous year, indicating illicit actors are keeping it in mind as a means to engage in fraud. Square also implemented the option for people to transact in Bitcoin on the app which has allowed money to be sent to anonymous addresses and more difficult to trace. Illicit actors are constantly finding means to exploit these apps and there are many more victim examples that exemplify the diligence needed by customers when utilizing these services.

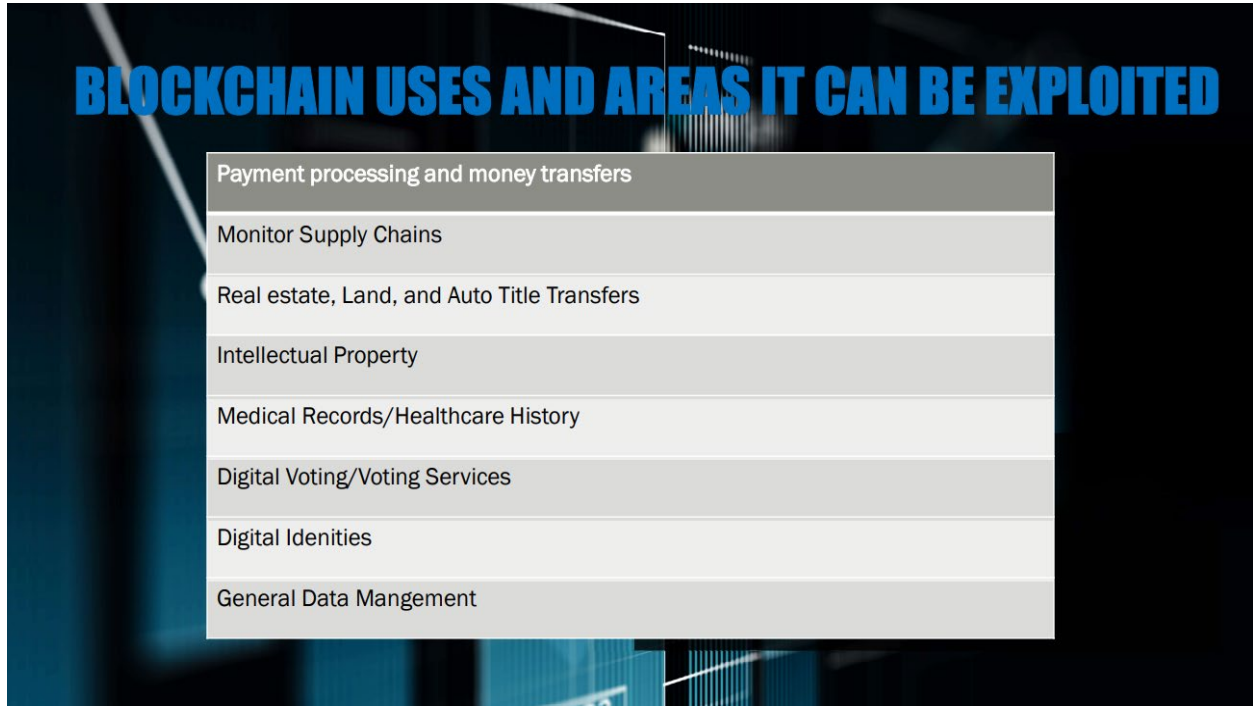
Another new development of concern that was addressed earlier in this report are mixers and tumblers which mix streams of potentially identifiable cryptocurrency. These make cryptocurrencies difficult to trace and improves anonymity of transactions making it another ideal choice for illicit actors. Although actors can use single privatized cryptocurrency, mainly Monero, to hide their identities there are still other currencies utilized in illicit transactions and criminals will always have to find creative ways in covering these transactions.

Case Study: Larry Harmon and Helix

In August 2021 Larry Harmon pleaded guilty to conspiracy to launder money instruments after it was discovered the bitcoin mixer he operated, Helix, was used to hide and launder money. Harmon was originally arrested for operating Helix as an unlicensed money-transmitting business and it was reported that more than \$300 million in bitcoin was laundered on the platform. Harmon admitted during his hearing that he colluded with several darknet marketplaces inducing AlphaBay, Evolution, and Cloud 9 to provide Bitcoin money laundering services to customers. This case again demonstrated how the transparent nature of the blockchain allowed investigators to determine Harmon as the operator of the service and the large amount of bitcoin he was earning from commissions of the service, which was valued at over \$300 million.¹⁷

There are a variety of other uses centering on blockchains that have the potential to be exploited in the future. Although payments processing and money transfers are the first use to come to mind, there are a variety of uses for blockchain technology. Although this does come with the benefit of making everyday actions more streamlined, it also comes with associated risks of putting information online and vulnerable to exploitation. A future research project or additional phase of this research could address the wide range of uses of blockchain technologies and the positive and negative implementations it can have. Our group identified

some of the key areas that can adopt blockchain technology and potentially be exploited in the chart below:¹⁸



Key Findings & Recommendations

The most effective changes to reduce illicit activity in emerging financial technologies, cryptocurrencies, blockchain applications, and other digital payments systems can be implemented by both stakeholders and consumers. Stakeholders hold the power to implement regulatory changes that can significantly reduce the opportunity for illicit activity. Consumers hold the power to be knowledgeable users of cryptocurrencies and online payment platforms to reduce the opportunities to be defrauded and scammed.

