Citation for published version:
Larkin, C, Pearce, N & Shannon, N 2021, Criminality and cryptocurrencies: Enforcement and policy responses - Part I. in S Corbet (ed.), *Understanding Cryptocurrency Fraud.* Batten-Corbet-Lucey Handbooks in Alternative Investments, vol. 2, De Gruyter, Germany, pp. 121-131. https://doi.org/10.1515/9783110718485-010

DOI:
10.1515/9783110718485-010

Publication date:
2021

Document Version
Peer reviewed version

Link to publication

Publisher Rights
CC BY-ND

University of Bath

Alternative formats
If you require this document in an alternative format, please contact:
openaccess@bath.ac.uk

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 08. Jun. 2022

Criminality and Cryptocurrencies: Enforcement and Policy Responses - Part I

Charles Larkin [Institute for Policy Research, University of Bath; Trinity Business School, Trinity College Dublin; Advanced Academic Programmes, Krieger School of Arts and Sciences, Johns Hopkins University],
Nick Pearce [Institute for Policy Research, University of Bath],
Nadine Shannon [Institute for Policy Research, University of Bath]

Introduction

In this chapter we focus on some examples of cryptocurrency fraud. Primarily the Silk Road (1.0 and 2.0) and various dark web frauds. This is part of a two part series of chapters addressing criminality and the usage of cryptocurrencies, this one focusing on dark web marketplace uses and the second looking at instances of wire fraud and money laundering. We also explain the linkages between older criminal and civil law law statutes that have been applied to the new world of cybercrime. At the outset, it is useful to cite the US Army War College manual of 2016 outlining the new field of battle, the Internet. While the Internet has disrupted commerce and politics, it has also changed the face of criminal activity. *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition* (2016) highlighted how cyberspace has become an effective force multiplier, essentially a source of disruption and vulnerability as well as a facilitator of globalisation.[1]

Cryptocurrencies & Crime

Organised crime has been able to take advantage of this force multiplier to perform the same illegal activities they have undertaken in the past but from the relative comfort of the keyboard. The use of Bitcoin, Etherum and other cryptocurrencies for criminality has been addressed in Kethineni and Cao (2019). [2]

> Counterterrorism experts are concerned about the popularity of virtual currency, its global outreach, decentralization, the speed of transactions, relative ease of use, and the lack of deterrence. However, the volatility of virtual currency, the possible theft of virtual

[1] Williams, Phil & Fiddner, Dighton, Eds. (2016) *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition.* US Army War College Press.

[2] Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. International Criminal Justice Review, 30(3), 325–344. https://doi.org/10.1177/1057567719827051

> currency held in virtual wallets, the potential inability to transfer virtual currency to and from foreign currencies, and the growing interest in tracking virtual currencies by law enforcement and government regulators may deter some cybercriminals (Brill & Keene, 2014). The recent crackdown on BTCs [Bitcoins] by the Chinese government led to a precipitous drop in the value of virtual currencies. Such volatility in value may explain why there is no widespread use of virtual currency in terrorist activities. As of now, there are only a few pieces of anecdotal evidence about the use of virtual currencies in terrorist operations. At present, most terrorist funding involves mechanisms such as the traditional hawala (informal cash transaction) system. Reports indicate that some technologically savvy terrorists groups are receptive to new technologies (Goldman, Maruyama, Rosenburg, Saravalle, & Solomon-Strauss, 2017).[3]

The pressure for state actors to address the challenge of cryptocurrencies as instruments of criminality and terrorist financing has elicited some initial responses as of writing.

> We can identify three ways that countries have tried to deal with cryptocurrencies: some such as Iceland, Nepal, and Lebanon have banned them. Others like Japan, states within the USA, Australia have accepted them as legal tender and have introduced a regulatory system allowing for their use in specific sectors as long as to those using this currency know their customer (KYC). There are also countries that are exploring the potential of cryptocurrencies but have yet to decide on whether to permit their use. There are also countries such as Iran, Venezuela and Russia that are looking to cryptocurrencies as a means of circumventing international sanctions and getting more revenue, which adds further challenges to countries that seek to develop this sector.
>
> Three things are clear when it comes to cryptocurrencies. Firstly, states have adopted a robust counterterrorism finance (CTF) regime, beginning with President Bush Executive Order 13224 (2001) which sought to starve off funding for terrorist groups, that has had a positive impact on hindering the ability of terrorist to fundraise. Consequently, terrorist groups and criminal enterprises constantly look for new ways to raise and transfer money.17 Secondly, firms operating in the digital currency space are determined to keep the sector clean as they want it to grow, which is why there is an internal incentive to engage in self-regulation and to be seen to be purer than pure. Thirdly, terrorist groups adapt and learn.18 A recent RAND Report pointed out:
>
> > should a single cryptocurrency emerge that provides widespread adoption, better anonymity, improved security, and that is subject to lax or inconsistent regulation, then the potential utility of this cryptocurrency, as well as the potential for its use by terrorist organizations, would increase.[4]

Even with these robust responses by state actors, it is clear that the skills gap between law enforcement and the criminal community that uses cryptocurrencies on a regular basis, remains

---

[3] Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. International Criminal Justice Review, 30(3), 325–344. P 330.

