Recovering Laundered Cryptocurrency Assets in an Evolving Regulatory Framework

Research Project for Emerging Issues/Advanced Topics Course

Master of Forensic Accounting Program

University of Toronto

Al Pomerant

June 19, 2022

Table of Contents

1.0 INTRODUCTION

In less than 15 years since its inception, cryptocurrency has grown exponentially in mainstream acceptance and popularity. In November 2021, the global cryptocurrency market capitalization was $3 trillion.[1] This year's Super Bowl in 2022 featured ads from three cryptocurrency exchanges starring celebrities like LeBron James and Matt Damon.[2] In March 2022, Conservative leader candidate Pierre Poilievre pitched cryptocurrency as a way that Canadians could "opt out of inflation".[3] Unprecedented increases in values and expectations of continual growth have drawn in investors with small amounts of savings willing to take big risks. As well, cryptocurrency exchanges have made it easy for the general public to become crypto investors.

[1] Asmakov, A. "Crypto's Total Market Cap Slips Below $1 Trillion as Bitcoin Drops Under $24,000," *Decrypt*, June 13, 2022. https://decrypt.co/102737/cryptos-total-market-cap-slips-below-1-trillion-as-bitcoin-drops-under-24000, Accessed June 14, 2022
[2] Mellor, S. "Crypto companies spent millions on Super Bowl ads. So did Pets.com," *Fortune*, February 14, 2022 https://fortune.com/2022/02/14/crypto-companies-super-bowl-ads-coinbase-ftx-bitcoin-ether/, Accessed April 29, 2022.
[3] Tasker, J.P. "In a pitch to cryptocurrency investors, Poilievre says he wants Canada to be 'blockchain capital of the world'," *CBC News*, March 28, 2022, https://www.cbc.ca/news/politics/poilievre-bitcoin-policy-1.6399986, Accessed April 30, 2022

In spite of the growth in value and public appeal, governments and regulatory agencies around the world have been slow to robustly enforce existing law or enact meaningful regulatory frameworks for cryptocurrencies. In the past month, one stablecoin has plummeted in value and a cryptocurrency exchange has frozen withdrawals amidst financial woes, contributing to the market capitalization of cryptocurrency dropping below $1 trillion, a mere 7 months from its all-time high.[4] Cryptocurrency's populist appeal has drawn unsophisticated and speculative investors who may not appreciate, or who may willingly ignore, the significant risks they take with their monies.

The 21st century has shown that governments can be slow to react and adapt to emergent technologies, with companies like Uber and AirBNB, able to generate massive profits and establish dominant market shares across the world, before regulatory regimes were enacted. And even in the instances where regulatory regimes have been implemented, they are often fragmented and weak, and bowing to the expectations of popular technology companies. Governments have been too willing to accept the arguments of Uber and AirBNB that they are not what they clearly are: a cab company and a small-scale hotel operator, respectively. Cryptocurrencies and exchanges are following a similar path, arguing they aren't currencies, commodities or securities. Cryptocurrency poses an even greater challenge to regulators than AirBNB and Uber, as the deliberate anonymity and lack of regulatory oversight has long attracted criminal actors. As with much of globalization, effective cryptocurrency regulation may require international cooperation. Even a few non-cooperating countries can provide immunity to bad actors.

The concern that unregulated cryptocurrencies may be used by criminal actors to carry out illicit acts and evade punishment dates back the early days of cryptocurrency. In 2011, the dark website 'Silk Road' was launched as a marketplace for narcotics, which was only possible because of the anonymity of

[4] Asmakov, A, 2022.

financial transactions of Bitcoin.[5] Silk Road had over 1 million users by 2013 before U.S. government agencies arrested the founder and shut down the site.[6] Cryptocurrency continues to be an attractive option for money laundering, with cybercriminals laundering $8.6 billion worth of cryptocurrency in 2021 and $33 billion since 2017.[7]

Investigative Forensic Accountants (IFAs) will need to increase their knowledge of cryptocurrency, crypto money laundering and crypto asset recovery in order to support investigative and law enforcement processes.

This paper intends to review the following:

- An overview of cryptocurrency technology
- An examination of law enforcement proceedings to recover stolen or laundered assets
- Techniques/methods for recovering assets
- An evaluation of regulatory challenges hindering asset recovery
- Recommendations for a robust regulatory framework
- Recommendations for IFA education in cryptocurrency knowledge

[5] Adler, D. "Silk Road: The Dark Side of Cryptocurrency," *Fordham Journal of Corporate & Financial Law*, February 21, 2018, https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/, Accessed May 1, 2022.
[6] Ibid.
[7] Grauer, K. et al. "The 2022 Crypto Crime Report," *Chainanalysis*, 2022, https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf, p10-11.

2.0 EXECUTIVE SUMMARY

This paper will provide an overview of key information that IFAs should know regarding cryptocurrencies, how they operate, how criminals are caught and what regulations apply (as well as what regulations may be coming).

Key Features

Cryptocurrencies are digital currencies that are encrypted using blockchain technology and operate in a decentralized fashion. Its data is spread across thousands of computers that verify the transactions. The twin features for an IFA is that the record of all blockchain transactions is public, but the transaction details are minimal and a buyer and seller are represented by an address code, not their names. Cryptocurrency is generated by mining whereby computers solve complex equations to update the transactions of the blockchain and are awarded newly minted cryptocurrency coins. Cryptocurrency can be stored in cold wallet where the private key is offline or hot wallets which are stored on electronic devices. Stablecoins are a subset of cryptocurrency that are pegged to an underlying asset; however, stablecoins are loosely regulated and susceptible to misuse by criminal actors.

Money Laundering Case Studies

This paper reviews the money laundering stages: placement into the system, layering through the system to cover their trackers and integration back into the economy. Several case studies are reviewed to demonstrate cryptocurrency fraud investigations in practice:

- Silk Road: In 2011, a dark web marketplace called Silk Road proliferated by matching drug dealers and buyers who made payments through Silk Road in Bitcoin.
- Quadriga: A popular Canadian cryptocurrency exchange turned out to be a ponzi scheme.

- Colonial Pipeline: A Russian-based ransomware hack into an American oil company ended with the U.S. recovering of over half the ransom payment.
- Glupteba Botnet: A sophisticated botnet encoded instructions on invalid bitcoin transactions. Investigators were able to trace the funds back to an office building in Moscow where a known cybercriminal had worked from
- Bitfinex Hack: The government traced over 100,000 in stolen Bitcoins to two associates, obtained a warrant and found wallet address passwords on a personal cloud storage.

The case studies highlight the traceability of cryptocurrency, particularly Bitcoin, through the public ledger and what can be accomplished by combining other pieces of information to public blockchain data to recover assets.

Money Laundering Methods

This section reviews some of the common obstacles created by criminal actors in laundering funds:

- Criminal actors can use mixing services, which break funds down into small amounts and combine them with various irrelevant transactions and then redistribute this mix of funds
- Chain peeling can move funds through dozens of wallets, then send small amounts through cryptocurrency exchanges
- Cryptocurrency exchanges have long been exploited by fraudsters, but these exchanges are becoming more regulated, allowing law enforcement to compel information.
- Privacy coins can keep the record of a transaction secret. In response, governments are trying to build better tracking tools and pressuring exchanges to shun privacy coins.

Current Regulation

This paper explores the following aspects of the current regulatory framework:

- The U.S. has a multifaceted and at times contradictory approach as various agencies attempt to regulate cryptocurrency. Cryptocurrency exchanges are regulated through existing law and are expected to comply with anti-money laundering (AML) protocols.
- Canada similarly has imposed requirements on exchanges with regulatory requirements and generally treats cryptocurrencies as securities.
- The Financial Action Task Force (FATF) has developed recommendations, which have influenced a recent EU Directive that orders EU member countries to enact robust laws.
- Switzerland has implemented clear regulatory expectations, encouraging blockchain innovation and providing certainty to entrants.
- Stablecoins make claims of stability that are not always truthful and the recent collapse of Terra Luna, which relied on a risky structure, is examined.
- As well, the challenges of unregulated are examined and sanctions and blacklist appear to be reasonable solution.

Regulatory Recommendations

Looking to the future, regulatory changes are required to avoid dual financial systems, the regulated government version and a wildly unstable cryptocurrency sphere with no oversight. Sensible recommendations include:

- Proactively enforce existing laws and regulations: regulators need to be clear and proactive in asserting their existing jurisdiction.
- Dedicated cryptocurrency legislation: because of the innovations of cryptocurrency, cryptocurrency-specific laws will bring stability
- Broaden the base of regulated entities and draw clear lines on who is excluded.

- Reporting by and oversight of stablecoins is urgently needed given the certainty stablecoins claim to offer in the absence of proof.

Tips for IFAs

Finally, the paper covers tips for IFAs investigating cryptocurrency money laundering:

- Follow the blockchain. The public ledger is a trail of transactions that can lead IFAs to the exit source of the funds or the funds themselves
- Rely on forensic cryptocurrency experts. If criminals attempt any laundering of funds through cryptocurrency, an IFA would be well served to engage cryptocurrency experts who have tracking and visualization tools.

3.0 CRYPTOCURRENCY TECHNOLOGY

3.1 PRIMARY FEATURES

In order for an IFA to investigate cryptoassets, it is essential to understand the underlying technology of cryptocurrency. Cryptocurrency is digital money that is encrypted and decentralized.[8]

Digital	• Exists only in electronic form • No physical equivalent (i.e. no physical coins or paper money) • Intended for use over the internet
Encrypted	• Secured using blockchain

[8] Ashford, K. "What is Cryptocurrency?," *Forbes*, January 25, 2022, https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/, Accessed May 5, 2022.

	• Mathematical codes are used to "store and transmit data values in a secure format"[9]
Decentralized	• No central bank/authority to manage the currency or its value • Also, no banking institutions required to store cryptocurrency/verify transactions • Data is spread across thousands of computers across the world, rather than in one bank's central database

A blockchain is an open ledger records transactions in encoded blocks "linked together on a 'chain' of previous cryptocurrency transactions".[10] Every cryptocurrency user has a copy of the blockchain and the blockchain is repeatedly updated with every new transaction. Computers constantly check and verify the blockchain, which is publicly published, thereby ensuring security.[11] Cryptocurrencies pay for transactions within blockchain networks.

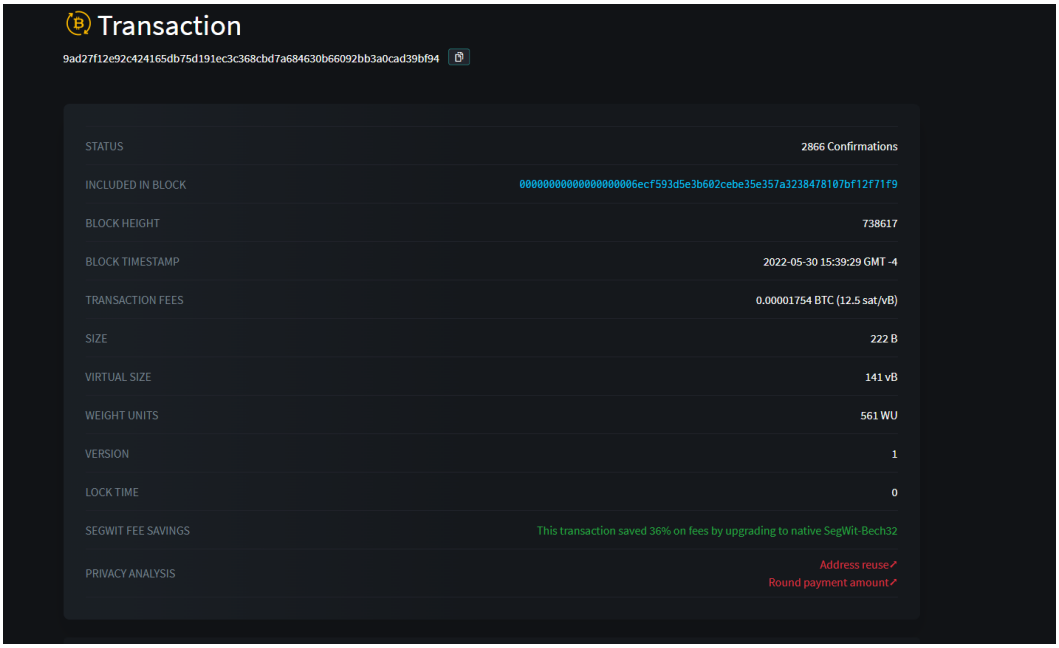
It is this security that afford cryptocurrency users a great deal of privacy. Transactions can at once be open to the public, but allow the user to retain anonymity. Anyone can see the public ledger, but unless they have additional information, they would be unable to identify the sender or receiver. Traditional physical currency moving through electronic financial institutions/systems requires identity verification, necessitating the transfer of personal information.

The combination of an open ledger, but privacy for holders of cryptocurrency poses an interesting combination for IFAs. The flow of assets can be tracked, but not always to specific individuals or specific beginnings or endpoints. Transactions, which can be viewed online provide consistent but

[9] Seth, S. "Explaining the Crypto in Cryptocurrency," *Investopedia*, May 15, 2022, https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/, Accessed May 9, 2022.
[10] Ashford, 2022.
[11] Coinbase. "What is Cryptocurrency?," *Coinbase*, 2022, https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency, Accessed May 9, 2022.

minimal details that reveal little unless combined with other information. See below for an example of a blockchain transaction record.

Figure 1[12]



Another key feature of cryptocurrency is the finality of transactions. Most traditional financial transactions are managed through a particular company, such as a bank or a credit card company. Transactions can be disputed and reversed by the banking institution or company. However, with cryptocurrency there is no centralized company able to undo a transaction. This is a feature that is advantageous to money launderers who can quickly move assets through multiple accounts.

3.2 How Cryptocurrency is Generated

Cryptocurrency mining is both a means of generating new cryptocurrency and a security feature of a blockchain system. Miners who are verified by the cryptocurrency, compute a complex math

[12] Blockstream Explorer, "Transaction," *Blockstream Explorer,* May 30, 2022, https://blockstream.info/tx/9ad27f12e92c424165db75d191ec3c368cbd7a684630b66092bb3a0cad39bf94?output:0, Accessed May 30, 2022.

equation in order to update transactions to the blockchain.[13] As a reward, miners are awarded a certain amount of the cryptocurrency.