One of the strongest changes cryptocurrency exchanges and other digital payment companies can implement are stronger KYC factors. Although cryptocurrency exchanges have adapted more KYC elements, many platforms are significantly lacking any or may not even possess any at all besides an email to sign up. Defi platforms especially have room for improvement. As stated in the Chainalysis 2021 Crime Report “DeFi platforms allow users to swap one type of cryptocurrency for another without a centralized platform ever taking custody

of the users' funds. The lack of custody means that many DeFi platforms believe they don't have to take KYC information from customers, making it easier for cybercriminals to move funds with greater anonymity." Defi platforms don't report on transaction activity as some other platforms are required by the Bank Secrecy Act and other financial regulations.¹⁹

Shifting to the consumer side, there are many precautions that can be taken to reduce exposure to illicit activity. In the 2021 IC3 Internet Crime Report it was reported that many victims of romance scams were being pressured into investment opportunities. "The IC3 received more than 4,325 complaints, with losses over \$429 million, from Confidence Fraud/Romance scam victims who also reported the use of investments and cryptocurrencies, or pig butchering." In these scams, initial contact is made via social media websites and dating apps. Once trust is gained, the scammer will bring up a cryptocurrency investment opportunity. Consumers need to be careful of who they communicate with and befriend online. Consumers should do their own diligent research before the purchase of any cryptocurrency and should be cautious when approached about any investment opportunities.²⁰

Another growing scam is cryptocurrency and online digital payment support impersonators. In these scams digital currency owners are informed of an issue with their crypto wallet and are told to give access to their wallet or transfer the content of their current wallet to a different one. On the other hand, digital currency owners are increasingly seeking advice and assistance with their currencies which is leading them to the wrong support contacts and potentially giving their information to the wrong people. Consumers have to guard their digital currency information closely. They should safeguard their keys and login information and be wary of any calls or contact from exchanges/providers. Consumers should verify any support information and contacts from where they currently hold their digital assets in the event they need assistance.

Account takeover has also been addressed in the Visa Biannual Threat Report where login credentials are often obtained through social engineering schemes and data breaches can be sold on the dark web. One of the most effective actions consumers can take to prevent this occurrence is to enable multi factor authentication on their accounts. This drastically reduces the potential for threat actors to successfully access a consumer's account. If informed of a data breach, users should change their passwords and login information immediately to protect their data and reduce the risk of their account being hacked.²¹

Consumers should only use reputable cryptocurrency and digital currency exchanges that are U.S. based for purchasing and maintaining funds. Due to a wide range of regulatory issues and differences that exist with non U.S. based cryptocurrency exchanges, the safest

option for consumers is to use U.S. based exchanges. If consumers wish to use exchanges outside the U.S., they should research the legal restrictions and regulatory environment of the country that exchange is based in.

For P2P payment services such as Zelle, consumers should treat transactions as actual cash and should only send the person money if they feel comfortable giving cash to that individual in person. Banks who utilize Zelle and stand-alone services such as Square and Paypal should continue to push out education for consumers of their services to protect them from any fraud. Consumers should use caution when receiving and replying to any text messages appearing to be P2P service related and bank related. They should not open links or attachments from texts and should immediately contact a verified bank number to check its legitimacy. Although federal laws could be strengthened to further combat illicit use of P2P services, the most effective change to stop criminal activity in this realm is consumer education.²²

Increased policies and regulations have to be implemented in the digital asset space. Government should determine the category of asset class for cryptocurrencies to enact and enforce policy and regulations. As things stand right now, cryptocurrency is still under debate as to what it should be classified as. Even if cryptocurrency has the classification as a security or commodity, this could still be challenged and other emerging blockchain financial interests like NFTs may not fall under the same designation.

Impact on Government and Private Sector

As criminals become more sophisticated in their fraud schemes and take advantage of emerging financial technologies, it will be important for laws to adapt to new technology and digital assets that emerge. Districts across the U.S. are at times hesitant to prosecute crimes involving digital assets due to their unregulated and less restricted nature. It is key for the U.S. to adapt swift laws and regulations as new digital assets such as NFTs rise in popularity. Without the right laws being put into effect and precedent taking place, illicit actors will continue to take advantage of new digital assets. It will also be important for legal personnel to keep the language of digital assets simple enough for judge, jury, etc. to understand so that case can successfully be tried. It will increasingly become important for both private and public sector collaboration to share intelligence and findings as the digital asset space evolves.

There are multiple federal agencies that are stepping up as leaders to combat crimes in the digital asset space including the FBI, Secret Service, IRS, and SEC. These agencies are becoming better equipped with cryptocurrency tracing tools and increasing case knowledge

that will help take action against illicit actors in the digital asset space and also help the everyday consumer who falls victim to fraud.