[4] Isaac Kfir (2020) Cryptocurrencies, national security, crime and terrorism, *Comparative Strategy*, 39:2, 113-127. P 114-5.

sizable.[5] In certain circumstances, tools developed by state actors for the purposes of security have had unintended consequences, such as the development of TOR. TOR has become the preferred platform for criminal activity on the dark net.

> Organized crime groups have not only found ways to improve classic forms of lucrative crime; they have also forged entirely new moneymaking and money laundering ventures with the aid of the Internet and its wide user base. Advancements in this technology and its proliferation have, in turn, allowed more actors to perform illegal cyber activities across the world. For example, technology like the TOR Browser, which was created by the U.S. Naval Research Laboratory, has allowed Internet users to access any website while remaining anonymous by bouncing their Internet Protocol (IP) address from one node to another around the world. It also has created the "Deep Web," which consists of websites that can only be accessed while using the TOR Browser. Virtual currencies, particularly crypto-currencies such as Bitcoin, have enabled these same users to transfer money globally within a matter of minutes and with a high degree of anonymity.[6]

The International Monetary Fund has provided a useful overview as well of how TOR and the dark net facilitate financial crime in their September edition of *Finance & Development* (2019).[7] Ultimately, criminality in cyberspace is a reflection of the pre-internet world but with some additions. Virtual currencies, and the anonymity they offer, have facilitated this expansion in the dark web. As has been highlighted in Corbet, et al (2018)[8] and Corbet, et al (2019)[9], cryptocurrencies are highly volatile assets. US Treasury Secretary Janet Yellen highlighted this in a recent comment:

> "I don't think that bitcoin ... is widely used as a transaction mechanism," she told CNBC's Andrew Ross Sorkin at a New York Times DealBook conference. "To the extent it is used I fear it's often for illicit finance. It's an extremely inefficient way of conducting transactions, and the amount of energy that's consumed in processing those transactions is staggering."[10]

This is a drawback but when looked at initially but when compared to cash mules, traditional wire transfers and EFTs, this is a relatively discrete and low cost method of paying for illicit goods. As Hoard, et al (2016) states:

---

[5] Isaac Kfir (2020) Cryptocurrencies, national security, crime and terrorism, *Comparative Strategy*, 39:2, 113-127.

[6] Hoard, Shawn C., Carasiti, Jeffrey L., & Masten, Edward J. (2016)"The Adaptive Nature of Crime: Co-opting the Internet." in Williams, Phil & Fiddner, Dighton, Eds. (2016) *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition.* US Army War College Press. P 274

[7] https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm

[8] Shaen Corbet, Andrew Meegan, Charles Larkin, Brian Lucey, Larisa Yarovaya. (2018) "Exploring the dynamic relationships between cryptocurrencies and other financial assets" *Economics Letters*, Volume 165, Pages 28-34.

[9] Shaen Corbet, Brian Lucey, Andrew Urquhart, Larisa Yarovaya. (2019) "Cryptocurrencies as a financial asset: A systematic analysis" *International Review of Financial Analysis,* Volume 62, Pages 182-199.

[10] https://www.cnbc.com/2021/02/22/yellen-sounds-warning-about-extremely-inefficient-bitcoin.html

> On the other hand, the risk has not deterred criminals, as it is one of the most anonymous ways of transferring money. Even though the ledger that contains all transactions is public, very little identifying information can be obtained regarding each transaction. What does appear in the block chain is simply the user's "public address" a string of 26-35 alphanumeric characters, for example, 1BwGkaVotRx8bXXXXtqsa-b1jHMDoQfWJc. Each time a user performs a transaction, a new public address will appear in association with that transaction, making it very difficult to identify spending patterns. To make Bitcoin transactions even more anonymous, software programmers have developed applications called mixers and tumblers. Essentially, these services are money-laundering programs intended to mask the source of the transaction. A user of a mixer will put his or her Bitcoins into a shared Bitcoin wallet with other users. When the user wants to perform a transaction, many small transactions are performed simultaneously from that single Bitcoin wallet. Using this method, it is nearly impossible for law enforcement to determine which user of a Bitcoin mixing service is the source of the transaction. One of these services is Dark Wallet. Dark Wallet encrypts and mixes users' payments, making the flow of online money untraceable.
>
> ...
>
> In order to purchase these drugs the user needs to purchase Bitcoins from an online exchange service or a peer-to-peer exchange and load a balance of Bitcoins to the Silk Road website. In effect, Silk Road operated as an escrow service where the administrators acted as middlemen between sellers and buyers. With a balance of Bitcoins uploaded to Silk Road, the user can start purchasing narcotics, including stimulants, psychedelics, prescription, precursors, opioids, ecstasy, cannabis, and steroids. Once these products were purchased, they were shipped in ordinary envelopes through the UPS, FedEx, and even the United States Postal Service.[11]

In this context it is easy to see the attraction of cryptocurrencies to those engaged in criminal activities.