There are two different contrasting methods for cryptocurrencies to mine[14]:

Proof of Work	Proof of Stake
• Computers compete to solve an equation in order to verify transactions • Requires vast computing power, as equations become more complex • Used by bitcoin	• Miners must stake (temporarily lock up) a certain amount of that cryptocurrency • Miners' rewards are limited to the amount they staked • Far less energy intensive and produces much faster transaction • Ethereum is planning to convert to proof of stake

Given the role miners play in building a blockchain and blockchain security, it is logical to question whether a cryptocurrency is safe from miners. In order for miners to interfere with the integrity of the blockchain system, the miners would need to control more than 50% of a network's computing power, referred to as a 51% attack.[15] In a successful 51% attack, this group of miners would be able to halt new transactions or reverse completed transactions and double spend cryptocurrency coins.[16] The larger the blockchain network, the more resources required for a group of miners to gain control of more than 50% of the blockchain. While a 51% attack isn't feasible for the world's largest

[13] Bogna, J. "How Does Bitcoin Mining Work?," *PC Mag*, December 9, 2021, https://www.pcmag.com/how-to/how-does-bitcoin-mining-work, Accessed May 3, 2022.
[14] Ashford, 2022
[15] Frankenfield, J. "51% Attack," *Investopedia*, April 27, 2022, https://www.investopedia.com/terms/1/51-attack.asp, Accessed May 25, 2022.
[16] Ibid.

cryptocurrencies, smaller cryptocurrencies, like Bitcoin Gold, an offshoot of Bitcoin, and Ethereum Classic, an offshoot of Ethereum, have been subject to 51% attacks.[17]

3.3 Cryptocurrency Storage and Exchanges

Holders of cryptocurrency assets have three options for storage of their cryptocurrency, with each offering varying degrees of security and ease of use[18]:

Cold Wallet	Hot Wallet	Exchange Wallet
• The private key to access cryptocurrency is stored on paper, not an electronic device • Most secure option from theft • More cumbersome for short term trading and most convenient for long-term holding	• The private key is stored on an internet connected device • Vulnerable to hacking • Best suited for smaller amounts of cryptocurrency	• Similar to a hot wallet, except the funds the funds are held by an exchange (e.g. Coinbase, Kraken, etc) • Vulnerable to hacking and subject to the security, or lack thereof, of the exchange • Convenient for trading

Sometimes cryptocurrency wallets can be so secure that the rightful owners are permanently locked out of their assets. Password keys, whether in a hot or cold wallet, can be lost. Given that cryptocurrency is decentralized, there is no bank or company to reset or recover the password. It is estimated that 20% of Bitcoin in circulation are in wallets where the password is lost or the assets otherwise unrecoverable.[19]

---

[17] Nahar, P. "What are 51% Attacks in Cryptocurrencies?," *The Economic Times*, August 31, 2021, https://economictimes.indiatimes.com/markets/cryptocurrency/what-are-51-attacks-in-cryptocurrencies/articleshow/85802504.cms?from=mdr, Accessed May 8, 2022.
[18] Conway, L. "What are the Safest Ways to Store Bitcoin?," *Investopedia,* February 28, 2021, https://www.investopedia.com/news/bitcoin-safe-storage-cold-wallet/, Accessed May 6, 2022.
[19] Popper, N. "Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes," *New York Times,* January 14, 2021, https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html, Accessed May 4, 2022.

On the other hand, as will be seen in the case studies below, the convenience of hot wallets and exchange wallets have led to the seizure of illegal funds. Hot wallets are especially convenient when making thousands of transactions and exchanges are excellent paths to reintegrating laundered funds back into cash.

While exchange wallets are convenient, the funds are held by the exchange itself. This leaves cryptocurrency holders subject to the risks of hackers as well as the decision-making of exchanges which may not be stringently regulated, as will be seen in the case study of Quadriga below.

3.4 The Role of Stablecoins

While cryptocurrencies are intended to be a form of currency and a medium of exchange, they have often been treated as speculative investment opportunities, leading to significant volatility. The value of cryptocurrencies is unpegged and decentralized allowing for much greater swings in price than with traditional currencies. Stablecoins are a subset of cryptocurrency that operate differently. A stablecoin is pegged to an underlying asset or formula, such as the US dollar.[20] In this sense, stablecoins are fundamentally different from other cryptocurrencies. Stablecoins have a central authority that holds an asset reserve or at least an asset ratio.[21] Many retail cryptocurrency traders use stablecoins to avoid fees when trading through cryptocurrency exchanges. This paper's section on the current regulatory landscape will evaluate the risks of unregulated stablecoins.

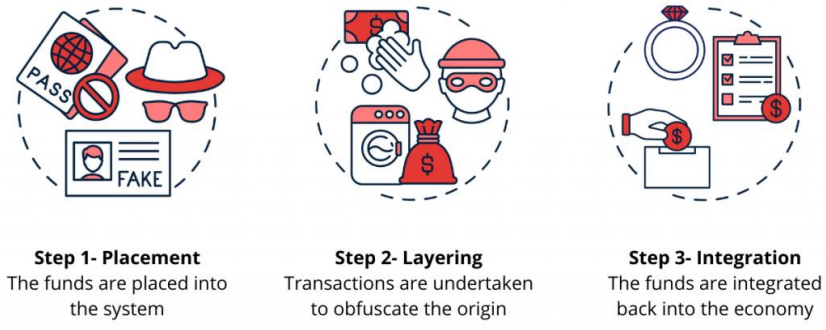
[20] Dossett, J. "What Are Stablecoins and Are They Less Risky? The Details Crypto Investors Should Know", *CNET*, May 31, 2022, https://www.cnet.com/personal-finance/crypto/what-are-stablecoins-and-are-they-less-risky-the-details-crypto-investors-should-know/, Accessed June 2, 2022.
[21] Ibid.

4.0 ASSET RECOVERY INVESTIGATIONS

4.1 Money Laundering Steps

While money laundering can take a variety of forms, there are three general phases[22]:

Figure 2[23]



1. Placement
    a. Can occur when fiat money (government-issued currency) is used to purchase cryptocurrency
    b. Additionally, ransomware demands request legitimate funds in cryptocurrency and quickly move to stage two, layering
2. Layering
    a. Steps taken to cover up the link to the illicit funds
    b. Often involves transferring funds to multiple accounts
    c. The decentralized nature of cryptocurrencies and variety of cryptocurrencies can allow a criminal actor to move the funds through many unregulated accounts/forums

[22] Kocegarovas, G. "Cryptocurrency money laundering risk: the best explanation of a 3-step process," *PSP Lab,* February 16, 2022, https://psplab.com/cryptocurrency-money-laundering-risk-a-3-step-process/#:~:text=If%20placement%20allows%20criminals%20to,transfers%20between%20different%20wallet%20addresses, Accessed May 4, 2022.
[23] Ibid.

3. Integration/Extraction
    a. Funds are reintroduced into the economy
    b. This can occur by converting cryptocurrency back to fiat money or by making purchases using cryptocurrency

During the placement and layering stages, illicit funds will be broken down into smaller amounts to make tracking more difficult and to avoid regulatory requirements.[24] At the layering stage, mixing can occur, whereby illicit fund transactions are combined with myriad irrelevant transactions to make tracing more challenging.[25] Section 5 will address specific means of layering and how IFAs can address these challenges.

The following case studies will demonstrate the opportunities and challenges for IFAs in attempting to recover stolen or laundered cryptocurrency assets.

4.2 Silk Road

As noted in the introduction, Silk Road represents one of the earliest prominent illegal uses of cryptocurrency as well as one of the earliest example of effective recovery of cryptocurrency assets by law enforcement. In 2011, Ross Ulbricht, using the alias Dread Pirate Roberts, founded the site Silk Road and acted as an escrow service to facilitate Bitcoin payments to buyers and sellers of narcotics.[26] At its height, Silk Road had over 13,000 listings for narcotics as well as listings for hacking services and murder for hire.[27]

[24] Liu, M. et al. "Detecting Roles of Money Laundering in Bitcoin Mixing Transactions: A Goal Modeling and Mining Framework," *Frontiers in Physics*, July 6, 2021. https://doi.org/10.3389/fphy.2021.665399, Accessed May 4, 2022.
[25] Ibid.
[26] Adler, 2018.
[27] Rooney, K. "Record $1 billion worth of bitcoin linked to the Silk Road seized by U.S. government," *CNBC,* November 6, 2020, https://www.cnbc.com/2020/11/05/1-billion-worth-of-bitcoin-linked-to-the-silk-road-seized-by-the-us.html#:~:text=The%20U.S.%20government%20seized%20an,the%20history%20of%20the%20agency., Accessed May 10, 2022.

United States law enforcement assembled an interagency task force involving the IRS, Department of Homeland Security, the FBI, the Drug Enforcement Agency and many other agencies. The collaborative effort took many forms, including the highlights below[28][29][30]:

Law Enforcement Actions	Description

Undercover Work	• The task force:
	  ○ set up accounts on Silk Road and engaged in transactions
	  ○ arrested those who transacted with them through Silk Road and obtained information about the workings of Silk Road
	• As an example, the task force created a screen name account named 'Nob' and used this account to build a relationship with Ulbricht. Nob convinced Ross to broker a transaction with a key site administrator who was then arrested by the task force.

Online Research	1. An IRS agent scoured internet forums and found Ulbticht's email on a post about an anonymous drug marketplace. Further research found multiple links between Ulbricht and Silk Road. 2. A cybercrime unit found a Reddit post explaining weaknesses in Silk Road's site security. Using this approach, agents were able to track down unencrypted IP addresses, including near Ulbricht's address in San Francisco. 3. Separate agencies gathered the information in points 1 and 2 and only when they shared information did they realize they had likely identified the site's founder and operator.
Sting Operation/Bitcoin Tracing	• The task force appropriated a moderator's account and while Ulbricht was at a public library and agents were present, they messaged Ulbricht to enter a sensitive area of the site. When he did, they arrested him and seized his laptop.

[28] Adler, 2018.
[29] Bearman J. and Hanuka, T. "The Rise and Fall of Silk Road," *Wired*, April and May 2015, https://www.wired.com/2015/04/silk-road-1/ and https://www.wired.com/2015/05/silk-road-2/, Accessed May 11, 2022.
[30] Greenberg, A. "Prosecutors Trace $13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop," *Wired*, January 29, 2015, https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/, Accessed May 12, 2022.

	• With the benefit of his laptop, they traced over 3,500 transactions of Bitcoin, proving that Ulbricht profited by $13.4 million in the year before his arrest.

The arrest and seizure of assets relied on the vast resources of US and international law enforcement bodies. Undercover work, a series of arrests leading to informants, online research and connecting information at disparate ends of the government contributed to a successful outcome for the government.

IFAs won't generally have the benefit of such resources or undercover work in order to trace laundered cryptocurrency assets. However, as will be further discussed in section 5 of this paper, when the public ledger of bitcoin is combined with other information, cryptocurrency investigators are able to gather a great deal of information. The permanence of the blockchain creates a complete record for investigators to follow. After the government seized the founder of Silk Road's assets and moved them into a single wallet, a researcher unaffiliated with the law enforcement effort were able to trace every transaction back to Silk Road, complete with a timestamp and value.[31] In another example of what can be accomplished without significant resources, a group of researchers made a total of 11 deposits or withdrawals and identified over 295,000 wallet addresses that had transacted on Silk Road.[32] Expertise in cryptocurrency tracing and computing can draw vast insight into the nature of transactions.

4.3 Quadriga

Although cryptocurrency exchanges can sometimes assist law enforcement proceedings when complying requests for information, the example of QuadrigaCX (Quadriga) demonstrates the risk of

[31] Weaver, N. "How I Traced 20% Of Ross Ulbricht's Biticoin To The Silk Road," *Forbes*, January 20, 2015, https://www.forbes.com/sites/frontline/2015/01/20/bitcoin-silk-road-ulbricht/?sh=712f96ec5637, Accessed June 2, 2022

[32] Greenberg, A. "Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market," *Forbes,* September 5, 2013, https://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/?sh=3d070482adf7, Accessed June 1, 2022.

entrusting largely unregulated cryptocurrency exchanges. In 2013, Gerald Cotton and Michael Patryn founded Quadriga as a Bitcoin exchange operating in Canada.[33] Quadriga struggled to raise funds and by 2016 Cotten was the sole owner/operator. The value of Bitcoin increased 30-fold in 2017 and in that year, $1.2 billion in Bitcoin was traded through Quadriga on a commission basis.[34] In 2018, as the price of Bitcoin plummeted, many customers could not withdraw their funds. By the end of the year, Quadriga announced that Cotten was dead. Shortly thereafter, his widow claimed that Cotten's laptop was encrypted, she did not have the password and only Cotten had control or access to Quadriga's cold storage system.[35] As noted earlier in this paper, cold storage is the most secure, but can run the risk of locking out the rightful owner. Bankruptcy proceedings followed thereafter, but the story of Quadriga does not end here.