Future Regulations, Forecast, and Areas for Future Study

There are multiple future forecasts and predictions we see illicit actors taking in the cryptocurrency, digital payment, and financial technology space. Firstly illicit actors will seek to use more privacy coins, mainly Monero, to conduct illicit activity as opposed to Bitcoin and other cryptocurrencies. Monero is known as the true private cryptocurrency and that is enticing for illicit actors to switch their activity towards. Monero already acts as a crypto mixer in obfuscating transactions, senders, and receivers so it takes a lot less work on behalf of illicit actors to utilize. Secondly, privacy wallets will increasingly be utilized in illicit activities due to their ability to combine multiple security features including encryption and IP address anonymization. Elliptic reported in 2020 that privacy wallets are used in 13% of Bitcoin proceeds of illicit actors, up 2% from the previous year.²³ This percentage will increase as more criminals seek to privatize the final source of their funds. There are already darknet markets emerging and in use which exclusively use Monero. This will likely become more of a common practice as federal agencies continue to have successful cases in criminals using Bitcoin and other currencies besides Monero. Darknet markets are implementing increased security and there will be an increase in direct buyer to vendor communication to avoid further parties in illicit transactions. Criminals will continue to seek opportunities for decentralization of digital assets through chain hopping and cashing out to fiat currency to decrease the risk of being discovered by investigators.²⁴

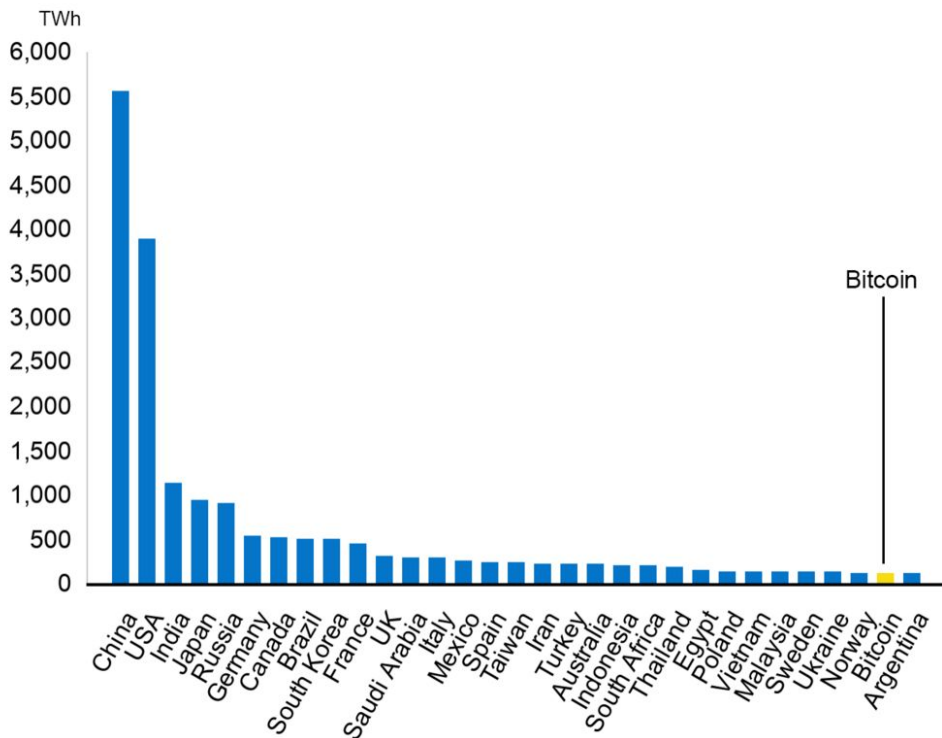
The SEC is currently examining NFTs to determine if they are illegal offerings. NFTs will be considered securities if they pass the Howey test, a standard used to determine if there is an investment contract in a transaction. SEC Commissioner Hester Peirce stated certain pieces of NFTs might fall in the SEC's jurisdictions. As cryptocurrencies see more regulations, people could potentially turn to NFTs as a main form of hiding money from illicit activity. We could also see more cryptocurrency exchanges and digital asset providers move headquarters outside the U.S. due to increased U.S. sanctions. There is already precedent of crypto exchanges moving their headquarters to other locations worldwide to avoid certain sanctions or even to gain certain advantages as some countries/locations offer to attract digital asset providers. We will likely increasingly see exchanges, NFT providers, and other digital asset suppliers be charged under money laundering or operating an unlicensed money service business. Chainalysis introduced cross chain investigations to their investigative tool, Reactor, in March 2022. As cryptocurrency tracing platforms and companies introduce the tools to allow tracing across

different blockchains, it will be harder for illicit actors to hide their activity. There will continue to be greater advancements in tracking activity across different blockchains. [25](#)