It appears that for distributed terrorist networks the attraction is not as great.

> As things stand, several factors seem to discourage terrorists from using cryptocurrencies (at least at this stage). First, terrorists need goods and services that until recently could be purchased only with hard currency. Second, the complexity of blockchain technologies means that it is possible that many terror groups still don't understand what blockchain can give them. Third, the price volatility of cryptocurrencies tends to discourage terrorists from investing too much, as some have very limited resources and don't want to waste what they have. A fourth issue, which is increasingly being addressed, is whether the use of cryptocurrencies is permissible under Islamic law. These are all transient issues as seen by the fact that the US Department of the Treasury, the British Gambling Commission and

[11] Hoard, Shawn C., Carasiti, Jeffrey L., & Masten, Edward J. (2016)"The Adaptive Nature of Crime: Co-opting the Internet." in Williams, Phil & Fiddner, Dighton, Eds. (2016) *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition.* US Army War College Press. P 296-297

> others including Interpol and the EU are taking the view that there is a need to remain vigilant about the possibility of terrorist groups moving into the cryptocurrencies sphere.[12]

The rise of cryptocurrencies has not been exclusively due to their usefulness in facilitating crime but largely an outgrowth of a desire for privacy and an interest in alternative financial structures that were attractive to those with a liberterian orientation. Ultimately, cryptocurrencies' capacity to operate in an environment of near complete anonymity has become a unifying force between those different groups of individuals and turned this new financial tool into an effective tool of criminality. Various cases of fraud have taken place in the past involving cryptocurrencies since their introduction. In this chapter we look at the nature of these cases and the legal instruments used to prosecute them.

The usefulness of Bitcoin to criminal enterprises is how it is able to operate outside of the normal exchange structures of the economy. As highlighted by work by Loretta Napeoleoni (2008), before the rise of Bitcoin in 2009, criminal enterprises suffer from very high transaction costs and will seek to reduce those costs where possible.[13] Here is where the Silk Road was able to thrive, as it allowed for the nexus of ideology, technology and criminality to thrive. Silk Road was an online exchange where illicit goods and services could be bought and sold anonymously outside of the reach of law enforcement. The site was hosted on the platform Tor (the onion router), which is an anonymous hidden hosting service as well as an internet browser designed to provide layers (hence the onion name) of anonymity. Tor, supported by the Tor Project, Inc, a 501(c)(3) non-profit in the US, was founded by a group of people who work to keep the internet anonymous: "...all of the people who have been involved in Tor are united by a common belief: internet users should have private access to an uncensored web. ... The goal of onion routing was to have a way to use the internet with as much privacy as possible, and the idea was to route traffic through multiple servers and encrypt it each step of the way."[14]

The matrix of potential criminal avenues for Bitcoin in this context were outlined by Bohme, et al (2015)

> Bitcoin receives regulatory scrutiny for three classes of criminal concerns: Bitcoin-specific crime, money laundering, and Bitcoin-facilitated crime.
> *Bitcoin-specific crimes* are attacks on the currency and its infrastructure like bitcoin theft, attacks on mining pools, and denial-of-service attacks on exchanges to manipulate exchange rates. Law enforcement often struggles to prevent or solve these crimes due to their novelty, lack of clarity on which agency and jurisdiction are responsible, technical complexity, procedural uncertainty, and limited resources.
> Second, Bitcoin can be used for *money laundering*. Bitcoin money laundering could evolve to become more difficult to trace, particularly when funds are routed through mixers, with mixing records concealed from the public and perhaps unavailable to law enforcement. These characteristics might assist perpetrators in concealing or mischaracterizing the

[12] Isaac Kfir (2020) Cryptocurrencies, national security, crime and terrorism, *Comparative Strategy*, 39:2, 113-127. P 119..
[13] Napoleoni, Loretta. (2011). *Rogue economics*. Seven Stories Press.
[14] https://www.torproject.org/about/history/

proceeds of crime. That said, Bitcoin also includes design elements that could facilitate the tracing of funds, including publication of the block chain (providing permanent publicly available records of what funds moved where).
Finally, *Bitcoin-facilitated crime* entails payment for unlawful services delivered (or purportedly delivered) offline, like the illegal goods and services sold on Silk Road and payment of funds in extortion. Criminals may be drawn to virtual currencies because they perceive a lack of regulatory oversight, because they distinctively value irreversible transactions, or because they have been banned or ejected from other payment mechanisms.[15]

Enforcement Case Studies: Silk Road (1.0 & 2.0), Sheep Marketplace & Joker's Stash

Wired provides a window into that nexus of ideology, technology and criminality when it quotes a note sent out by Ross Ulbricht, the man behind the creation of Silk Road, to his Internet followers:

> "MONEY IS POWERFUL," DPR [Dread Pirate Roberts, a.k.a. Ross Ulbricht] wrote to the Silk Road faithful, "and it's going to take power to effect the changes I want to see." By that time, DPR was a millionaire many times over, but those resources, he told his followers, were for the revolution. Freedom, after all, needs financing.
>
> DPR had founded Silk Road as a digital instantiation of the libertarian ideal: a frictionless marketplace where everyone had freedom as long as it didn't impinge on someone else's freedom. For DPR and the community that grew around him, Silk Road was about more than contraband; it was a movement. As Silk Road quickly grew, DPR's pronouncements became more grandiose. He wrote that "every single transaction is a victory" in weakening the "thieving, murderous" state. What began as a belief in free choice came to sound like revolutionary dogma.
>
> It made for ambitious business plans. DPR wanted to expand his liberty-fueled brand into an empire, with his own Silk Road–affiliated bitcoin exchange, credit union, and encrypted communication service. Buoyed by quick success, DPR shared the heady enthusiasm of the licit startup world. Whereas he'd once considered selling Silk Road for $1 billion, he told a reporter in a rare, encrypted chat interview that Silk Road was worth 10 figures, maybe 11.
>
> But behind the scenes, Ross faced constant crises. There were technical problems, management issues, a quickly changing marketplace, and the volatility of bitcoin. There

[15] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of economic Perspectives*, *29*(2), 213-38.P230

were scammers on the site. And even as Silk Road made more money, the cost to maintain it rose. Ross, feeling besieged from all sides, recorded his efforts in a log.

...

In an incredible twist, Force [convicted former DEA Agent Carl M. Force[16]], along with a Secret Service agent on his team, was also indicted and arrested this past March for running an elaborate series of rackets and thefts on Silk Road. The 95-page indictment alleged that they stole bitcoins from Silk Road and other exchanges (the digital equivalent of keeping the suitcase full of cash after a dockside heroin bust); pocketed $50,000 from DPR for intel services from "Kevin"; laundered at least half a million of that (some of which made it to Panama); and served a false subpoena on a digital currency exchange when they questioned his transactions and froze his account. It was, in fact, when all this came to the attention of the Department of Justice that Force left the DEA. "In retrospect," Tarbell said when he heard about the investigation of Force, "it's as if you found out at the end of Breaking Bad that Hank was dirty the whole time."

In retrospect, a lot of Force's story takes on a different light. Ironically, he had warned DPR about the danger of double identity, but if this indictment is true he seems to have fallen prey to it himself. Force allegedly operated online not only as Nob but had also created several other identities and used them to blackmail DPR with law enforcement information for at least $100,000. Like Ross, Force must have believed in the secrecy of Tor. During the sting operation with Curtis Green, Force even told Green he thought the Silk Road servers would never be found. But they were, and after they documented Ross' misdeeds, they also revealed that it was Force and the Secret Service agent who had stolen $350,000 in bitcoins from Silk Road—the theft that led Ross to put the hit on Curtis Green.[17]

While Bitcoin offered many of the technological and ideological requirements for the operation of this criminal enterprise, it still suffered from very high transaction costs, not just from price volatility but also from the ease of theft, facilitated by the need for exchanges and the use of Bitcoin "wallets". While this digital "currency" was able to circumvent many of the limitations of moving money between parties, especially when compared to cash, it was still far from the seamless alternative. The Common Law tradition is to treat virtual currencies as the same as a foreign money, in effect as a commodity, and therefore not money. This means that for the purposes of settling contracts in the law, the contract will need to be expressed in the local currency, be that US dollars or sterling.[18] Given the volatility of cryptocurrencies, this will make it a poor unit of account and contracting currency if all transactions had to be ultimately settled in US dollars or sterling. The nature of the transactions, being in effect "wire transfers", allows for the criminal

[16] Department of Justice. Former DEA Agent Sentenced for Extortion, Money Laundering and Obstruction Related to Silk Road Investigation. https://www.justice.gov/opa/pr/former-dea-agent-sentenced-extortion-money-laundering-and-obstruction-related-silk-road#:~:text=Force%20was%20a%20special%20agent,activity%20on%20the%20Silk%20Road

[17] Bearman, Joshua & Hanuka, Tomer. (2015) The Untold Story of Silk Road, Part 2: The Fall. *Wired.* https://www.wired.com/2015/05/silk-road-2/

[18] Gleeson, S. (2018). *The legal concept of money*. Oxford University Press.

code as it relates to wire fraud, which are frauds using the non-postal communications network, to be a useful entrepot to more serious offences, like those leveled against Ross Ulbricht.