While the Quadriga story has a great deal of intrigue and mystery worthy of documentaries, the focus on this paper is on asset recovery. Many of the case studies in this paper feature law enforcement proceedings attempting to follow a trail of transactions across various accounts and platforms and overcome jurisdictional obstacles. What makes Quadriga unique is that a reputable auditing firm, Ernst & Young, became bankruptcy trustee for Quadriga and the Ontario Securities Commission (OSC) conducted a thorough review which examined account data compelled from Ernst & Young. Rarely is the level of detail found in the Quadriga matter shared with the public. The OSC determined that 76,000 clients were owed a total of $215 million and Ernst & Young only recovered $46 million, leaving $169

[33] Bochan, T. "The Story Behind QuadrigaCX and Gerald Cotten, Netflix's 'Crypto King'," *CoinDesk*, March 29, 2022, https://www.coindesk.com/learn/the-story-behind-quadrigacx-and-gerald-cotten-netflixs-crypto-king/#:~:text=%22The%20downfall%20of%20crypto%20asset,those%20assets%20would%20be%20safeguarded, Accessed May 7, 2022.
[34] Castaldo, J. et al. "Crypto chaos: From Vancouver to Halifax, tracing the mystery of Quadriga's missing millions," *The Globe and Mail*, February 8, 2019, https://www.theglobeandmail.com/business/article-crypto-chaos-from-vancouver-to-halifax-tracing-the-mystery-of/, Accessed May 7, 2022.
[35] Bochan, 2022

million in unrecovered assets.[36] The OSC's report concluded that "Quadriga was an old-fashioned fraud wrapped in modern technology".[37]

The OSC summarized the lost assets as follows, showing that other than the $46 million recovered in the first row, the remainder of the funds were never recovered[38]:

Assets	Recovery Process
• $25 million frozen by CIBC • $6 million held by contractor • $600,000 held by payment processors • $12 million in assets held by widow	Sums recovered: • CIBC froze and assets in January 2018 due to dispute over ownership of funds • $6.6 million held by contractor/payment processors in course of business subsequent to Cotten's death • $12 million surrendered by widow given that the funds were given to her via Cotten's fraudulent dealings
$115 million in trading losses on Qaudriga	• Cotten created fake assets and accounts, giving the appearance to clients that sales/purchases of crypto assets had occurred. By the time bankruptcy proceedings began, these funds had been lost
$28 million in trading losses on external platforms	• Using deposits from Quadriga clients, Cotten moved assets to other trading platforms in his own name and lost this amount through trading
$2 million misappropriated to fund his lifestyle	• Cotten had misappropriated at least $24 million, but pre-bankruptcy, he returned $10 million to fund client withdrawals and $12 million was later surrendered by his widow (above)
$1 million in operating losses	• N/A
$23 million in additional trading losses, operating losses and misappropriation	• OSC had access to limited records and estimated that these sources accounted for further losses

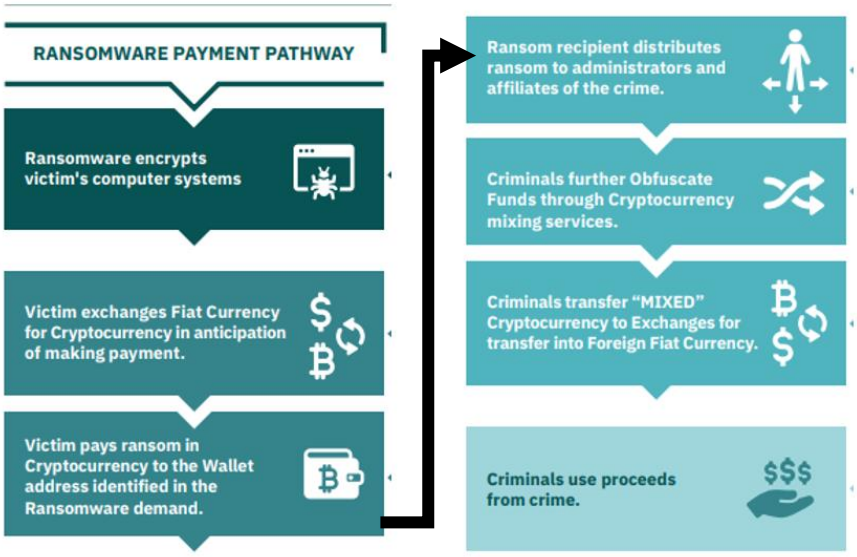
[36] Ontario Securities Commission, "QuadrigaCX: A Review by Staff of the Ontario Securities Commission," April 14, 2020, p3.
[37] Ibid, p4.
[38] Ibid, p25-27

Quadriga demonstrates the risks of cryptocurrency exchanges. Whereas Canadian banks have deposit insurance, cryptocurrency exchanges generally offer no equivalent protections. Investors take risks with the cryptocurrencies they choose and by placing their funds in exchanges as a leap of faith.

4.4 Colonial Pipeline

An increasingly popular method to illegally obtain large funds of cryptocurrency is ransomware.

Figure 3[39]



Hackers enter a legitimate business' computer system and hold their data ransom in exchange for large sums of cryptocurrency.[40] In 2021, Colonial Pipeline had to shut down over 5,000 miles of fuel pipeline due to a ransomware attack by Russian-based DarkSide, a criminal enterprise that develops ransomware tools and sells them to criminals.[41] Colonial Pipeline paid $4.4 million the hackers to have

[39] Institute for Security and Technology, "Combating Ransomware," *Ransomware Task Force,* 2021, p. 63.
[40] Macias, A. and Wilkie, C. "U.S. recovers $2.3 million in bitcoin paid in the Colonial Pipeline ransom," *CNBC*, June 7, 2021, https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html, Accessed June 6, 2022.
[41] Ibid.

their systems restored, and to the surprise of cryptocurrency experts, over half the funds were recovered by the US' Ransomware and Digital Task Force in short order.[42] Given the recency of this matter and that the criminal actors have not been arrested, full details are not available on the government's methods. However, certain aspects of the legal efforts have been disclosed[43][44]:

- Court records stated that a special agent identified the 75 bitcoins transferred to the hackers from Colonial Pipeline. Hackers moved the funds through at least six other wallets. The special agent noted that 64 bitcoins were transferred to another address.
- While initial reports claimed that the FBI had access to the encryption key linked to the Bitcoin account that received the 64 bitcoins, a review of the warrant showed the FBI seized the funds from the exchange holding the 64 bitcoins.
- Experts noted that a year's worth of surveillance on DarkSide may have led to search warrants that gave the government access to email accounts of participants.
- Alternatively, given DarkSide's business model, the layering of cryptocurrency may have been carried out by unsophisticated money launderers who did not understand the government's abilities to trace and seize funds.
- Although the remaining bitcoin were not recovered, investigators have identified the wallet that holds the funds, though the US is unable to seize those funds.

The FBI stated that even foreign-based criminals often use American infrastructure during the course of a crime, which allows the FBI a legal avenue to intervene and recover funds.[45] This case study

[42] Romo, V. "How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom," *NPR*, June 8, 2021 https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac, Accessed June 6, 2022.
[43] Romo, 2021.
[44] Uberti, D, "How the FBI Got Colonial Pipeline's Ransom Money Back," *Wall Street Journal*, June 11, 2021, https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981, Accessed June 7, 2022.
[45] Macias and Wilkie, 2021.

is a reminder of the importance of IFAs to know the regulations of local jurisdictions and any foreign jurisdiction through which funds travel in order to be able to leverage support through law enforcement or court orders.

Many cybercriminals have taken note of the FBI's success in recovering these funds. DarkSide accepts payment in Bitcoin, or a privacy coin named Monero (discussed further in section 5.3), but charge a 10-20% premium on payments received in Bitcoin, because of its traceability.[46] As expected, high profile law enforcement success stories will lead criminals to seek out more secretive ways to carry out illegal acts.

4.5 Glupteba Botnet

As described in Chainalysis's 2022 Crypto Crime Report, in 2021, Google discovered that Russian entities were using malware to use the computing power of devices to mine cryptocurrency, a practice known as cryptojacking.[47] Glupteba Botnet was also stealing and selling credit card information and account information from infiltrated Google servers. Botnets seek out servers infected with their malware and rely on command and control (C2) servers to send commands to infected servers. Law enforcement and cybersecurity firms will try to take down or disrupt C2 servers. As a result, botnets have algorithms to generate new domain addresses while commands are transferred to backup servers.

While highly technical, what makes Glupteba Botnet unique is that it encrypts special instructions on invalid Bitcoin transactions allowing it to find other servers. When under attack by law enforcement, the Glupteba Botnet searches the Bitcoin blockchain, which keeps a record of invalid transactions, for the instructions. These encrypted instructions are imprinted on a handful of small transactions that are scattered among daily transactions numbering in the hundreds of thousands.

[46] Murphy. H., "Monero emerges as crypto of choice for cybercriminals," *Financial Times*, June 22, 2021, https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6, Accessed June 12, 2022.
[47] This case study references Grauer, K. et al., 2022, p.65-68 unless noted otherwise.

While this builds an immensely resilient malware program, because of the public ledger, it does offer some clues that investigators can follow.

Google was able to identify several Glupteba Botnet invalid transactions. For the majority of transactions, the path of funds was as follows:

- Initial funds received from a mixing service
- Moved to Glupteba wallet
- Invalid transaction sends funds to refund wallet
- Which redirects funds to Glupteba wallet

Google provided the wallet addresses to Chainanlysis who decrypted the special instructions and found the new C2 server. Chainanlysis also identified one transaction where the funds initiated with a luxury office building in Moscow where a cybercriminal and cryptocurrency exchange operator had previously worked and had already been arrested by US authorities.

This case study demonstrates that while cybercriminals take extensive steps to layer funds and cover their tracks, it only takes one slip up or loose end for investigators to be able to track down those responsible.

4.6 Bitfinex Hack Recovery[48]

In 2016, two hackers stole 119,000 Bitcoins from the cryptocurrency exchange, Bitfinex by redirecting 2,000 transactions to a single wallet. The proceeds were worth $72 million at the time of theft and appreciated in value to $4.5 billion in 2022. For over a year, the funds sat untouched in the single wallet. In 2017, the hackers began routing funds through Alphabay, a dark web exchange for illicit goods. Once sent through this exchange, investigators could no longer tracker funds. However, Alphabay

[48] Chow, A. "Inside the Chess Match That Led the Fed to $3.6 Billion in Stolen Bitcoin," *Time*, February 10, 2022, https://time.com/6146749/cryptocurrency-laundering-bitfinex-hack/, Accessed June 10, 2022

was shut down by the US government later that year. Hackers then switched to another dark web marketplace, Hydra, and made small transactions.

In 2020, when the price of Bitcoin soared, the hackers began processing conjoin transactions through a Wasabi Wallet which prevents blockchain tracing. A Wasabi Wallet, which does not have KYC requirements, generates a new address for each transaction and can mask IP addresses.[49] As with many cryptocurrency money laundering investigations, law enforcement was likely able to combine several pieces of information to be able to trace the funds both backward and forward. The seizure of the Alphabay account likely gave the government an internal transaction record that they could tie back to the initial large wallet that held 119,000 bitcoins and then forward to other accounts to which the funds were transferred after Alphabay was shutdown or from the initial wallet.

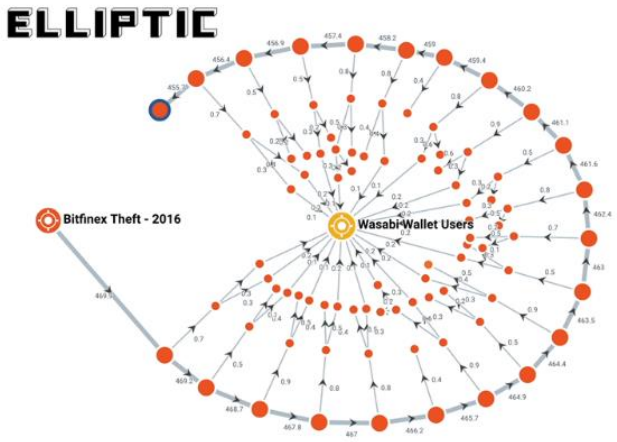
The government was able to determine that funds moved from shell accounts to the accounts of two associates in the scheme, Ilya Lichtenstein and Heather Morgan. Law enforcement obtained a search warrant for Lichtenstein's personal cloud storage, which contained wallet addresses with passwords. Authorities then logged into the account that held $3.6 billion and seized the funds, representing a seizure of 80% of the stolen funds recovered.

Government shutdown and seizure of dark web marketplace data provides a trove of information to investigators to link accounts to illicit activity. This case study also represents the effectiveness of increasing regulation. In 2017, money could have been laundered through cryptocurrency exchanges without KYC protocols and converted to fiat currency.[50] However, criminal

[49] The first three paragraphs cite the following, unless noted otherwise: Adegbe, L, "Wasabi Cryptocurrency Wallet Review," *Investopedia*, June 4, 2022, https://www.investopedia.com/wasabi-cryptocurrency-wallet-review-5271348, Accessed June 12, 2022.
[50] Robinson, T. "Elliptic Follows the $7 Billion in Bitcoin stolen from Bitfinex in 2016," *Elliptic*, May 13, 2021, https://www.elliptic.co/blog/elliptic-analysis-bitcoin-bitfinex-theft, Accessed June 12, 2022.

actors now require more elaborate means to launder funds. A forensic cryptocurrency firm, Elliptic, was able to track funds from the theft through dozens of addresses with automatic tracing techniques.[51]

Figure 4[52]



An investigation in Elliptic Forensics, tracing the stolen bitcoins through a peeling chain.

These case studies demonstrate that despite the obstacles, thoroughly researched investigations that follow the blockchain and combine other datapoints and use warrants to secure information can result in asset recovery.

[51] Ibid.
[52] Ibid.

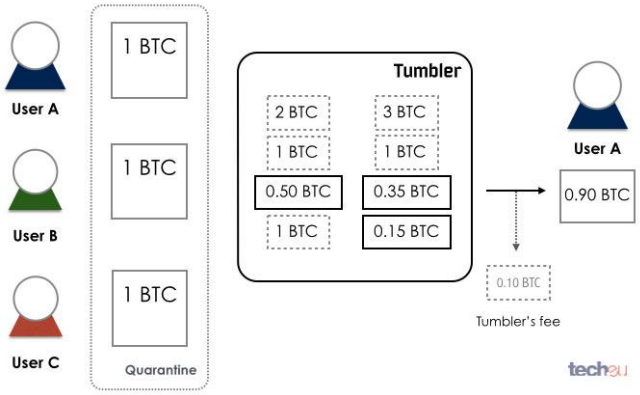
5.0 MONEY LAUNDERING METHODS AND INVESTIGATIVE CHALLENGES

This section will demonstrate the cat and mouse game between criminals and investigators, detailing money laundering methods and how these techniques can be investigated. There are countless methods criminal actors can employ and this paper will focus on the most commonly reported types.