Another area that will see increased regulation is the process of cryptocurrency mining. New York has recently introduced legislation that would restrict the mining of digital assets. In this legislation, there would be a two year suspension on reactivating fossil fuel plants for off the grid cryptocurrency mining. Mining has become a hot topic due to the high amount of energy involved and environmental impact it has. Texas is already becoming a hub to Bitcoin mining and we will likely see other states embrace mining due to the economic benefits associated with the practice. However some states will increasingly issue restrictions on the practice due to the overall environmental implications it has. [26](#)

Bitcoin uses more energy than Argentina

If Bitcoin was a country, it would be in the top 30 energy users worldwide



National energy use in TWh/h

Source: University of Cambridge Bitcoin Electricity Consumption Index



We will also continue to see the creation, rise, and growth of blockchain analytic firms that work with both the private and public sector to provide greater visibility into digital asset transactions. This space is still developing and we will likely see new entrants as digital assets evolve and both compliance and investigations increase. Our group examined some of the top analytic firms throughout our research and they are summed up in the table below:²⁷

Company	Description
Chainalysis	Currently the top analytic firm in monitoring blockchain transactions. Utilizes a tool called Reactor that can conduct cross chain investigations.
Elliptic	Draws data from both the public and private to identify real world identities on blockchain. Has assessed risk on transactions worth several trillion dollars
CipherTrace	One of first firms to emerge. Collects millions of data points each week and implements machine learning to remove anonymity from transactions.
Coin Metrics	Delivers one of the largest feeds of on chain data for analysis and trading. Helps users to create value and better use blockchain based assets.
Elementus	Uses a blockchain index methodology similar to Google. Provided key data for Cryptopia hack and QuadrigaCx collapse.

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 Separated by Sections

Most Common Illicit Finance Activities

1. <https://www.bloomberg.com/news/articles/2022-03-10/crypto-obfuscator-tornado-says-sanctions-cant-affect-smart-contracts>
2. <https://www.bleepingcomputer.com/news/cryptocurrency/620-million-in-crypto-stolen-from-axie-infinitys-ronin-bridge/>
3. <https://go.chainalysis.com/2022-Crypto-Crime-Report.html>
4. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Most Exploited Elements of Financial Technologies

1. <https://financesonline.com/what-is-fintech/>
2. <https://www.bankrate.com/investing/best-online-brokers-for-stock-trading/>
3. <https://www.morningstar.com/articles/1088193/the-best-robo-advisors-of-2022>
4. <https://www.pwc.co.uk/financial-services/fintech/assets/FinTech-Global-Report2016.pdf>
5. <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>
6. https://www.business-standard.com/article/international/germany-s-wirecard-fake-client-data-to-gain-%C2%A3900-mn-from-softbank-report-122071100662_1.html
7. <https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million>
8. <https://cyware.com/news/hackers-demand-300-btc-from-binance-cryptocurrency-exchange-over-kyc-data-leak-95acc1b5>

Legal & Technological Vulnerabilities

1. <https://www.newyorker.com/business/currency/the-challenges-of-regulating-cryptocurrency>
2. <https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122>
3. <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa>
4. <https://www.weforum.org/agenda/2022/03/where-is-cryptocurrency-regulation-heading/>
5. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>
6. <https://www.fincen.gov/news/news-releases/agencies-invite-comment-proposed-rule-under-bank-secrecy-act>

Pseudo-Anonymity and Weaknesses in KYC through Future Regulations, Forecast, and Areas for Further Study

1. <https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer>
2. <https://www.ai-cio.com/news/fbi-arrests-alleged-operator-of-longest-running-bitcoin-laundering-service/>
3. <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>
4. <https://cointelegraph.com/news/doj-seizes-3-6b-in-crypto-and-arrests-two-in-connection-with-2016-bitfinex-hack>
5. <https://www.miamiherald.com/news/local/article260097885.html>

6. <https://protos.com/fincen-crypto-exchanges-must-register-treasury-bank-secrecy-act/>
7. <https://getid.com/aml-kyc-crypto-exchanges-wallets/>
8. <https://complyadvantage.com/insights/crypto-regulations/cryptocurrency-regulations-united-states/>
9. <https://www.reuters.com/legal/government/two-us-men-arrested-1-mln-non-fungible-token-rug-pull-scheme-2022-03-24/>
10. <https://www.forbes.com/sites/jeffkaufman/2022/04/14/why-jack-dorseys-first-tweet-nft-plummeted-99-in-value-in-a-year/?sh=515a0e8c65cb>
11. <https://www.zdnet.com/article/bugs-allowing-malicious-nft-uploads-uncovered-in-opensea-marketplace/>
12. <https://www.jdsupra.com/legalnews/fincen-issues-report-addressing-nfts-4844549/>
13. <https://slate.com/technology/2019/01/fortnite-video-games-money-laundering-scams.html>
14. <https://librehash.org/squid-token-rug-pull-analysis-entire-crypto-space-needs-to-pay-attention/>
15. <https://www.reuters.com/article/us-secondlife-gambling-1/fbi-checks-gambling-in-second-life-virtual-world-idUSHUN43981820070405>
16. <https://www.nafcu.org/compliance-blog/cfpb-updates-regulation-e-faqs-address-p2p-payments-and-providers>
17. <https://www.justice.gov/usao-dc/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300>
18. <https://www.insiderintelligence.com/insights/blockchain-technology-applications-use-cases/>
19. <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. <https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/visa-public-pfd-biannual-threats-report.pdf>
22. <https://www.nclc.org/media-center/fed-must-do-more-to-protect-consumers-from-fraud-and-mistakes-in-new-p2p-payment-system.html>
23. <https://www.elliptic.co/blog/13-bitcoin-crime-laundered-through-privacy-wallet>
24. <https://slate.com/technology/2021/11/monero-privacy-coin-racists-cybercriminals.html>
25. <https://www.jdsupra.com/legalnews/can-some-nfts-be-considered-securities-4145661/>
26. <https://www.cnn.com/2022/05/05/new-york-bitcoin-mining-moratorium-proceeding-through-state-house.html>
27. <https://101blockchains.com/top-blockchain-analytics-companies/>