The US wire fraud statute is typically the starting point for prosecutors seeking indictments related to cryptocurrency activity. Due to the nature of cryptocurrency transactions, those found guilty of criminal activity while transacting with a cryptocurrency largely fall into the category of wire fraud. The US code defines wire fraud as such in 18 USC § 1343:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation occurs in relation to, or involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

While the wire fraud statute was used against the former DEA agent Carl M. Force, it was not used in the indictment of Ross Ulbricht. The extensive criminality and management role taken up by Ulbricht in the Silk Road was seen as going beyond the behaviours of a normal fraudster, as Ulbricht had created a new type of grand bazaar of criminal activity. This triggered an unusual indictment by the US Attorney. In the case of Silk Road the US Attorney for the Southern District of New York, Preet Bharara, went beyond the typically cryptocurrency suite of indictments and used a special "kingpin" statute 21 USC § 848, Continuing Criminal Enterprise, normally reserved for prosecutions related to the organized crime (more famously the RICO Act, 18 USC § 1961-1968 has been applied, along with this statute, in the prosecution of organized crime.) The indictment filed by the US Attorney states that Ulbricht had operated the Silk Road website between January 2011 and October 2013 as a sophisticated and extensive criminal marketplace on the Internet, with several thousand drug dealers and unlawful vendors selling to over a hundred thousand purchasers globally. Ulbricht's role in this was one of organizer, supervisor and manager and from this role obtained substantial income and resources, therefore attracting an indictment of Continuing Criminal Enterprise. The use of computer hacking in violation of 18 USC 1030 (a) (2) and money laundering conspiracy added the cryptocurrency dimension. Ulbricht deliberately designed the Silk Road marketplace to operate a Bitcoin-based payment system to facilitate illegal commerce by concealing the identities and locations of the users sending and receiving funds, a violation of 18 USC 1956.[19]

The infamous Silk Road 1 case was summarised in the statements made by Katherine B. Forrest, a United States District Judge of the United States District Court for the Southern District of New

[19] US v. Ross William Ulbricht. Indictment. 4 February 2014. https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf

York when she sentenced Ross Ulbricht, the mastermind of the Silk Road marketplace. Judge Forrest, when handing down a life sentence, told Mr. Ulbricht that "what you did in connection with Silk Road was terribly destructive to our social fabric."[20]

As the *New York Times* described it:

> Mr. Ulbricht's novel high-tech drug bazaar operated in a hidden part of the Internet sometimes known as the dark web, which allowed deals to be made anonymously and out of the reach of law enforcement. In Silk Road's nearly three years of operation, over 1.5 million transactions were carried out involving several thousand seller accounts and more than 100,000 buyer accounts, the authorities have said.
>
> Transactions were made using the virtual currency Bitcoin, and Mr. Ulbricht, operating under the pseudonym Dread Pirate Roberts, took in millions of dollars in commissions, prosecutors have said. They said Mr. Ulbricht had "developed a blueprint for a new way to use the Internet to undermine the law and facilitate criminal transactions," and that his conviction was "the first of its kind, and his sentencing is being closely watched."
>
> Judge Forrest echoed that message. "What you did was unprecedented," she told Mr. Ulbricht, "and in breaking that ground as the first person," he had to pay the consequences. Anyone who might consider doing something similar, the judge added, needed to understand clearly "and without equivocation that if you break the law this way, there will be very serious consequences."[21]

This was not the end of the Silk Road site. Ulbricht's security assistant on the original Silk Road, took over the Dread Pirate Roberts title, becoming Dread Pirate Roberts 2. Thomas White, who was eventually arrested, convicted and sentenced to 5 years and 4 months by Liverpool Crown Court for the management of the Silk Road 2.0 site from his Liverpool, UK flat. Thomas White, 24, admitted to: Supplying a controlled drug of class A, contrary to section 4(3)(a) of the Misuse of Drugs Act 1971; assisting or inducing the commission of an offence abroad, contrary to section 20 of the Misuse of Drugs Act 1971; transferring criminal property, contrary to section 327(1)(d) of the Proceeds Of Crime Act 2002; and making 464 indecent images of children of category A, contrary to section 1(1)(a) of the Protection of Children Act 1978.[22]

The UK Crown Prosecution Service once again highlighted to role of Bitcoin:

---

[20] Paul, Kari. (2015) Unsealed Transcript Shows How a Judge Justified Ross Ulbricht's Life Sentence. *Vice.* https://www.vice.com/en/article/53dm8a/unsealed-transcript-shows-how-a-judge-justified-ross-ulbrichts-life-sentence

[21] Weiser, Benjamin. (2015) Creator of Silk Road, a Secretive Online Drug Bazaar, Gets Life in Prison. *New York Times.* https://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html

[22] https://www.cps.gov.uk/cps/news/dark-web-drug-dealer-jailed-after-rebooting-worlds-biggest-online-drug-marketplace

> John Williams, from the CPS, said: "Although Thomas White used anonymity and pseudonyms to try and cover his tracks, the CPS was able to show that he was the guiding mind behind the building of Silk Road 2.0.
>
> "Copies of back-ups of Silk Road were found on an encrypted laptop seized from White's flat following his arrest in November 2014, along with crypto-currency Bitcoin relating to Dread Pirate Roberts 2.
>
> "Parcels sent to StExo, the online user name featured on Silk Road 2.0 ended up at his home address in Liverpool and a rented mailbox.
>
> "He received an income that allowed lavish spending with no credible explanation. He had also provided money laundering advice and sold MDMA on the original Silk Road site."[23]

The Silk Road and Silk Road 2.0 are two examples of where the nexus of ideology, technology and criminality thrive but they are not necessarily the entirety of the so-called "dark web" or "darknet".[24] The dark web is part of the wider "deep web". The deep web is the part of the internet that is not regularly accessible via standard search platforms such as Google. The dark web is a specific part of the deep web that preferences anonymity of use. The dark web, as a result of that anonymous feature, is preferred for transactions in criminal goods and services (e.g. stolen/illegal goods, stolen financial data, passwords, identities and human trafficing and pornography). These goods and services are typically purchased using cryptocurrencies, such as Bitcoin. The rationale for using a cryptocurrency is that it protects the identity of the buyer and seller in a transaction. The Silk Road was considered, in 2011, one of the most well-developed and mature of these dark web markets.