5.1 Cryptocurrency Mixing

Criminal actors can secure the services of cryptocurrency mixers, also known as tumblers. These services will jumble amounts of cryptocurrencies in private pools and then distribute cryptocurrency back to the user, with a fee deducted. With a decentralized mixer, a large group of users can contribute an amount and then be redistributed the cryptocurrency of other users, without ever knowing whose funds they received.[53]

Figure 5[54]



[53] Stevens, R. "Bitcoin Mixers: How Do They Work and Why Are They Used?," *CoinDesk*, March 8, 2022, https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/, Accessed June 13, 2022.

[54] Deepwebsitelinks, "Top 10 Bitcoin Tumbler Services 2021,", Deepwebsitelinks, 2021, https://www.deepwebsiteslinks.com/bitcoin-tumbler-services/, Accessed June 13, 2022.

While cryptocurrency is anonymous from a personal identity perspective, a wallet address is very public. If an IFA is able to find a wallet address, tracing the cryptocurrency's steps forward or backward is possible, but may still be challenging. Those interested in hiding their activities may send cryptocurrency through channels where they are mixed and aggregated with non-illicit transactions.

In 2021, the IRS arrested Roman Sterlingov, who laundered over $300 million through the cryptocurrency mixing service Bitcoin Fog.[55] The investigation made use of undercover accounts, tracing Sterlingov's assets from a long defunct exchange and using a search warrant on Sterlingov's Google account.[56] A common theme is the need for investigators to comb through the blockchain record and combine different research to tie the funds to a particular individual.

Cryptocurrency mixing can be amplified by a process known as dusting. With dusting, a large number of small transactions are made to create a high volume of alerts with a cryptocurrency exchange, to overwhelm exchanges and obscure illicit transactions.[57] Chain peeling is a similar concept, whereby funds are moved to a large number of addresses, then moved into exchanges through dozens of transactions.[58] In 2018, hackers stole more than $13 million in Bitcoin, moved the funds through 70 wallet addresses, and then used 68 separate transactions to deposit the funds in a Russian-based cryptocurrency exchange.[59] As with many layering techniques, the goal is to create noise and obscure the movement of funds.

Government agencies and cybersecurity firms are developing software tools that can automatically trace a crypto fraud chain through various layering methods.[60] Moreover, regulators are

[55] Ravelli, R. "Arrest of Alleged Bitcoin Fog Operator Signals Continued DOJ Focus on Crypto "Mixers"," *Lexology*, May 18, 2021, https://www.lexology.com/library/detail.aspx?g=b46073d7-0731-42d2-b319-270bd0c17c6e, Accessed June 4, 2022.
[56] Ravelli, 2021.
[57] ComplyAdvantage, "A Guide to Anti-Money Laundering for Crypto Firms," *ComplyAdvantage*, 2022, p.14.
[58] Carlisle, D., "Preventing Financial Crime in Cryptoassets," *Elliptic,* 2022, p.89.
[59] Ibid, p.90
[60] Chow, 2022.

also exerting pressure over cryptocurrency entities with privacy features that may facilitate money laundering. As noted earlier, Wasabi Wallets are another form of blockchain obfuscation. Wasabi Wallet has announced it start preventing certain users, individuals already subject to government sanctions, from using its services.[61] The decision was announced soon after the U.K.'s National Crime Agency announced its intention to regulate Wasabi Wallet's services given the way it can be exploited by criminals.[62] Regulatory pressure can have as much an influence as new laws or rules.

5.2 Cryptocurrency Exchanges

One of the most promising avenues for any law enforcement proceeding is to subpoena or summons (depending on the jurisdiction) information from a cryptocurrency exchange. In United States v. Gratkowski, related to a child pornography trafficker, a federal court accepted evidence obtained through a subpoena to Coinbase.[63] The court held that there is no constitutional privacy right with bitcoin transactions because such a transaction is "affirmative act and that users are unlikely to expect any privacy related to the information published on the blockchain."[64] The means of law enforcement bodies to obtain information from exchanges is likely to increase in the future, both through regulatory schemes and court orders. While the focus of this paper is on money launderers, even investors who fail to declare capital gains will be ensnared in the government's movement toward greater transparency from exchanges. In 2021, a federal court authorized the IRS to serve a 'John Doe summons' to Kraken to obtain information about any US taxpayers who conducted at least $20,000 in transactions over the previous five years.

---

[61] Namcios, "Wasabi Wallet Parent Company Explains Decision To Censor Bitcoin Transactions," *Bitcoin Magazine,* March 28, 2022, https://bitcoinmagazine.com/business/wasabi-wallet-explains-new-bitcoin-censorship, Accessed June 17, 2022.
[62] Ibid.
[63] Montgomery, J. "Bare Bitcoins — No Fourth Amendment Privacy in Virtual Currency Records," Freeman Law, 2021, https://freemanlaw.com/bare-bitcoins-no-fourth-amendment-privacy-in-virtual-currency-records/, Accessed June 5, 2022.
[64] Ibid.

Exchanges can generally be classified in three ways[65]:

Type of Cryptocurrency Exchange	Main Features
Regulated Exchange	• High liquidity and able to handle large volume of transactions • Subject t AML/KYC requirements
Minimally Regulated Exchange	• Located in laxer jurisdiction • Few controls to identify illicit funds • May directly with dark web entities or unregulated exchanges used by dark web entities
Peer to Peer Exchange	• Freely available software allows users anywhere to make direct transactions • No oversight or central body holding funds

For many years, exchanges have been exploited by fraudsters. A Reuters investigation found that between 2017 and 2021, Binance, one of the largest cryptocurrency exchanges, accepted over $2.35 billion in funds generated from crime.[66] It was only by August 2021 that Binance required all new and existing customers to provide identification to Binance, and in the months that followed the flow of illicit funds dropped significantly.[67] As will be discussed further in section 6, many countries have imposed KYC requirements on cryptocurrency exchanges.

Although law enforcement can take advantage of such means of obtaining information, criminals continue to go to lengths to evade detection. Criminals can engage in chain-hopping whereby criminals use bought or stolen accounts and move their money through various exchanges, exploiting

[65] Institute for Security and Technology, 2021, p. 67.
[66] Berwick, A. and Wilson, T. "How crypto giant Binance became a hub for hackers, fraudsters and drug traffickers," *Reuters*, June 6, 2022, https://www.reuters.com/investigates/special-report/fintech-crypto-binance-dirtymoney/?utm_source=Sailthru&utm_medium=newsletter&utm_campaign=daily-briefing&utm_term=06-06-2022, Accessed June 14, 2022.
[67] Ibid.

the time-consuming process for investigators to track and freeze assets.[68] Some exchanges have prohibited transactions with known mixers, though criminals can simply utilize other exchanges.[69] Given the public nature of the blockchain ledger, investigators can still track assets through chain-hopping, but it becomes a more onerous process.

Criminal actors may seek out 'off-chain' networks where KYC requirements aren't in place. It is also possible to engage in transactions that do not get recorded on the public ledger.[70] Some networks can use an overlay network to allow direct exchanges between two individuals, thereby eliminating a record of the transaction.[71] Law enforcement and forensic investigative firms continue to seek out new tools to overcome criminal methods of laundering funds.

5.3 Privacy Coins

Although Bitcoin has the largest market capitalization of any cryptocurrency, there is a subset of cryptocurrency called privacy coins. Privacy coins are "cryptocurrencies that obscure transactions on their blockchain to maintain the anonymity of its users and their activity."[72] Ordinary cryptocurrencies can maintain the anonymity of their users (though not their wallet address), but make transactions public. Privacy coins take anonymity a step farther by keeping transaction records secret. The following are examples of prominent privacy coins:[73]

Zcash	Monero
• Validates transactions between two parties • Public ledger will show only that a transaction occurred at a certain time	• Uses stealth addresses/one-time public keys ○ Can't be linked to other wallets used; essentially breaks the chain

[68] Stevens, 2022.
[69] Ibid.
[70] ComplyAdvantage, 2022, p.14.
[71] Ibid.
[72] Kim, P. "Privacy coins are cryptocurrencies that can be traded anonymously," *Business Insider*, February 10, 2022, https://www.businessinsider.com/personal-finance/privacy-coins, Accessed June 7, 2022.
[73] Ibid.

• Ledger does not show:
  ○ Who participated
  ○ Amount of transaction
	• Ring signatures mix identities with other decoy identities so that no one can decipher the true identity
	• Obscures transaction amounts as well

Some dark web and ransomware groups are moving away from Bitcoin and toward privacy coins like Monero. REvil, a Russian-linked cyberhacking organization now only accepts ransom payments in Monero.[74] It is estimated that 50% of online ransom payments are now made in Monero.[75] One barrier that inhibits further uptake of Monero and other privacy coins by criminals is that they have lower market capitalizations and thus are less liquid than Bitcoin.[76]

Given the ease of use of privacy coins for criminals, governments can approach privacy coins in three ways:

- Pressure cryptocurrency exchanges to stop its users from trading with privacy coins
  - In 2021, Bittrex announced it would delist Monero and Zcash.[77] It is likely that KYC and anti-money laundering (AML) requirements imposed by many countries make it challenging for exchanges to be compliant with privacy coin users.
  - Australia and South Korea have banned exchanges from offering privacy coins.[78]
- Regulate privacy coins
  - The US Secret Services has been advocating since 2018 that the US regulate and combat privacy coins given their use in criminal activities.[79]

[74] Murphy, 2021.
[75] Ibid.
[76] Institute for Security and Technology, p. 14.
[77] Reynolds, K. "Bittrex to Delist 'Privacy Coins' Monero, Dash and Zcash," *CoinDesk*, January 1, 2021, https://www.coindesk.com/markets/2021/01/01/bittrex-to-delist-privacy-coins-monero-dash-and-zcash/, Accessed June 8, 2022.
[78] Stevens, R. "What Are Privacy Coins and Are They Legal?," *CoinDesk,* January 10, 2022, https://www.coindesk.com/learn/what-are-privacy-coins-and-are-they-legal/, Accessed June 8, 2022
[79] Reynolds, 2021.

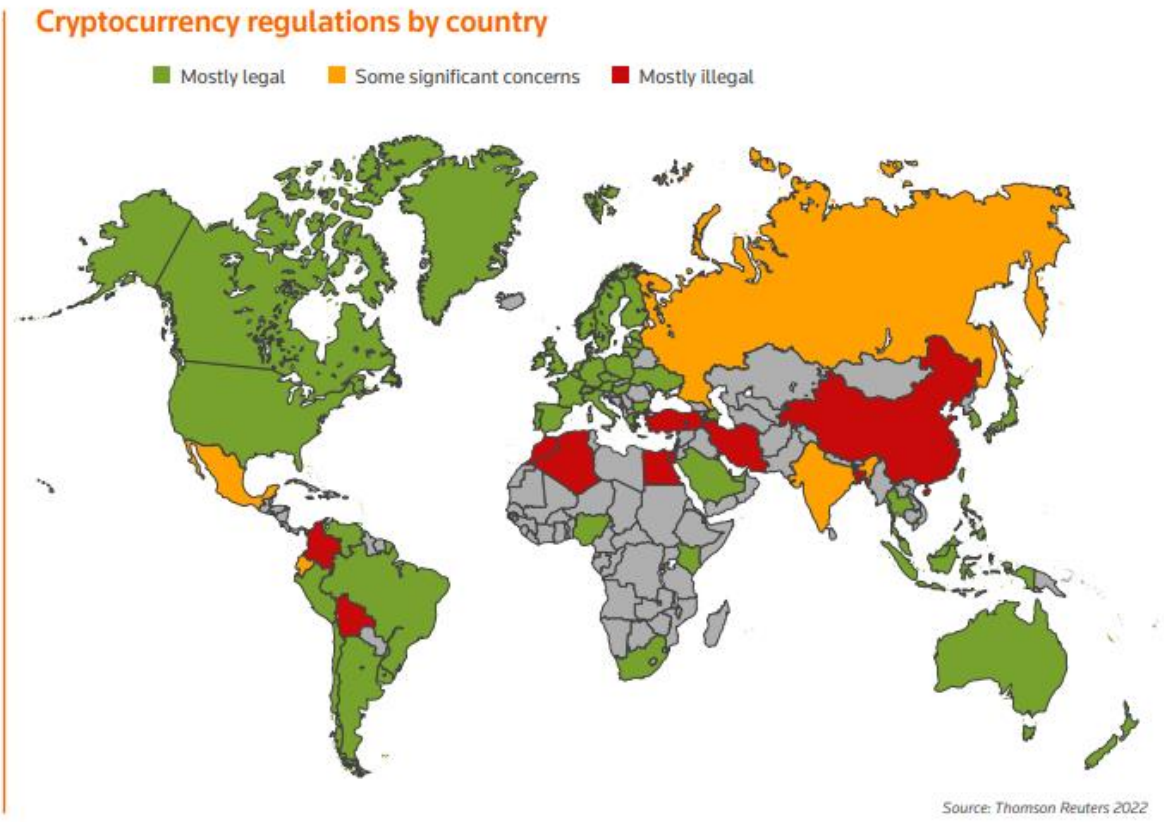
- Build technology to crack the privacy
    - CipherTrace has been working on behalf of the Department of Homeland Security to develop probabilistic and tracing methods to track monero transactions.[80]

6.0 CURRENT REGULATORY LANDSCAPE

A significant challenge for any IFA investigating cryptocurrency is being aware of the global regulatory patchwork that currently exists. In a matter of minutes, funds can move through exchanges operated in myriad countries. IFAs need to know which countries may offer legal resources to allow the IFA to obtain information or seize funds.

[80] CipherTrace, "CipherTrace Files Two Monero Cryptocurrency Tracing Patents," CipherTrace, November 20, 2020, https://ciphertrace.com/ciphertrace-files-two-monero-cryptocurrency-tracing-patents/, Accessed June 9, 2022.