Citations for Most Common Illicit Finance Activities

(U) | Bloomberg | MAR 2022 | Crypto Mixer Tornado Cash Says Sanctions Can't Apply to Smart Contracts <https://www.bloomberg.com/news/articles/2022-03-10/crypto-obfuscator-tornado-says-sanctions-cant-affect-smart-contracts#xj4y7vzkg>

(U) | Bleeping Computer | MAR 2022 | \$620 million in crypto stolen from Axie Infinity's Ronin bridge <https://www.bleepingcomputer.com/news/cryptocurrency/620-million-in-crypto-stolen-from-axie-infinitys-ronin-bridge/>

(U) | FBI | MAR 2022 | The 2021 IC3 Internet Crime Report https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf



(U) | Chainalysis | 2022 Crypto Crime Report | FEB 2022 | The 2022 Crypto Crime Report
<https://go.chainalysis.com/2022-Crypto-Crime-Report.html>

Citations for Most Exploited Elements of Financial Technologies

(U) | Finances Online | OCT 2019 | What is FinTech? Examples of Types, Products, & Regulations
<https://financesonline.com/what-is-fintech/>

(U) | Bankrate | JUNE 2022 | Best Online Brokers for stock trading in June 2022
<https://www.bankrate.com/investing/best-online-brokers-for-stock-trading/>

(U) | Morningstar | APRIL 2022 | The Best Robo-Advisors of 2022
<https://www.morningstar.com/articles/1088193/the-best-robo-advisors-of-2022>

(U) | PWC | MARCH 2016 | Blurred lines: How FinTech is shaping Financial Services
<https://www.pwc.co.uk/financial-services/fintech/assets/FinTech-Global-Report2016.pdf>

(U) | Business Standard | JULY 2022 | Germany's Wirecard fake client data to gain £900 mn from SoftBank: Report
https://www.business-standard.com/article/international/germany-s-wirecard-fake-client-data-to-gain-%C2%A3900-mn-from-softbank-report-122071100662_1.html

(U) | Department of Justice | Aug 2021 | Ohio Resident Pleads Guilty to Operating Darknet Based Bitcoin Mixer Laundered Over 300 Million
<https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million>

(U) | Cyware Social | Aug 2019 | Hackers demand 300 BTC from Binance cryptocurrency exchange over KYC data leak
<https://cyware.com/news/hackers-demand-300-btc-from-binance-cryptocurrency-exchange-over-kyc-data-leak-95acc1b5>

Citations for Legal & Technological Vulnerabilities

(U) | The New Yorker | OCT 2021 | The Challenges of Regulating Cryptocurrency
<https://www.newyorker.com/business/currency/the-challenges-of-regulating-cryptocurrency>

(U) | Investopedia | MAY 2022 | Cryptocurrency Regulations Around the World
<https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122>



(U) | Global Legal Insights | 2022 | Blockchain and Cryptocurrency Laws and Regulations 2022
<https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa#chaptercontent1>

(U) | World Economic Forum | MAR 2022 | Cryptocurrency Regulation: where are we now, and where are we going <https://www.weforum.org/agenda/2022/03/where-is-cryptocurrency-regulation-heading/>

(U) | FATF | OCT 2021 | Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Providers <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>

(U) | FinCen | OCT 2020 | Agencies Invite Comment on Proposed Rule under Bank Secrecy Act
<https://www.fincen.gov/news/news-releases/agencies-invite-comment-proposed-rule-under-bank-secrecy-act>

Citations for Pseudo-Anonymity and Weaknesses in KYC - Future Regulations, Forecast, and Areas for Further Study

(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) | Chief Investment Officer | MAY 2021 | FBI Arrests Alleged Operator of Longest Running Bitcoin Laundering Service <https://www.ai-cio.com/news/fbi-arrests-alleged-operator-of-longest-running-bitcoin-laundering-service/>