While it is important to note that while these elements allow a certain amount of anonymous activity, the active investigations by the DEA and FBI along with the US Attorney's Office resulted in the successful revelation of Ross Ulbricht's identity and subsequently in the UK by the Crown Prosecution Service of Thomas White. Possession was taken of the assets of Ulbricht and White. In the case of Ulbricht, the US Marshall's Service auctioned off 30,000 Bitcoins as part of the sale of Silk Road seized assets in 2014.[25] In November 2020, there was a movement of nearly $1bn worth of Bitcoin related to the Silk Road out of a Ulbricht-related wallet to a new unknown wallet.[26] This was subsequently seized by the criminal investigations unit of the IRS.[27]

> "Silk Road was the most notorious online criminal marketplace of its day," said U.S. Attorney Anderson. "The successful prosecution of Silk Road's founder in 2015 left open a billion-dollar question. Where did the money go? Today's forfeiture complaint answers

---

[23] https://www.cps.gov.uk/cps/news/dark-web-drug-dealer-jailed-after-rebooting-worlds-biggest-online-drug-marketplace

[24] The terms "dark web" and "darknet" can be used interchangeably in this and the subsequent chapter.

[25] https://www.wired.com/2014/07/vaurum/

[26] https://www.theguardian.com/technology/2020/nov/04/silk-road-bitcoins-worth-1bn-change-hands-after-seven-years

[27] https://www.irs.gov/compliance/criminal-investigation/united-states-files-a-civil-action-to-forfeit-cryptocurrency-valued-at-over-one-billion-us-dollars

this open question at least in part. $1 billion of these criminal proceeds are now in the United States' possession."

The civil complaint merely alleges that certain property is subject to forfeiture. The United States must prove, by a standard of preponderance of the evidence, that the items are subject to forfeiture. If the United States prevails, the court will order all interests of any potential claimant forfeited.

The forfeiture action is the result of an investigation by IRS – Criminal Investigation Cyber Crimes Unit with assistance from Chainalysis and Excygent.[28]

According to Chainanalysis, "Silk Road accounted for nearly 20% of total Bitcoin economic activity at its peak in 2013. Silk Road's economic activity reached $435 million total (calculated based on the price of Bitcoin at the time) with a peak of just under $40 million in monthly volume in September of 2013."[29]

The capacity of US Government authorities to track and confiscate illegally obtained Bitcoin wealth, despite the supposed anonymity of the transactions is underscored by the 2013 shutdown of the Sheep Marketplace (owned by Czech national Tomáš Jiřikovský), an alternative dark web site for the sale and purchase of illegal drugs and the first to use Bitcoin as a means of exchange. 5,400 Bitcoins were stolen from Sheep Marketplace, exploiting a flaw in the code of the website. It was rumored to be worth at the time between $100m and $200m but $4.5m was confiscated by US Federal authorities, along with the arrest of the two thieves Nathan Gibson and Sean Mackert, (they have subsequently pleaded guilty) in 2016.[30],[31]

In early 2021 there was one example where a cryptocurrency-funded dark net site was able to close down operations on more-or-less it's own terms. Joker's Stash, a website begun in 2014 on the dark net that sold stolen credit card and identity information for cryptocurrency tokens, closed with having made over $1bn in cryptocurrency-denominated revenue. Interpol and the FBI were able to shut down the various websites used by Joker's Stash in December 2019, though many remained operational due to TOR mirrors. The possibility of those being co-opted by the police for sting operations was considered high, which means that the shutdown of the Joker's Stash site for good in February 2021 was a defensive measure on the part of the individual(s) to prevent capture.[32] The Dutch police engaged in a similar hijack recently and it appears to be a moderately successful tactic for combating cybercrime in the dark net.[33]

---

[28] https://www.irs.gov/compliance/criminal-investigation/united-states-files-a-civil-action-to-forfeit-cryptocurrency-valued-at-over-one-billion-us-dollars

[29] https://blog.chainalysis.com/reports/silk-road-doj-seizure-november-2020

[30] https://www.forbes.com/sites/laurashin/2016/05/30/mystery-solved-6-6-million-bitcoin-theft-that-brought-down-dark-web-site-tied-to-2-florida-men/?sh=2974a71523d5

[31] https://www.justice.gov/usao-mdfl/pr/more-17-million-forfeited-funds-presented-law-enforcement-agencies

[32] https://www.reuters.com/article/us-crypto-currency-crime-idUSKBN2AC14R

[33] https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm

The understanding of many of those involved in the creation and maintenance of these sites was that the technology and the rapid accumulation of wealth would ensure that their activities were anonymous to fellow criminals and the government. This was ultimately not the case, most especially when Federal investigators infiltrated the Silk Road. Persistent, technologically assisted, police investigations can achieve positive results given time and resources.