Figure 6[81]



Governments have had centuries to regulate banks, enacting and amending laws. Banks processed government issued currencies, existed in physical currency and were tracked through banking records. Even so, money laundering and financial crime persist for various reasons. Jurisdictions with weak regulatory regimes can be used for tax evasion, as seen with the Panama Papers affair. A recent B.C. report on money laundering revealed that over $1 billion in illicit cash was laundered through casinos, due to lax enforcement and a lack of a dedicated enforcement agency.[82] Criminals will always

[81] Hammond, S. and Ehret, T., "Cryptocurrency regulations by country," *Thomson Reuters*, April 2022, https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf, p.2

[82] Cooper, S. "Federal 'failures' on money laundering prompt B.C. inquiry to call for provincial watchdog," *Global News,* June 15, 2022, https://globalnews.ca/news/8922745/cullen-commission-findings-report-bc-money-laundering-inquiry/, Accessed June 16, 2022.

be motivated to evade legal regimes. Given the technological innovations of cryptocurrencies, simply attempting to replicate banking requirements on cryptocurrency exchanges would be an imperfect solution, though it may be a worthwhile starting point.

Cryptocurrency is a 21st century phenomenon and poses even greater jurisdictional and technological challenges to regulators. While many governments were relatively lax and slow to respond to the emergence of cryptocurrency, there is an increased sense of urgency, both given the ease with which criminals can move assets and the potential harms to legitimate investors and holders of cryptocurrencies. Parts of the legal framework described in this section may well be out of date in five years' time.

6.1 U.S.

Given the broad international investigative reach of the US and its global financial dominance, it is appropriate to review the US legal framework vis-à-vis cryptocurrency. Even within a country, regulatory agencies may differ in their interpretations, as they attempt to fit cryptocurrency into their purview. The following is a list of agencies and their general view on cryptocurrency[83]:

- Securities and Exchange Commission (SEC): mostly views cryptocurrency as securities
- Commodity Futures Trading Commission (CFTC): refers to bitcoin as a commodity
- U.S. Treasury: mostly views cryptocurrency as currency

The President has issued an Executive Order directing agencies to coordinate their cryptocurrency regulatory efforts.[84]

Given that cryptocurrencies are decentralized, for cryptocurrency regulation to be effective, jurisdictions need to have authority over a centralized organization. As such, regulation of

[83] Hammond, S. and Ehret, T., 2022, p.5.
[84] Ibid, p.5.

cryptocurrency exchanges is equally important. In 2013, the Financial Crimes Enforcement Network (FinCEN), a branch of the U.S. Treasury, issued guidance that cryptocurrency exchanges are money transmitters and therefore fall within the scop of the *Bank Secrecy Act* (BSA) of 1970.[85] As such, exchanges must have in place AML/KYC frameworks in order to be compliant with the BSA.[86]

The U.S.' ad hoc approach to regulating different facets of cryptocurrency creates uncertainty for all involved. The example of BlockFi shows how the U.S. government can be slow to react, allowing cryptocurrency-related businesses to develop a market foothold without regulatory oversight. Since 2019, BlockFi, a U.S. based financial institution had been offering users a chance to lend digital assets to BlockFi in exchange for future interest, sometimes as high as 9%.[87] It was not until 3 years later that the SEC charged BlockFi with failing to register with the *Investment Company Act* (ICA) of 1940 or comply with the Securities Act of 1933.[88] The U.S. has been tentative and unclear in the application of decades old banking/securities laws to cryptocurrency, which allows cryptocurrency companies to lure in clients without strict oversight. While BlockFi agreed to settle the matter by paying a $100 million fine, they also have the benefit of an existing customer base and agreement from the U.S. that they can register under the aforementioned acts and continue offering their services.[89] This case study shows the challenges the U.S. faces without cryptocurrency-specific laws, leaving it with piecemeal enforcement and individual negotiations with possibly offending organizations.

[85] ComplyAdvantage, "Cryptocurrency Regulations Around The World," *ComplyAdvantage,* June 10, 2022, https://complyadvantage.com/insights/cryptocurrencyregulationsaroundworld/#:~:text=Cryptocurrency%20exchanges%20are%20legal%20in,submit%20reports%20to%20the%20authorities, Accessed June 13, 2022.
[86] ComplyAdvantage, 2022, p.6.
[87] Flitter, E. "BlockFi, a crypto firm, reaches a $100 million settlement for failing to register loan products," *New York Times,* February 14, 2022, https://www.nytimes.com/2022/02/14/business/blockfi-sec-crypto-loans.html, Accessed June 13, 2022.
[88] SEC, "BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of its Crypto Lending Product," *SEC*, February 14, 2022, https://www.sec.gov/news/press-release/2022-26, Accessed June 13, 2022.
[89] Flitter, E., 2022.

6.2 Canada

Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) regulates exchanges based in Canada or not based in Canada but transacting with Canadian clients.[90] Canada takes the position that cryptocurrency businesses or dealers are money service businesses and regulates them as such.[91] The PCMLTFA and its regulations impose AML/KYC requirements, record-keeping requirements, reporting of suspicious transactions and enhanced record-keeping requirements for transactions greater than $10,000.[92]

Although securities laws in Canada are provincial jurisdiction, the Canadian Securities Administrators (CSA), comprised of provincial regulators, has been instrumental in harmonising Canadian treatment of cryptocurrencies primarily as securities.[93] The CSA directs provinces to impose greater restrictions on cryptocurrency exchanges that hold funds internally (the exchange is the true holder, as with Quadriga), as opposed to where funds are an "immediate delivery" asset held by clients.[94]

Since 2021, Canada imposed the travel rule on a variety of financial entities and businesses (FEB) specific to cryptocurrencies.[95] FEBs "must include the travel rule information when they send VC transfers, and must take reasonable measures to ensure that this information is included when they

[90] ComplyAdvantage, 2022, p.6-7.
[91] Anne-Bloom, C. et al., "Cryptocurrency Businesses Are Becoming A FINTRAC Reporting Entity," *MNP*, April 27, 2020, https://www.mnp.ca/en/insights/directory/cryptocurrency-businesses-are-becoming-a-fintrac-reporting-entity, Accessed June 5, 2022.
[92] ComplyAdvantage, 2022, p.6-7.
[93] Grant, S. et al., "Blockchain & Cryptocurrency Laws and Regulations 2022: Canada," *Global Legal Insight,* 2022, https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/canada, Accessed June 11, 2022.
[94] Ibid.
[95] Government of Canada, "Travel rule for electronic funds and virtual currency transfers," *Government of Canada,* April 22, 2022, https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/travel-acheminement/1-eng, Accessed June 10, 2022.

receive VC transfers which require a VC record to be kept".[96] Given the automatic and final nature of cryptocurrency transactions, the travel rule recognizes that FEBs may not always have the required information every time funds are received; however, FEBs are required to make inquiries and have risk-management policies that address when transactions should be suspended.

6.3 International bodies: Financial Action Task Force (FATF) and European Union (EU)

The FATF is an international body made up of 38 member states, ranging from the G7 countries to Russia and Saudi Arabia, dedicated to combating money laundering and terrorism financing.[97] The FATF publishes standards and recommendations and regularly revises their guidance. Recommendation 15 and its interpretive note specifically addresses cryptocurrencies, which it refers to as virtual assets.[98] The FATF directs countries to apply relevant FATF guidance applicable to traditional financial institutions to virtual assets and virtual asset service providers (VASPs), which encompasses exchanges. The FATF provides the following guidance:

Area	Guidance
VASPs/Exchanges	• Require VASPs/Exchanges to be licensed or registered, at a minimum in the jurisdiction where they are created • Do not allow known criminals to be beneficial owners of VASPs
AML protocols	• VASPs must adopt AML protocols and have a competent oversight authority that is not a self-regulating body • Such bodies must be able to impose requirements, compel VASPs to produce information in its possession and sanction VASPs when warranted

[96] Ibid.
[97] FATF, "Who we are," *FATF,* 2022, https://www.fatf-gafi.org/about/, Accessed June 11, 2022.
[98] FATF, "International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation," *FATF*, 2022, p.17 and 76-77

International Cooperation	• Rapidly work with other countries to facilitate the exchange of information across countries when required by law enforcement
Application of general FATF recommendations	• VASPs should comply with similar requirements imposed on banks/financial institutions, including but not limited to: o Record-Keeping o Customer due diligence o Internal controls and controls over subsidiaries o Reporting of suspicious transactions

The FATF proposes sensible regulations that would provide greater security and stability, many countries are struggling to enact comprehensive and cohesive frameworks, such as the U.S. New legislation or bolder interpretation from existing regulatory agencies may be needed to make FATF recommendations a reality throughout the world.

In 2018, the EU issued the 5th Anti-Money Laundering Directive (the Directive), which endorsed FATF standards and directed countries to adopt more specific, harmonised standards.[99] The Directive identified cryptocurrency exchanges as 'obliged entities' who must put in place AML protocols and report to competent authorities.[100] Moreover, the Directive identified enhanced due diligence steps required when obligated entities transact with 'high-risk' countries and encourage cooperation among regulators.[101] While the Directive, once implemented into law by individual countries, will provide greater operational clarity to cryptocurrency exchanges, as of 2022, only 70% of EU countries have fully enacted

[99] European Union, "Directive (Eu) 2018/843 Of The European Parliament And Of The Council Of 30 May 2018," *Official Journal of the European Union*, May 30, 2018.
[100] Ibid, p.2.
[101] Ibid, p.3 and 9.

6.4 Switzerland

The Swiss regulatory model presents a clearer and more favourable framework for cryptocurrency-related entities. In 2018, the Swiss Federal Council published a report that concluded while Switzerland's existing legal framework could adequately regulate cryptocurrency, the report recommended laws specific to cryptocurrency.[102] By 2022, Switzerland passed the *Law on Distributed Ledger Technology* (DLT Law), which explicitly addresses when a cryptocurrency becomes a security instrument.[103] The Swiss Financial Market Supervisory Authority (FINMA) has licensing requirements for all forms of cryptocurrency firms and have risk management policies, which should include circumstances under which transactions could be suspended or rejected.[104]

The DLT has created an environment favourable to cryptocurrency innovation through clear laws and provides investor protection. Under the DLT law, if a cryptocurrency custodian, such as an exchange, goes bankrupt, digital assets are allocated to clients, rather than forming part of the bankruptcy estate.[105] The purpose of regulation is to ensure clients and users can have safeguards.

The example of Ripple Labs (Ripple), a U.S. based company that has created the XRP token, is an example of the benefits of regulatory clarity. In determining whether a cryptocurrency is a security, Switzerland considers the functionality of the digital asset.[106] Where the digital asset is limited to payments and does not have voting rights, it would be unlikely to be classified as a security; instead, it would likely be classified as a utility token.[107] Meanwhile, in 2020, the U.S. charged Ripple with violating

[102] Haeberli, D. et al., "Blockchain & Cryptocurrency Laws and Regulations 2022: Switzerland," *Global Legal Insights,* 2022, https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/switzerland, Accessed June 10, 2022.
[103] Ibid.
[104] Ibid.
[105] Hurry, S. et al., "New tech act in Switzerland secures legal environment, allows blockchain to flourish," *IMD*, February 2021, https://www.imd.org/news/updates/new-tech-act-Switzerland-secures-legal-environment-blockchain-flourish/, Accessed June 5, 2022.
[106] Hurry, S. et al., 2022.
[107] Ibid.

the *Securities Act* by illegal selling $1.38 billion in digital money to investors.[108] The SEC argues that Ripple is structured like a stock trade in that purchasers get a stake in Ripple, whereas Ripple argues it is a currency and should be treated like a currency or commodity.[109] While Ripple's treatment as a security or commodity

6.5 Stablecoins

Stablecoins warrant their own section on regulation. Although stablecoins may not appear as directly connected to money laundering, the FATF has identified that stablecoins have the same allure for money launderers as other cryptocurrencies, namely anonymity, widespread global adoption and layering.[110] Cryptocurrencies like Bitcoin and Ethereum are often attractive to ordinary users for investment purposes. As their name suggests, stablecoins are intended to provide stability, however, a review of Terra Luna and other stablecoins will reveal the lack of existing regulatory oversight.

TerraUSD (UST) was pegged to the US dollar, while its sister coin Luna was the backing asset and able to absorb volatility.[111] At their safest, stablecoins can be fully-backed by the assets they are pegged to at a 1:1 ratio. If a stablecoin pegged to the US dollar had 1 million stablecoins, it could have $1 million in US dollars to ensure stability. The Terra Luna approach was instead an algorithmic stablecoin, which uses an algorithm to either reduce or increase supply to ensure the price of the stablecoin matches its peg.[112]

---

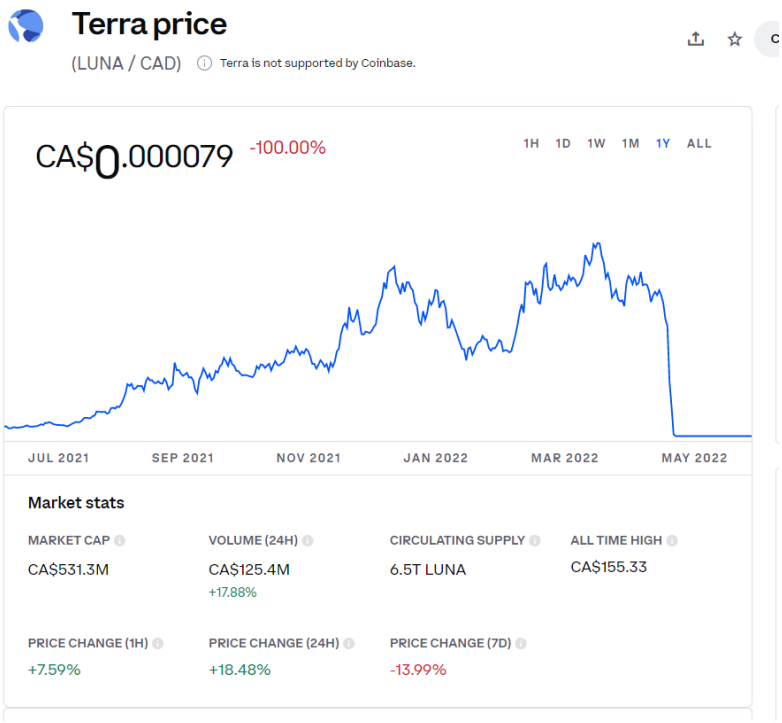
[108] Lipton, E. "As Scrutiny of Cryptocurrency Grows, the Industry Turns to K Street," *New York Times,* November 1, 2021, https://www.nytimes.com/2021/05/09/us/politics/cryptocurrency-regulation-sec-ripple-labs.html, Accessed June 16, 2022.
[109] Ibid.
[110] FATF, "FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins," *FATF*, June 2020, p.6.
[111] Davies, P., "Terra Luna stablecoin collapse explained: Is this the 2008 financial crash moment of cryptocurrency?," *EuroNews*, May 12, 2022, https://www.euronews.com/next/2022/05/12/terra-luna-stablecoin-collapse-is-this-the-2008-financial-crash-moment-of-cryptocurrency, Accessed June 1, 2022.
[112] Cryptopedia, "What are Stablecoins?," *Cryptopedia*, May 10, 2022, https://www.gemini.com/cryptopedia/what-are-stablecoins-how-do-they-work#section-algorithmic-stablecoins, Accessed June 2, 2022.