(U) | New York Times | MAR 2022 | Fraud is Flourishing on Zelle. The Banks Say It's Not Their Problem <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>

(U) | Coin Telegraph | FEB 2022 | DOJ Seizes \$3.6B In Crypto and Arrests two in connection with 2016 Bitfinex hack <https://cointelegraph.com/news/doj-seizes-3-6b-in-crypto-and-arrests-two-in-connection-with-2016-bitfinex-hack>

(U) | Miami Herald | APRIL 2022 | Feds seize \$34 million of illicit bitcoin linked to 'Dark Web'
<https://www.miamiherald.com/news/local/article260097885.html>



(U) | Protos | MAR 2022 | US Treasury urges crypto exchanges to register with FinCEN
<https://protos.com/fincen-crypto-exchanges-must-register-treasury-bank-secrecy-act/>

(U) | getid | JAN 2022 | The 2022 Guide to KYC/AML for Crypto Exchanges & Wallets
<https://getid.com/aml-kyc-crypto-exchanges-wallets/>

(U) | Comply Advantage | Cryptocurrency Regulations in the US
<https://complyadvantage.com/insights/crypto-regulations/cryptocurrency-regulations-united-states/>

(U) | Reuters | MAR 2022 | Two U.S. Men Arrested for \$1 mln non-fungible token “rug pull” scheme
<https://www.reuters.com/legal/government/two-us-men-arrested-1-mln-non-fungible-token-rug-pull-scheme-2022-03-24/>

(U) | Forbes | APR 2022 | Why Jack Dorsey’s First-Tweet NFT Plummeted 99% In Value In A Year
<https://www.forbes.com/sites/jeffkauffman/2022/04/14/why-jack-dorseys-first-tweet-nft-plummeted-99-in-value-in-a-year/?sh=2161f55e65cb>

(U) | ZDnet | OCT 2021 | Bugs Allowing Malicious NFT uploads in OpenSea marketplace
<https://www.zdnet.com/article/bugs-allowing-malicious-nft-uploads-uncovered-in-opensea-marketplace/>

(U) | JDSUPRA | FEB 2021 | FinCEN Issues Report Addressing NFTs
<https://www.jdsupra.com/legalnews/fincen-issues-report-addressing-nfts-4844549/>

(U) | SLATE | JAN 2019 | Cybercriminals are using Fortnite to Launder Money
<https://slate.com/technology/2019/01/fortnite-video-games-money-laundering-scams.html>

(U) | LibreHash Newsletter | NOV 2021 | SQUID Token ‘Rug Pull’ Analysis (Entire Crypto Space Needs to Pay Attention)
<https://librehash.org/squid-token-rug-pull-analysis-entire-crypto-space-needs-to-pay-attention/>

(U) | Reuters | APRIL 2007 | FBI checks gambling in Second Life virtual world
<https://www.reuters.com/article/us-secondlife-gambling-1/fbi-checks-gambling-in-second-life-virtual-world-idUSHUN43981820070405>

(U) | NAFCU | FEB 2022 | CFPB Updates Regulation E FAQs to Address P2P Payments and Providers
<https://www.nafcu.org/compliance-blog/cfpb-updates-regulation-e-faqs-address-p2p-payments-and-providers>

(U) | U.S. Dept. of Justice | AUG 2021 | Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin ‘Mixer’ That Laundered Over \$300 Million
<https://www.justice.gov/usao-dc/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300>



(U) | Insider Intelligence | APRIL 2022 | The growing list of applications and use cases of blockchain technology in business and life
<https://www.insiderintelligence.com/insights/blockchain-technology-applications-use-cases/>

(U) | Chainalysis | 2022 Crypto Crime Report | FEB 2022 | The 2022 Crypto Crime Report
<https://go.chainalysis.com/2022-Crypto-Crime-Report.html>

(U) | FBI | MAR 2022 | The 2021 IC3 Internet Crime Report
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

(U) | Visa | DEC 2021 | Biannual Threat Report
<https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/visa-public-pfd-biannual-threats-report.pdf>

(U) | NCLC | SEPT 2021 | Feds Must Do More to Protect Consumers From Fraud and Mistakes in New P2P Payment System
<https://www.nclc.org/media-center/fed-must-do-more-to-protect-consumers-from-fraud-and-mistakes-in-new-p2p-payment-system.html>

(U) | Elliptic | DEC 2020 | Over 13% of All Crime in Bitcoin are Now Laundered Through Privacy Wallets
<https://www.elliptic.co/blog/13-bitcoin-crime-laundered-through-privacy-wallet>

(U) | SLATE | NOV 2021 | The Bitcoin Competitor Beloved by the Alt-Right and Criminals
<https://slate.com/technology/2021/11/monero-privacy-coin-racists-cybercriminals.html>

(U) | JDSUPRA | MAR 2022 | Can Some NFTs be Considered Securities? THE SEC Is Watching
<https://www.jdsupra.com/legalnews/can-some-nfts-be-considered-securities-4145661/>

(U) | CNBC | MAY 2022 | New York is close to a bitcoin mining crackdown - here's what that means for the industry
<https://www.cnbc.com/2022/05/05/new-york-bitcoin-mining-moratorium-proceeding-through-state-house.html>

(U) | 101 BLOCKCHAINS | JUNE 2021 | Top 5 Blockchain Analytic Companies 2022
<https://101blockchains.com/top-blockchain-analytics-companies/>

Appendices

Appendix A: Cryptocurrency Pamphlet

Items to Consider Before Investing

The below table reflects some of the most common examples of fraudulent, illegal, and legal crypto exchanges and/or websites.