Ulbricht's manifesto was that "MONEY IS POWERFUL, and it's going to take power to effect the changes I want to see." In the end, neither Ulbricht nor his cryptocurrency wealth was powerful enough to withstand the soft budget constraint of determined state actors in possession of the law and the capacity to enforce it.

Conclusion

In this first part, we focused on the application of cryptocurrencies to the dark net. While the deep web and even the dark web were both produced to assist communities seeking privacy and the creation of cryptocurrencies was an attempt at an alternative, government-free monetary system, they have both given rise to exploitation by criminal elements. The capacity for law enforcement to make inroads has been marked by the use of old-fashioned techniques with modern-day advances but has been marred by the fact that some undercover agents have crossed the line into criminality. As will be seen in Part II, the need for greater coordination between domestic agencies and internationally is the key to developing an effective regulatory response and the transnational enforcement of the law.

****

Criminality and Cryptocurrencies: Enforcement and Policy Responses - Part II

Charles Larkin [Institute for Policy Research, University of Bath; Trinity Business School, Trinity College Dublin; Advanced Academic Programmes, Krieger School of Arts and Sciences, Johns Hopkins University],
Nick Pearce [Institute for Policy Research, University of Bath],
Nadine Shannon [Institute for Policy Research, University of Bath]

Wire Fraud: An Introduction to the Legal Position

The US wire fraud statute is typically the starting point for prosecutors seeking indictments related to cryptocurrency activity. Due to the nature of cryptocurrency transactions, those found guilty of criminal activity while transacting with a cryptocurrency largely fall into the category of wire fraud. The US code defines wire fraud as such in 18 USC § 1343:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation occurs in relation to, or involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

Wire fraud, as stated in a previous chapter, can be applied to a wide range of criminal activities. The main criteria for applying 18 USC § 1343 is the use of telephony, telecommunications technology for the committing of financial fraud. A scheme to defraud committed that involves material misrepresentation or omission involving the use of wires to further the scheme will fall within the remit of this statute. The US legal system has an extensive structure of financial fraud statutes. This is an indicative but not exhaustive list of statutes related to financial crimes of fraud and attempted fraud:

- Section 32(a) of the Securities Exchange Act of 1934 (Exchange Act) (*15 U.S.C. § 78ff(a)*).
- Section 24 of the Securities Act of 1933 (Securities Act) (*15 U.S.C. § 77x*).
- Sarbanes–Oxley Act of 2002 (SOX) (*Pub L. No. 107-204*).
- Mail and wire fraud statutes (*18 U.S.C. §§ 1341, 1343*).
- Bank fraud statute (*18 U.S.C. § 1344*).
- Misapplication and embezzlement statute (*18 U.S.C. § 656*).

- Fraudulent and fictitious claims statute (also known as the Criminal False Claims Act) (*18 U.S.C. § 287*).
- Tax evasion and fraud provisions of the Internal Revenue Code (*26 U.S.C. §§ 7201, 7206*).
- Computer Fraud and Abuse Act of 1986 (*18 U.S.C. § 1030(a)(4)*).
- False statements statute (*18 U.S.C. § 1001*).
- Major Fraud Act of 1988 (*18 U.S.C. § 1031*).

Relevant provisions that impose civil liability for fraud, and which can serve as predicates for criminal violations in certain circumstances, include:

- False Claims Act (also known as the Lincoln Law) (*31 U.S.C. §§ 3729–3733*).
- Sections 11, 12(a), and 17(a) of the Securities Act (*15 U.S.C. §§ 77k, 77l(a), 77q(a)*).
- Sections 9, 10(b), 14, 16(b), and 18 of the Exchange Act (*15 U.S.C. §§ 78i, 78j(b), 78n, 78p(b), 78r*).
- Securities and Exchange Commission (SEC) Rules 10b-5 and 14a-9 (*17 C.F.R. §§ 240.10b-5, 240.14a-9*).
- Sections 4b, 6(c), and 6c of the Commodity Exchange Act (*7 U.S.C. §§ 6b, 9, 13a-1*).
- Commodity Futures Trading Commission (CFTC) Rule 180.1 (*17 C.F.R. § 180.1*).
- Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) (*12 U.S.C. § 1833a(c)(2)*).[34]

Enforcement comes from various agencies of the government:

- Department of Justice (DOJ), including the US Attorney's Office (USAO) in each federal district and the Federal Bureau of Investigation (FBI).
- Securities and Exchange Commission (SEC).
- Commodities Futures Trading Commission (CFTC).
- Non-governmental self-regulatory organisations (SROs) such as the Financial Industry Regulatory Authority (FINRA).
- Department of the Treasury, including the Internal Revenue Service (IRS).
- Federal Trade Commission (FTC).