The downfall of UST and Luna is complex and involves many interrelated flaws that appear hard to sustain together, particularly in challenging times:[113]

- By design, creating UST burned (destroyed) Luna, which would make the value of remaining Luna more valuable;
- To entice users to burn Luna, UST's creators offered a 20% return (the Anchor Protocol), an impossible rate to sustain, particularly in the event of a cryptocurrency downturn;
    - 70% of UST's supply was deposited in this process, then worth $14 billion
- Beyond the algorithm, UST had $2.3 billion in reserve and ready to be sold if needed;
- As interest rates went up, cryptocurrency markets went down;
- On May 7, 2022, $2 billion worth of UST was taken out of the Anchor Protocol and UST fell to 91 cents. It is unclear if this was caused by investor panic or a hacker;
- In less than 3 weeks, UST's value dropped below 20 cents, Luna dropped from $82.55 to $0.01 and over $17 billion in supposedly stable assets had been erased.

[113] Van Boom, D., "Luna Crypto Crash: How UST Broke and What's Next for Terra," *CNET,* May 25, 2022, https://www.cnet.com/personal-finance/crypto/luna-crypto-crash-how-ust-broke-and-whats-next-for-terra/, Accessed June 11, 2022.

Figure 7[114]



Tether is a more traditionally structured asset-backed stablecoin, or so Tether would lead the public to believe. Tether is owned by the same corporate entity that owns Bitfinex, a cryptocurrency exchange. The New York state Attorney General uncovered that Bitfinex moved $850 million to a Panamanian cryptocurrency company and exposed Tether to this risky debt, meaning that Tether was not fully asset-backed as it claimed.[115] The matter was settled with Bitfinex and Tether agreeing to the following[116]:

- Stop trading activity with New Yorkers;

[114] CoinBase, "Luna Price," *CoinBase*, June 19, 2022, https://www.coinbase.com/price/terra-luna, Accessed June 19, 2022.
[115] Browne, R. "Cryptocurrency firms Tether and Bitfinex agree to pay $18.5 million fine to end New York probe," *CNBC,* February 23, 2021, https://www.cnbc.com/2021/02/23/tether-bitfinex-reach-settlement-with-new-york-attorney-general.html, Accessed June 12, 2022.
[116] Atkins, J. "Tether, Bitfinex prohibited from operating in New York, pays $18.5M settlement in NYAG case," *CoinGeek* February 23, 2021, https://coingeek.com/tether-bitfinex-prohibited-from-operating-in-new-york-pays-18-5m-settlement-in-nyag-case/, Accessed June 12, 2022.

- Pay an $18.5 million settlement;
- Provide quarterly reports to the Attorney General showing proper segregation of corporate and client accounts; and
- Public disclosures regarding its backing.

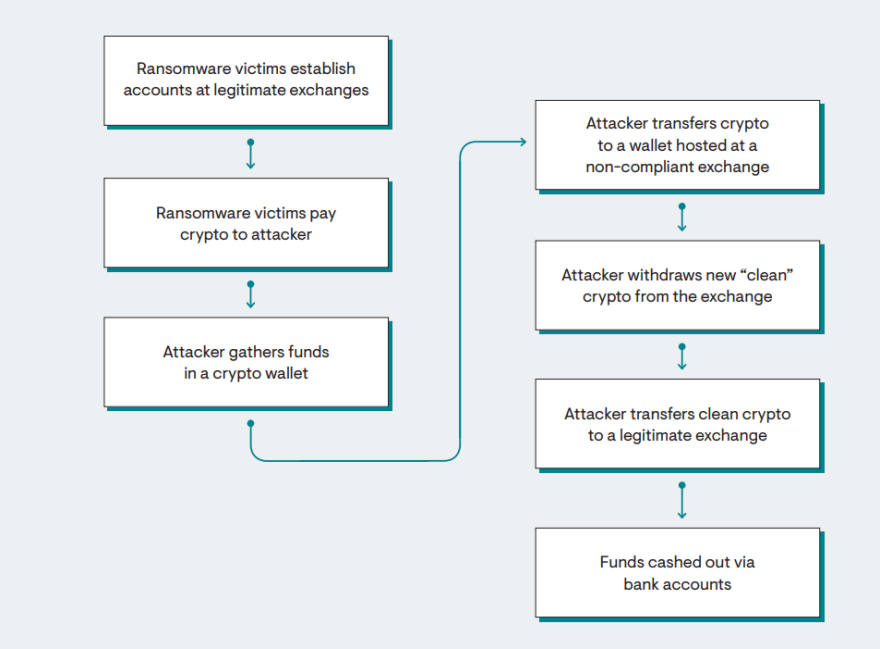
While independent audits would be an ideal solution, public disclosure creates an expectation of transparency and allows investors to evaluate claims made by otherwise opaque financial entities. Stablecoins may not seem like the main target of criminal actors, but for the cryptocurrency ecosystem to be a functioning, predictable and lawful environment, stablecoin regulation and oversight is needed.

6.6 Unregulated Exchanges

No matter their size, unregulated or loosely regulated exchanges pose significant problems for law enforcement bodies. In some instances, these unregulated exchanges may largely exist to facilitate money laundering. In 2021, the U.S. Treasury's Office of Foreign Assets Control (OAFC), imposed sanctions on two exchanges owner by the same entity, SUEX, an exchange registered Czech Republic, and Chatex, an exchange registered in St. Vincent and the Grenadines.[117] Both exchanges were found to have processed hundreds of millions in funds for illicit activities, such as ransomware orchestrated by Russian entities, allowing the funds to move to larger exchanges and into fiat currency.[118]

[117] Carlisle, 2022, p. 14.
[118] Ibid. and Chainanalysis, "Chainalysis in Action: OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over $160 million from Ransomware Attackers, Scammers, and Darknet Markets," *Chainanalysis,* September 22, 2021 https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021/, Accessed June 13, 2022.

Figure 8[119]



One of the key impacts of the sanctions is to prohibit any other exchanges from doing transacting with these sanctioned exchanges.[120] As a result, illicit actors relying on SUEX and Chatex would not be able to reach stage three of the money laundering process, reintegration into the economy. Unregulated exchanges will never go away entirely, but they can be blacklisted and therefore a much less practical tool for criminal actors.

[119] Carlisle, D., 2022, p.13.
[120] Ibid, p.14.

7. REGULATORY RECOMMENDATIONS

One challenge facing government is how to impose regulatory regimes that will achieve the greatest level of cooperation. Treasury Secretary Janet Yellen stated ""We have a strong interest in ensuring that innovation does not lead to a fragmentation in international payment architectures."[121] This statement acknowledges that blockchain technology has the potential to enhance economic output, for instance, through the use of smart contracts. A good regulatory regime will encourage innovation by providing clarity to legitimate ventures and create a broad framework for a variety of participants from exchanges to token creators to lending institutions. Creating a clear regulatory framework essentially builds partnerships with businesses who are then obligated to police the users of their services. Innovation cannot require or result in a zone of lawlessness. As this paper has shown, dark web markets proliferate, some are shut down and others spring up replace them. An effective regulatory regime will need to provide robust enforcement powers to pursue illicit actors.

7.1 Proactive Enforcement of Existing Regulations

Comprehensive legislation from G7 countries will take time. In the meantime, regulators need to coherently use the tools they have now. Far too often regulators have been tentative or vague and allowed cryptocurrency entities to grow in size prior to intervening, posing risks to clients. The OSC report on Quadriga states:

> Quadriga did not consider its business to involve securities trading and it did not register with any securities regulator. This lack of registration facilitated Cotten's ability to commit a large-scale fraud without detection.[122]

[121] Hussein, Fatima, "Treasury Secretary Yellen calls for cryptocurrency regulation to reduce risk, fraud," *PBS*, April 7, 2022, https://www.pbs.org/newshour/economy/treasury-secretary-yellen-calls-for-cryptocurrency-regulation-to-reduce-risk-fraud, Accessed June 5, 2022.
[122] OSC, 2020, p. 4.

The above phrasing is passively worded and does not capture the regulator's role. It would be just as accurate to state "Existing securities regulations could have been applied to Quadriga and stopped a large-scale fraud before Quadriga took possession of $100+ million of ordinary investors' money. Instead, regulators waited until Quadriga went broke to declare Quadriga was not compliant with existing laws".

One think tank has argued that U.S. regulators already have the powers to regulate cryptocurrency entities and that lax enforcement may create the impression that stronger regulations are unnecessary.[123] For instance, courts have ruled that crypto assets like Bitcoin are commodities and the *Commodity Exchange Act* gives the CFTC broad powers to sanction entities that manipulate or provide false information regarding markets for commodities.[124] SEC Chair Gary Gensler has said that the top five exchanges, which account for almost all trading, "likely are trading securities" and should be regulated by the SEC.[125] Regulatory agencies need to make the most of their powers to ensure cryptocurrency entities, such as exchanges, deter fraud and gather the information needed to assist law enforcement investigations. Regulators must walk a fine line between calling for better legislation and claiming existing legislation is not adequately enforceable.

7.2 Dedicated Cryptocurrency Legislation

Regulators across the world are increasing their enforcement efforts, but the problem is twofold. For one, these efforts are inadequate. In May 2022, the SEC announced it would double the

[123] Phillips, T. and Thornton, A., "Congress Must Not Provide Statutory Carveouts for Crypto Assets," *Center for American Progress,* March 1, 2022, https://www.americanprogress.org/article/congress-must-not-provide-statutory-carveouts-for-crypto-assets/, Accessed June 17, 2022.
[124] Ibid.
[125] Sharma, R., "How SEC Regs Will Change Cryptocurrency Markets," *Investopedia,* June 7, 2022, https://www.investopedia.com/news/how-sec-regs-will-change-cryptocurrency-markets/, Accessed June 17, 2022.

staffing of its Crypto Assets and Cyber Unit.[126] Unfortunately, growing the unit to 50 employees when the SEC employs over 4,500 staff is inadequate.[127] The second problem is that laws and regulations tailored to cryptocurrency need to be put in place immediately.

Him Das, the Director of FinCEN, the financial crimes enforcement branch of the U.S. Treasury, has said that existing U.S. laws are inadequate combat cryptocurrency money laundering.[128] Mr. Das cited the *Patriot Act* has an insufficient tool for combatting money laundering through the dark web. Some of the *Patriot Act's* powers were geared toward requirements imposed on traditional banking and financial institutions.

While the example of BlockFi demonstrated how the U.S. government can resolve challenging legal questions and integrate cryptocurrency entities into the existing regulatory framework, Ripple highlights the shortcomings of antiquated legislation in a new technological reality. The U.S.'s lawsuit with Ripple is ongoing and Ripple is attempting to compel documents from the SEC that support its argument that the SEC is selectively enforcing regulations on cryptocurrency entities.[129] It is conceivable that the U.S. could enact cryptocurrency legislation before it reaches a resolution with Ripple. When it comes to regulatory enforcement, the concern is not simply with the impact to Ripple and its customers, but rather all entities engaging in or contemplating similar approaches. Regulatory uncertainty as described in section 7.1 creates a grey area for cryptocurrency entities and pushes entities to

[126] Kirmi, A., "SEC doubles down on crypto regulation by expanding unit," *Coin Telegraph*, May 3, 2022, https://cointelegraph.com/news/sec-doubles-down-on-crypto-regulation-by-expanding-unit, Accessed June 11, 2022.
[127] SEC, "Fiscal Year 2021 Agency Financial Report," *SEC,* November 2021, https://www.sec.gov/files/sec-2021-agency-financial-report.pdf, p.1
[128] Wright, T., "FinCEN acting director says PATRIOT Act provision isn't 'right sized' for crypto enforcement," *Coin Telegraph*, April 28, 2022, https://cointelegraph.com/news/fincen-acting-director-says-patriot-act-provision-isn-t-right-sized-for-crypto-enforcement, Accessed June 12, 2022.
[129] Bank Frick, "Are crypto projects winning against the US regulator?," *Bank Frick,* May 5, 2022, https://www.bankfrick.li/en/are-crypto-projects-winning-against-us-regulator, Accessed June 12, 2022.

jurisdictions with laxer but clearer rules. New laws will make it make it easier for regulatory agencies to deal specifically with innovative technologies that evade law enforcement tracking, like privacy coins.

7.3 Broaden the Base, Draw Clear Lines

As of today, there are a host of entities that are unregulated, loosely regulated compared to fiat currency equivalents or exist in a grey zone, such as Ripple. What domestic legislation and global cooperation need to achieve is a broad consensus on who is 'in' and who is 'out'. The greater the inclusion of regulated entities, the greater the stability and cooperative partners in deterring fraud. Mere regulatory pressure has achieved some measures as noted in this paper: deterring exchanges from accepting funds from potentially illicit sources like privacy coins and similar tools and encouraging exchanges to adopt more robust KYC practices (prior to the implementation of direct regulations). New crypto-specific legislation should avoid large grey areas. Instead, a regulatory framework should welcome major players, allow room for innovative entrants early in their existence and outlaw and sanction bad actors. Legislation must be narrow enough to address the present, but be broad enough to address future innovation. Although many cryptocurrency entities view regulations as stifling, clear regulations can provide certainty within which to operate.