It is important to note that scams work because they often appear as legitimate activity.

✔	⚠	✘
Information can be found online for the company, white papers, and products.	Information is limited on the company, white papers, and products.	Information is not available for the company and products and no white paper is available.
Website has a security certification, good grammar, company logo, and secure payment options. Verifiable contact information.	Domain appears similar and has company logo but contact information is not verifiable.	Suspicious domain name (.xyz), website has misspellings, and no security certificate.
Reviews are good and indicate happy customers.	Reviews are limited or include no details on customer experience.	Reviews are negative and indicate customers have been scammed or were involved in bad activity.
Has country regulator and oversight.	Has minimal oversight.	Country has no or limited regulator oversight.
Product is regulated by state and/or federal authority.	Product is not regulated by any state and/or federal authority.	State and/or federal authority has warned about the product/exchange.
You are only able to deposit transactions on your own behalf.		You are being requested to deposit, transact on behalf of another person.
Return is based on investment and time.	Is there a promise to make money within two to three months?	Is there a promise to make money at no cost or within 24, 48 hours?
Are you required to provide a photo ID, address, and telephone number before making purchase?	Exchange does not require any information to transact.	Exchange requests information which could be used for identity theft to include security questions/ answers.

Additional Resources

The following websites may provide additional information:

www.ic3.gov
Fraud types and schemes
Report a crime

www.secretservice.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

<https://bitcoin.org/en/scams>
Reporting on common scams



DEFENSE INTELLIGENCE AGENCY
COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION

RITM0387993 | This product was designed by FAC2A Creative Design Services.

Tips For a Safe Cryptocurrency Experience



2022

PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies

This program enable 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.

What You Need to Know

About Protecting Yourself

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

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.

About the Cryptocurrency Service Provider

The cryptocurrency market is changing and growing daily. As an investor it is important to understand how to identify available resources, and the indicators of a good or bad exchange as well as understanding that with the changing market, those resources may also change. Additionally, you must have a firm grasp of your own comfort level with the risk posed in trading and investing in cryptocurrency.

Below are some items to consider and understand before investing in the cryptocurrency market.

Before selecting an exchange/platform, understand who the company is and read up on the company. Below are examples of items to understand about the company.

- **Team/Ownership/Partnership**
 - ✓ Publicly available profiles and ownership information as well as company goals and partners or investors.
 - ✗ No available information for company ownership or company goals, partners or investors.
- **Company's Technology**
 - ✓ Easily accessible web page and white paper that outlines specifics and details of the project.
 - ✗ No white paper available, or few details on the specifics behind the project.
- **Purpose**
 - ✓ Website explains the origins of the company and reasons the team started the project are values you agree with.
 - ✗ Website does not include origins of the company and reasons the project was started are not listed or you do not represent values you agree with.
- **Regulation**
 - ✓ The service provider is regulated by a trusted regulator such as a country Financial Intelligence Unit or Financial Crimes Enforcement Network.
 - ✗ The service provided is unregulated or in a country that has legal or regulatory challenges.
- **Review Customer Support Options**
 - ✓ Website with published FAQs on how to use the product, live customer support, and tips for safe investing.
 - ✗ No FAQs and no or only automated customer support options.

About Digital Assets

As with any investment, it is important to understand exactly what you are investing in before you start. Crypto is an evolving world, and exchange ratings change often. Conduct your research before investing.

Ensure that you understand cryptocurrency key terms such as:

- Bitcoin and Altcoins
- Token/Non-Fungible token (NFT)
- Blockchain
- Public Key/Address
- Wallet and Private Key
- Seed Phrase

Cryptocurrency

A digital currency that isn't regulated by a central authority, like a bank. Cryptocurrency, such as Bitcoin or Ethereum, can be used to buy everyday items, purchased on cryptocurrency exchanges, or traded on investment platforms.

Stablecoins

Cryptocurrencies can experience significant changes in value, so stablecoins are pegged to a more stable currency on commodity, such as the U.S. dollar or gold, in an attempt to offer price stability.

CBDCs

Central Bank Digital Currencies, such as China's digital yuan, are issued and regulated by a country's central bank and pegged to the value of that country's fiat currency.

Privacy Coins

Privacy coins like Monero offer users more anonymity than other cryptocurrencies by hiding the value of payments across their networks as well as their senders and recipients.