7.4 Regulate Stablecoins

In light of the stablecoin concerns outlined in section 6 of this paper, stablecoin regulation and oversight is urgently needed. In November 2021, the President's Working Group on Financial Markets requested that Congress make stablecoins subject to bank-like requirements of reserves and liquidity.[130] In May 2022, two U.S. senators went further when they proposed legislation that would require all

[130] Livni, E. and Lipton, E. "Regulators Ask Congress to Create New Rules for Cryptocurrencies," *New York Times,* November 1, 2021, https://www.nytimes.com/2021/11/01/business/stablecoins-cryptocurrency-regulation.html, Accessed June 12, 2022.

stablecoins to have 100% reserves and maintain a 1:1 peg with that asset.[131] Regulators in the UK This proposal is the most sensible path forward. While cryptocurrency will continue to attract those who believe deals that are too good to be true, like UST's 20% yield to maintain a stablecoin, there must be reliable, government-regulated stablecoins for investors to be able to safely trade within the cryptocurrency market. In order to achieve this safety, regulators will need not only to set a standard for stablecoins, but to have the power to audit reserves to ensure stablecoins are what they say they are. Public disclosure of reserves, as was agreed noted with the Tether settlement, should be required, akin to securities disclosure requirements for publicly-listed companies.

7.5 The Cryptocurrency Perspective

Part of what makes cryptocurrency regulation challenging is the ideological opposition of cryptocurrency entities. Fast moving technological innovation does not mix well with regimented regulation. Many cryptocurrency entities sought to create solutions not found in the traditional financial regime and escape bureaucracy. Cryptocurrency proponents view the decentralization of finance and corresponding absence of central government regulation to be key achievement of blockchain technology.[132] Regulation could inhibit future innovation from ever getting started.

Cryptocurrency proponents may also argue that regulation is ineffective. By one estimate, worldwide spending on anti-money laundering initiatives costs $180 billion a year whereas it's

[131] Smith, M. and Versprille, A, "Crypto Implosion Juices Senate Odd Couple's Push to Clamp Down," *Bloomberg*, May 20, 2022, https://www.bloomberg.com/news/articles/2022-05-20/crypto-unites-left-right-senate-odd-couplepushingtoclampdown?utm_campaign=socialfloworganic&utm_content=crypto&utm_source=twitter&utm_medium=social, Accessed June 12, 2022.

[132] Manzer, D. "The Challenges Of Regulating Cryptocurrency And Decentralized Finance," *Cassels*, October 12, 2021, https://cassels.com/insights/the-challenges-of-regulating-cryptocurrency-and-decentralized-finance/#:~:text=The%20crypto%20community%20at%20large,to%20these%20new%2C%20innovative%20offerings, Accessed June 15, 2022.

estimated that only $1-2 billion of criminal assets are seized annually.[133] Applying decades old banking laws to a technologically advanced field may not create the security regulators are seeking.

Given cryptocurrency entities resources and ability to lobby the government, it will be important to monitor future regulatory laws to assess the sway cryptocurrency achieves in setting its own rules.

8.0 IFA KEY LEARNINGS AND EDUCATION

While IFAs are trained to detect and track fraud, cryptocurrency money laundering investigations present difficulties for IFAs for the following reasons:

- Cross-jurisdictional flows of funds through dozens of platforms
- Varying regulatory treatment of cryptocurrencies and cryptocurrency platforms and many lax regulatory jurisdictions
- Laws, regulations and interpretations of them are rapidly evolving
- While blockchain ledger is public, trying individuals to transactions and tracing cryptocurrency requires specialized knowledge

[133] Sobrado, B., "Crypto Should Disrupt Current Anti-Money Laundering Practices, Not Adopt Them," *CoinDesk*, March 31, 2022, https://www.coindesk.com/layer2/2022/03/31/crypto-should-disrupt-current-anti-money-laundering-practices-not-adopt-them/, Accessed June 16, 2022.

Some investigations, particularly those involving millions of dollars worth of cryptocurrency or involving sophisticated dark web actors or criminal enterprises will require the use of experts. The *Standard Practices for Investigative and Forensic Accounting Engagements* provides several points of guidance to IFAs when relying on the work of others, notably in section 400, subsections 14 to 16.[134] When relying on other individuals or organizations, the IFA will need to consider their expertise and competence, professional reputation, objectivity and the reasonableness of their methodology and findings. This paper has relied on the research of leading cryptocurrency investigative firms, such as Chainanalysis, CipherTrace and Elliptic. It is a growing field that IFAs will likely need to work with and understand given the growth of cryptocurrency money laundering.

If IFAs have one takeaway for cryptocurrency investigations from this paper, it would be to follow the blockchain. The blockchain is an unbroken link from the start to the end for funds. The challenge is often finding the blockchain transaction with which to make a link. But once it is made, investigators may be able to track the funds to law-abiding entities.

For IFAs doing cryptocurrency-related investigations, the Journal of Accountancy offers five tips[135]:

- Find the exit and entry points
    - As this paper noted with the Colonial Pipeline and Bitfinex cases, finding where cryptocurrency either enters or exits the cryptocurrency ecosystem can allow an investigator to then have access to the chain of transactions going both backward and forward.

[134] Alliance for Excellence in Investigative and Forensic Accounting (AEIFA), "Standard Practices for Investigative and Forensic Accounting Engagements," *AEIFA,* November 2006.
[135] Hares, S., "5 Ways Accountants Can Track Cryptocurrency," *Journal of Accountacy*, June 29, 2020, https://www.journalofaccountancy.com/newsletters/2020/jun/accountants-track-cryptocurrency.html, Accessed June 3, 2022.

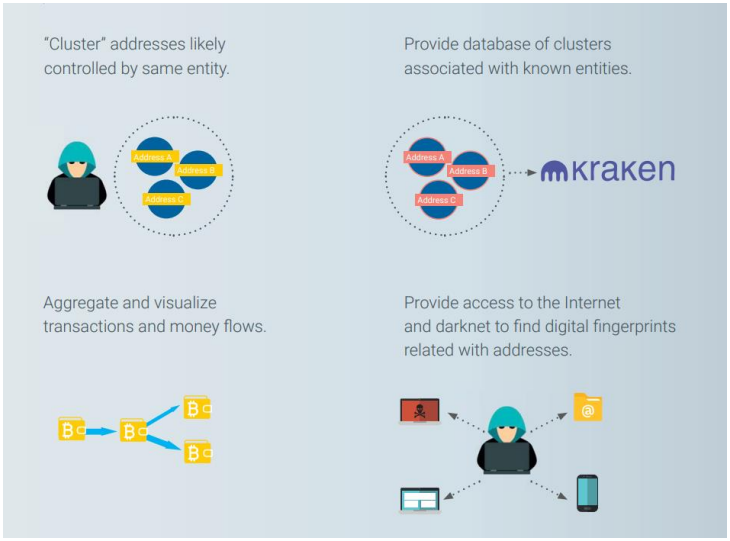
    - Once accomplished, IFAs can summons or subpoena regulated and/or cooperating cryptocurrency exchanges. Doing so can allow the IFA to track down the culprit, prove the fraud or potentially allow for the seizure of funds

- Create a profile of the suspect
    - The focus of this paper was generally related to high profile money laundering by criminal organizations.
    - However, the Journal of Accountancy article notes that IFAs may be conducting a wide variety of investigations and will need to consider the knowledge and experience of suspects to determine if IFAs should give thought to tracing cryptocurrency avenues.
- Find the device and extract the evidence
    - Case studies in this paper such as Silk Road, where the founder's computer was seized, or Bitfinex, where the government gained access to a suspect's cloud storage and found wallet address passwords.
- Drill down into transaction details
    - While this paper did cover the steps an IFA might need to undertake in order to present evidence in court, the money laundering techniques described in this paper reveal that organizing and showing the flow of cryptocurrency would be an arduous process
- Retain experts
    - As noted above, cryptocurrency investigations require such a specialized subset of knowledge and advanced computing skill that IFAs will need to work with forensic blockchain investigative firms
    - Cryptocurrency money laundering with extensive layering and would be impossible to decipher manually. Tools like automated searches and tracing and probabilistic analysis would be necessary.

- Even as IFAs grow more familiar with cryptocurrency, criminals are continually turning to advanced tools and methods. Wasabi Wallets and privacy coins will require technical expertise and once decryption of these processes becomes mainstream, criminal will move on to other tools.

Without advanced tools, typically possessed by experts, IFAs will be unlikely to experience success in tracing money laundered through cryptocurrency and related entities. Forensic cryptocurrency tools can identify patterns to determine clusters of transactions belonging to one individual or related entities, scan the internet and dark web for ties to the laundered money and visualize the flow of funds.[136]

Figure 9[137]



[136] Data Walk, "Cryptocurrency Investigations 101," *Data Walk,* November 2020, https://datawalk.com/wp-content/uploads/2020/11/Cryptocurrency-Investigations-101-What-Every-Analyst-Should-Know-DataWalk-ebook.pdf, Accessed June 15, 2022.
[137] Ibid.

Criminals are prone to pursue the most secretive and complex methods they can to hide the trail of illicit funds, so it is likely cryptocurrency will play a large role in IFA investigations in the years ahead.

9.0 CONCLUSION

In sum, law enforcement agencies, particularly in the U.S. have had successes in tracing and recovering stolen and laundered cryptocurrency assets. With that said, cryptocurrency crime is proliferating, specialized crypto criminals can be highly innovative and enforcement resources are limited. Moreover, regulatory uncertainty resulting from outdated laws pose additional challenges. While governments across the world are responding to the need to regulate cryptocurrency, jurisdictional limitations are hindering the ability to arrest and prosecute cryptocurrency money launderers. Money launderers operating in jurisdictions without extradition treaties can continue their fraudulent activities even after asset recovery by law enforcement officials. While better laws and global cooperation are an obvious answer, in light of rising global tensions and isolationism, notably with Russia, who often protects cryptocurrency criminals, cryptocurrency crimes are likely to continue. In five years time, the regulatory regimes will be improved, but so will the tools and techniques used by cybercriminals, however, the challenges faced by IFAs investigating cryptocurrency money laundering are likely to persist.

10.0 REFERENCES

Adegbe, L, "Wasabi Cryptocurrency Wallet Review," *Investopedia*, June 4, 2022, https://www.investopedia.com/wasabi-cryptocurrency-wallet-review-5271348, Accessed June 12, 2022.

Adler, D. "Silk Road: The Dark Side of Cryptocurrency," *Fordham Journal of Corporate & Financial Law*, February 21, 2018, https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/, Accessed May 1, 2022.

Anne-Bloom, C. et al., "Cryptocurrency Businesses Are Becoming A FINTRAC Reporting Entity," *MNP*, April 27, 2020, https://www.mnp.ca/en/insights/directory/cryptocurrency-businesses-are-becoming-a-fintrac-reporting-entity, Accessed June 5, 2022.

Ashford, K. "What is Cryptocurrency?," *Forbes*, January 25, 2022, https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/, Accessed May 5, 2022.

Asmakov, A. "Crypto's Total Market Cap Slips Below $1 Trillion as Bitcoin Drops Under $24,000," *Decrypt*, June 13, 2022. https://decrypt.co/102737/cryptos-total-market-cap-slips-below-1-trillion-as-bitcoin-drops-under-24000, Accessed June 14, 2022

Atkins, J. "Tether, Bitfinex prohibited from operating in New York, pays $18.5M settlement in

NYAG case," *CoinGeek* February 23, 2021, https://coingeek.com/tether-bitfinex-prohibited-from-operating-in-new-york-pays-18-5m-settlement-in-nyag-case/, Accessed June 12, 2022.

Bank Frick, "Are crypto projects winning against the US regulator?," *Bank Frick,* May 5, 2022, https://www.bankfrick.li/en/are-crypto-projects-winning-against-us-regulator, Accessed June 12, 2022.

Bearman J. and Hanuka, T. "The Rise and Fall of Silk Road," *Wired*, April and May 2015, https://www.wired.com/2015/04/silk-road-1/ and https://www.wired.com/2015/05/silk-road-2/, Accessed May 11, 2022.

Berwick, A. and Wilson, T. "How crypto giant Binance became a hub for hackers, fraudsters and drug traffickers," *Reuters*, June 6, 2022, https://www.reuters.com/investigates/special-report/fintech-crypto-binance-dirtymoney/?utm_source=Sailthru&utm_medium=newsletter&utm_campaign=daily-briefing&utm_term=06-06-2022, Accessed June 14, 2022.

Blockstream Explorer, "Transaction," *Blockstream Explorer,* May 30, 2022, https://blockstream.info/tx/9ad27f12e92c424165db75d191ec3c368cbd7a684630b66092bb3a0cad39bf94?output:0, Accessed May 30, 2022.

Bochan, T. "The Story Behind QuadrigaCX and Gerald Cotten, Netflix's 'Crypto King'," *CoinDesk*, March 29, 2022, https://www.coindesk.com/learn/the-story-behind-quadrigacx-and-gerald-cotten-netflixs-crypto-king/#:~:text=%22The%20downfall%20of%20crypto%20asset,those%20assets%20would%20be%20safeguarded, Accessed May 7, 2022.

Bogna, J. "How Does Bitcoin Mining Work?," *PC Mag*, December 9, 2021, https://www.pcmag.com/how-to/how-does-bitcoin-mining-work, Accessed May 3, 2022.

Browne, R. "Cryptocurrency firms Tether and Bitfinex agree to pay $18.5 million fine to end New York probe," *CNBC,* February 23, 2021, https://www.cnbc.com/2021/02/23/tether-bitfinex-reach-settlement-with-new-york-attorney-general.html, Accessed June 12, 2022.

Carlisle, D., "Preventing Financial Crime in Cryptoassets," *Elliptic,* 2022.

Castaldo, J. et al. "Crypto chaos: From Vancouver to Halifax, tracing the mystery of Quadriga's missing millions," *The Globe and Mail*, February 8, 2019, https://www.theglobeandmail.com/business/article-crypto-chaos-from-vancouver-to-halifax-tracing-the-mystery-of/, Accessed May 7, 2022.

Chainanalysis, "Chainalysis in Action: OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over $160 million from Ransomware Attackers, Scammers, and Darknet Markets," *Chainanalysis,* September 22, 2021 https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021/, Accessed June 13, 2022.

Chow, A. "Inside the Chess Match That Led the Fed to $3.6 Billion in Stolen Bitcoin," *Time*, February 10, 2022, https://time.com/6146749/cryptocurrency-laundering-bitfinex-hack/, Accessed June 10, 2022.

CipherTrace, "CipherTrace Files Two Monero Cryptocurrency Tracing Patents," CipherTrace,

November 20, 2020, https://ciphertrace.com/ciphertrace-files-two-monero-cryptocurrency-tracing-patents/, Accessed June 9, 2022.

CoinBase, "Luna Price," *CoinBase*, June 19, 2022, https://www.coinbase.com/price/terra-luna, Accessed June 19, 2022.

Coinbase. "What is Cryptocurrency?," *Coinbase*, 2022, https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency, Accessed May 9, 2022.

ComplyAdvantage, "A Guide to Anti-Money Laundering for Crypto Firms," *ComplyAdvantage*, 2022.

ComplyAdvantage, "Cryptocurrency Regulations Around The World," *ComplyAdvantage,* June 10, 2022, https://complyadvantage.com/insights/cryptocurrencyregulationsaroundworld/#:~:text=Cryptocurrency%20exchanges%20are%20legal%20in,submit%20reports%20to%20the%20authorities, Accessed June 13, 2022.

Conway, L. "What are the Safest Ways to Store Bitcoin?," *Investopedia,* February 28, 2021, https://www.investopedia.com/news/bitcoin-safe-storage-cold-wallet/, Accessed May 6, 2022.

Cooper, S. "Federal 'failures' on money laundering prompt B.C. inquiry to call for provincial watchdog," *Global News,* June 15, 2022, https://globalnews.ca/news/8922745/cullen-commission-findings-report-bc-money-laundering-inquiry/, Accessed June 16, 2022.

Cryptopedia, “What are Stablecoins?,” *Cryptopedia*, May 10, 2022, https://www.gemini.com/cryptopedia/what-are-stablecoins-how-do-they-work#section-algorithmic-stablecoins, Accessed June 2, 2022.

Davies, P., “Terra Luna stablecoin collapse explained: Is this the 2008 financial crash moment of cryptocurrency?,” *EuroNews*, May 12, 2022, https://www.euronews.com/next/2022/05/12/terra-luna-stablecoin-collapse-is-this-the-2008-financial-crash-moment-of-cryptocurrency, Accessed June 1, 2022.

Deepwebsitelinks, “Top 10 Bitcoin Tumbler Services 2021,”, Deepwebsitelinks, 2021, https://www.deepwebsiteslinks.com/bitcoin-tumbler-services/, Accessed June 13, 2022.

Dossett, J. “What Are Stablecoins and Are They Less Risky? The Details Crypto Investors Should Know”, *CNET*, May 31, 2022, https://www.cnet.com/personal-finance/crypto/what-are-stablecoins-and-are-they-less-risky-the-details-crypto-investors-should-know/, Accessed June 2, 2022.

European Union, “Directive (Eu) 2018/843 Of The European Parliament And Of The Council Of 30 May 2018,” *Official Journal of the European Union*, May 30, 2018.

FATF, “FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins,” *FATF*, June 2020.

FATF, “International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation,” *FATF*, 2022.

FATF, “Who we are,” *FATF,* 2022, https://www.fatf-gafi.org/about/, Accessed June 11, 2022.

Flitter, E. “BlockFi, a crypto firm, reaches a $100 million settlement for failing to register loan products,” *New York Times,* February 14, 2022, https://www.nytimes.com/2022/02/14/business/blockfi-sec-crypto-loans.html, Accessed June 13, 2022.

Frankenfield, J. “51% Attack,” *Investopedia*, April 27, 2022, https://www.investopedia.com/terms/1/51-attack.asp, Accessed May 25, 2022.

Government of Canada, “Travel rule for electronic funds and virtual currency transfers,” *Government of Canada,* April 22, 2022, https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/travel-acheminement/1-eng, Accessed June 10, 2022.

Grauer, K. et al. “The 2022 Crypto Crime Report,” *Chainanalysis*, 2022, https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

Greenberg, A. “Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market,” *Forbes,* September 5, 2013, https://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/?sh=3d070482adf7, Accessed June 1, 2022.

Greenberg, A. “Prosecutors Trace $13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop,” *Wired*, January 29, 2015, https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/, Accessed May 12, 2022.

Hammond, S. and Ehret, T., “Cryptocurrency regulations by country,” *Thomson Reuters*, April

2022, https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf.

Haeberli, D. et al., "Blockchain & Cryptocurrency Laws and Regulations 2022: Switzerland," Global Legal Insights, 2022,https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/switzerland, Accessed June 10, 2022.

Hurry, S. et al., "New tech act in Switzerland secures legal environment, allows blockchain to flourish," *IMD*, February 2021, https://www.imd.org/news/updates/new-tech-act-Switzerland-secures-legal-environment-blockchain-flourish/, Accessed June 5, 2022.

Hussein, Fatima, "Treasury Secretary Yellen calls for cryptocurrency regulation to reduce risk, fraud," *PBS*, April 7, 2022, https://www.pbs.org/newshour/economy/treasury-secretary-yellen-calls-for-cryptocurrency-regulation-to-reduce-risk-fraud, Accessed June 5, 2022.

Institute for Security and Technology, "Combating Ransomware," *Ransomware Task Force,* 2021.

Kim, P. "Privacy coins are cryptocurrencies that can be traded anonymously," *Business Insider*, February 10, 2022, https://www.businessinsider.com/personal-finance/privacy-coins, Accessed June 7, 2022.

Kirmi, A., "SEC doubles down on crypto regulation by expanding unit," *Coin Telegraph*, May 3, 2022, https://cointelegraph.com/news/sec-doubles-down-on-crypto-regulation-by-expanding-unit, Accessed June 11, 2022.

Kocegarovas, G. "Cryptocurrency money laundering risk: the best explanation of a 3-step

process," *PSP Lab,* February 16, 2022, https://psplab.com/cryptocurrency-money-laundering-risk-a-3-stepprocess/#:~:text=If%20placement%20allows%20criminals%20to,transfers%20between%20different%20wallet%20addresses, Accessed May 4, 2022.

Lipton, E. "As Scrutiny of Cryptocurrency Grows, the Industry Turns to K Street," *New York Times,* November 1, 2021, https://www.nytimes.com/2021/05/09/us/politics/cryptocurrency-regulation-sec-ripple-labs.html, Accessed June 16, 2022.

Liu, M. et al. "Detecting Roles of Money Laundering in Bitcoin Mixing Transactions: A Goal Modeling and Mining Framework," *Frontiers in Physics*, July 6, 2021. https://doi.org/10.3389/fphy.2021.665399, Accessed May 4, 2022.

Livni, E. and Lipton, E. "Regulators Ask Congress to Create New Rules for Cryptocurrencies," *New York Times,* November 1, 2021, https://www.nytimes.com/2021/11/01/business/stablecoins-cryptocurrency-regulation.html, Accessed June 12, 2022.

Macias, A. and Wilkie, C. "U.S. recovers $2.3 million in bitcoin paid in the Colonial Pipeline ransom," *CNBC*, June 7, 2021, https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html, Accessed June 6, 2022.

Manzer, D. "The Challenges Of Regulating Cryptocurrency And Decentralized Finance," *Cassels*, October 12, 2021, https://cassels.com/insights/the-challenges-of-regulating-

cryptocurrencyandecentralizedfinance/#:~:text=The%20crypto%20community%20at%20large,to%20these%20new%2C%20innovative%20offerings, Accessed June 15, 2022.

Mellor, S. "Crypto companies spent millions on Super Bowl ads. So did Pets.com," *Fortune*, February 14, 2022 https://fortune.com/2022/02/14/crypto-companies-super-bowl-ads-coinbase-ftx-bitcoin-ether/, Accessed April 29, 2022.

Montgomery, J. "Bare Bitcoins — No Fourth Amendment Privacy in Virtual Currency Records," Freeman Law, 2021, https://freemanlaw.com/bare-bitcoins-no-fourth-amendment-privacy-in-virtual-currency-records/, Accessed June 5, 2022.

Murphy. H., "Monero emerges as crypto of choice for cybercriminals," *Financial Times*, June 22, 2021, https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6, Accessed June 12, 2022.

Nahar, P. "What are 51% Attacks in Cryptocurrencies?," *The Economic Times*, August 31, 2021, https://economictimes.indiatimes.com/markets/cryptocurrency/what-are-51-attacks-in-cryptocurrencies/articleshow/85802504.cms?from=mdr, Accessed May 8, 2022.

Namcios, "Wasabi Wallet Parent Company Explains Decision To Censor Bitcoin Transactions," *Bitcoin Magazine,* March 28, 2022, https://bitcoinmagazine.com/business/wasabi-wallet-explains-new-bitcoin-censorship, Accessed June 17, 2022.

Ontario Securities Commission, "QuadrigaCX: A Review by Staff of the Ontario Securities Commission," April 14, 2020.

Phillips, T. and Thornton, A., "Congress Must Not Provide Statutory Carveouts for Crypto Assets," *Center for American Progress,* March 1, 2022,

https://www.americanprogress.org/article/congress-must-not-provide-statutory-carveouts-for-crypto-assets/, Accessed June 17, 2022.

Popper, N. "Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes," *New York Times,* January 14, 2021, https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html, Accessed May 4, 2022.

Ravelli, R. "Arrest of Alleged Bitcoin Fog Operator Signals Continued DOJ Focus on Crypto "Mixers"," *Lexology*, May 18, 2021, https://www.lexology.com/library/detail.aspx?g=b46073d7-0731-42d2-b319-270bd0c17c6e, Accessed June 4, 2022.

Reynolds, K. "Bittrex to Delist 'Privacy Coins' Monero, Dash and Zcash," *CoinDesk*, January 1, 2021, https://www.coindesk.com/markets/2021/01/01/bittrex-to-delist-privacy-coins-monero-dash-and-zcash/, Accessed June 8, 2022.

Robinson, T. "Elliptic Follows the $7 Billion in Bitcoin stolen from Bitfinex in 2016," *Elliptic*, May 13, 2021, https://www.elliptic.co/blog/elliptic-analysis-bitcoin-bitfinex-theft, Accessed June 12, 2022.

Romo, V. "How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom," *NPR*, June 8, 2021 https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac, Accessed June 6, 2022.

Rooney, K. "Record $1 billion worth of bitcoin linked to the Silk Road seized by U.S. government," *CNBC,* November 6, 2020, https://www.cnbc.com/2020/11/05/1-billion-worth-of-bitcoin-linked-to-the-silk-road-seized-by-the-

us.html#:~:text=The%20U.S.%20government%20seized%20an,the%20history%20of%20the%20agency., Accessed May 10, 2022.

SEC, "BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of its Crypto Lending Product," *SEC*, February 14, 2022, https://www.sec.gov/news/press-release/2022-26, Accessed June 13, 2022.

SEC, "Fiscal Year 2021 Agency Financial Report," *SEC*, November 2021, https://www.sec.gov/files/sec-2021-agency-financial-report.pdf.

Seth, S. "Explaining the Crypto in Cryptocurrency," *Investopedia*, May 15, 2022, https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/, Accessed May 9, 2022.

Sharma, R., "How SEC Regs Will Change Cryptocurrency Markets," *Investopedia,* June 7, 2022, https://www.investopedia.com/news/how-sec-regs-will-change-cryptocurrency-markets/, Accessed June 17, 2022.

Smith, M. and Versprille, A, "Crypto Implosion Juices Senate Odd Couple's Push to Clamp Down," *Bloomberg*, May 20, 2022, https://www.bloomberg.com/news/articles/2022-05-20/crypto-unites-left-right-senate-odd-couplepushingtoclampdown?utm_campaign=socialfloworganic&utm_content=crypto&utm_source=twitter&utm_medium=social, Accessed June 12, 2022.

Sobrado, B., "Crypto Should Disrupt Current Anti-Money Laundering Practices, Not Adopt

Them," *CoinDesk*, March 31, 2022, https://www.coindesk.com/layer2/2022/03/31/crypto-should-disrupt-current-anti-money-laundering-practices-not-adopt-them/, Accessed June 16, 2022.

Stevens, R. "Bitcoin Mixers: How Do They Work and Why Are They Used?," *CoinDesk*, March 8, 2022, https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/, Accessed June 13, 2022.

Stevens, R. "What Are Privacy Coins and Are They Legal?," *CoinDesk,* January 10, 2022, https://www.coindesk.com/learn/what-are-privacy-coins-and-are-they-legal/, Accessed June 8, 2022.

Tasker, J.P. "In a pitch to cryptocurrency investors, Poilievre says he wants Canada to be 'blockchain capital of the world'," *CBC News*, March 28, 2022, https://www.cbc.ca/news/politics/poilievre-bitcoin-policy-1.6399986, Accessed April 30, 2022.

Uberti, D, "How the FBI Got Colonial Pipeline's Ransom Money Back," *Wall Street Journal*, June 11, 2021, https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981, Accessed June 7, 2022.

Van Boom, D., "Luna Crypto Crash: How UST Broke and What's Next for Terra," *CNET,* May 25, 2022, https://www.cnet.com/personal-finance/crypto/luna-crypto-crash-how-ust-broke-and-whats-next-for-terra/, Accessed June 11, 2022.

Weaver, N. "How I Traced 20% Of Ross Ulbricht's Biticoin To The Silk Road," *Forbes*, January 20,

2015, https://www.forbes.com/sites/frontline/2015/01/20/bitcoin-silk-road-ulbricht/?sh=712f96ec5637, Accessed June 2, 2022.

Wright, T., “FinCEN acting director says PATRIOT Act provision isn't 'right sized' for crypto enforcement,” *Coin Telegraph*, April 28, 2022, https://cointelegraph.com/news/fincen-acting-director-says-patriot-act-provision-isn-t-right-sized-for-crypto-enforcement, Accessed June 12, 2022.