Tokens

A unit of value on a blockchain that also has some other value propositions. For example, non-fungible tokens (NFTs) are used to represent ownership of unique digital items like art or collectibles.

Appendix B: NFT Product

Tips for a Safe Non-Fungible Tokens (NFTs) Experience

2022 Public-Private Analytic Exchange Program

A non-fungible token (NFT) is a cryptocurrency token that is indivisible and unique. One NFT cannot be interchanged with another NFT, and the whole cannot be broken down into smaller parts and used. NFTs are a niche market and a very new commodity. Some NFTs may be valuable, which can make them a target for fraud, counterfeiting, and/or theft. NFTs have been utilized for purposes such as creating digital or crypto-collectibles, managing ownership of digital items within blockchain-integrated games, and proving authenticity of digital art while allowing artists to retain their intellectual property—and in some cases, are used for items such as event tickets.

For a safer experience, ensure you understand Non-Fungible Tokens (NFTs) and key related terms, such as the below, before you invest.

- Smart contract
- Blockchain
- Contract address
- Token ID

The NFT market is a new and evolving market. As with any new investment, there are risks involved. The below chart is designed to assist you in better understanding some of the red flag scenarios you should be aware of.

✓	✗
Website is a known NFT marketplace with good reviews and reputation.	Website has limited or negative reviews or reports indicating customers have been victims of fraud.
Seller has an external site with the NFT road map, history of sales, good reviews, and information about their art.	Seller has an external site with limited or no reviews or other information.
The time, place and price of the NFT sale is widely publicized.	NFT sale information is shared in a limited manner or sent via DM or individual communication.
The cost of the NFT is reasonable in comparison to the rarity and popularity of the NFT.	The cost of the NFT is significantly higher than others of the same popularity or significantly lower than others of the same rarity.
The purchase is conducted on an open-forum website which charges fees.	The purchase is conducted in a private setting to avoid paying any fees.

Common Scams Involving NFTs

Impersonation/Phishing: Scammers can replicate popular NFT websites and marketplaces to trick users into logging into a counterfeit website. These scams can result in account login information being compromised, or trick users into spending money on counterfeit digital artwork on the fake page. Scammers posing as legitimate trading platforms can also send phishing emails containing fake NFT offers, with the aim of obtaining your login information.

To avoid this scam: Always verify the URL of the NFT marketplace website you are using and the sender address of any related email you receive before attempting to login or make purchases.

Rug pull scams: In this type of scam, a criminal promotes an NFT to investors which appears legitimate, but turns out not to be resellable, and then disappears with all the funds, leaving victims with an asset that has little to no resale value.

To avoid this scam: Verify the credentials of any NFT investment project you are pursuing, including researching the background of the project owners.

Counterfeit NFTs: Counterfeit NFTs are copied from someone else's genuine work. Scammers selling counterfeit NFTs trick victims into believing they are buying a unique NFT; however, just like with physical counterfeit goods, the counterfeit NFT has no genuine value.

To avoid this scam: Always confirm the seller's credibility and stick to reputable marketplaces.

Pump and dump scheme: Scammers use these schemes to artificially drive up the price of an NFT by making several bids within a short time span to make it appear as though the NFT is popular. Once the selling price is inflated, the scammers will cash out and sell it to the highest bidder for far above its true value.

To avoid this scam: Review the transaction history of the desired NFT. Several transactions centered around one date could indicate a pump and dump scheme.

Smart Contract scams: Scammers can include hidden fees or clauses in smart contracts designed to steal your money—such as 99% buy or sell fees—and cybercriminals can also exploit vulnerabilities in legitimate smart contracts.

To avoid this scam: Ensure that you review a token's smart contract before purchasing, and engage a trusted resources to help you understand it if necessary.

Tips to Keep You and Your NFT Safe

There are simple steps which can be taken to safeguard your online information as well as your NFT when participating in cryptocurrency markets.

- **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 seed phrase, and do not repeat them or share them.
- When possible, store your NFT in a cold-storage wallet that is protected from hackers.
- Only purchase NFTs from reputable sites—not via social media requests from persons you do not know.
- If you receive an email regarding a password change that you did not request, do not click the links.
- Always ensure you understand the smart contract or obtain assistance from a reputable/trusted person.
- Always log out of your wallet and any sites you may have your wallet connected to.
- If it seems "too good to be true"—it probably is a scam.

Additional Resources

Definitions
investopedia.com - Smart contracts
coinbase.com - What is a smart contract?

Fraud Resources
nftnow.com - How to identify and avoid NFT scams
fbi.gov - Scams and safety on the Internet
secretsservice.gov - Combating illicit use of digital assets

Federally Prosecuted Cases
justice.gov - Former employee of NFT marketplace charged in first ever digital asset insider trading scheme
justice.gov - Two defendants charged in NFT fraud and money laundering scheme

2022 Public-Private Analytic Exchange Program
Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies

Disclaimer: 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 purposes only and may not be used for advertising or product endorsement purposes. All judgements and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.