The above are all related to the US Federal jurisdiction. While this is the most important for the purposes of most financial crime, and in particular the case of the original Silk Road, it is not the only jurisdiction that matters. As much of the financial apparatus of the globe is to be found in New York and London, local investigatory powers come into play. In the case of New York, the Attorney General of the State of New York has previously prosecuted financial frauds. In the case of London, the Serious Fraud Office (SFO) and Financial Conduct Authority (FCA) in conjunction with the Crown Prosecution Service (CPS) investigate and enforce UK laws in England and Wales.[35] It is important to note that in the UK context the law of England and Wales

[34] David M Zornow, Jocelyn E Strauber and Daniel Merzel. (2021) *Financial crime in the United States: overview.* https://uk.practicallaw.thomsonreuters.com/7-520-6422?transitionType=Default&contextData=(sc.Default)&firstPage=true

[35] https://uk.practicallaw.thomsonreuters.com/8-520-4390?__lrTS=20201015042943723&transitionType=Default&contextData=(sc.Default)&firstPage=true#co_anchor_a950827

is different to that of Scotland despite both being part of the United Kingdom, but given the preeminence of London in financial services most attention is focused on English law.

Wire Fraud & Scams

Given the design of the wire fraud statute, there are many manifestations of criminality. Some are more rudimentary, like that of GAW Miners and ZenMiner, where $20m worth of fake Bitcoins were sold to unsuspecting investors. The operation of this criminal enterprise was via a classic "Ponzi" scheme, with later investors paying for the returns enjoyed by early investors. At no point did Homero Joshua Garza, the perpetrator of this crime, have the computer power to deliver the Bitcoins that he was purporting to sell. The Securities and Exchange Commission in their December 2015 release following the arrest of Garza outlined the crimes and the SEC complaint:

> The SEC alleges that Homero Joshua Garza perpetrated the fraud through his Connecticut-based companies GAW Miners and ZenMiner by purporting to offer shares of a digital Bitcoin mining operation. In reality, GAW Miners and ZenMiner did not own enough computing power for the mining it promised to conduct, so most investors paid for a share of computing power that never existed. Returns paid to some investors came from proceeds generated from sales to other investors.
>
> "As alleged in our complaint, Garza and his companies cloaked their scheme in technological sophistication and jargon, but the fraud was simple at its core: they sold what they did not own, misrepresented what they were selling, and robbed one investor to pay another," said Paul G. Levenson, Director of the SEC's Boston Regional Office.
>
> According to the SEC's complaint:
>
> - From August 2014 to December 2014, Garza and his companies sold $20 million worth of purported shares in a digital mining contract they called a Hashlet.
> - More than 10,000 investors purchased Hashlets, which were touted as always profitable and never obsolete.
> - Although Hashlets were depicted in GAW Miners' marketing materials as a physical product or piece of mining hardware, the promised contract purportedly entitled the investor to control a share of computing power that GAW Miners claimed to own and operate.
> - Investors were misled to believe they would share in returns earned by the Bitcoin mining activities when in reality GAW Miners directed little or no computing power toward any mining activity.
> - Because Garza and his companies sold far more computing power than they owned, they owed investors a daily return that was larger than any actual return they were making on their limited mining operations.
> - Therefore, investors were simply paid back gradually over time under the mantra of "returns" out of funds that Garza and his companies collected from other investors.

- Most Hashlet investors never recovered the full amount of their investments, and few made a profit.[36]

"Ponzi" schemes, named after the most famous of all practitioners of this fraud Charles Ponzi in the 1920s. According to the US Securities and Exchange Commission's consumer investor protection service Investor.gov, they define a "Ponzi" scheme as such:

> A Ponzi scheme is an investment fraud that pays existing investors with funds collected from new investors. Ponzi schemes are named after Charles Ponzi. In the 1920s, Ponzi promised investors a 50% return within a few months for what he claimed was an investment in international mail coupons. Ponzi used funds from new investors to pay fake "returns" to earlier investors.
>
> Ponzi scheme organizers often promise high returns with little or no risk. Instead, they use money from new investors to pay earlier investors and may steal some of the money for themselves.
>
> With little or no legitimate earnings, Ponzi schemes require a constant flow of new money to survive. When it becomes hard to recruit new investors, or when large numbers of existing investors cash out, these schemes tend to collapse.[37]

This definition, almost perfectly fits the definition of the fraud committed by Garza with the sale of non-existent computing power, therefore non-existent Bitcoins. These types of fraud are easily facilitated by the information asymmetries that exist between cryptocurrency investors, especially novices in this area and lack a technical background, treating cryptocurrencies as yet another commodity investment class, and cryptocurrency miners and exchange managers who understand (to a certain extent) the full technical requirements of the blockchain.

It is important to note that "Ponzi" schemes have a near relative, the pyramid scheme. These schemes are also attractive to those wishing to exploit the bandwagon effect of bubbles that exist within Bitcoin and other cryptocurrencies.[38] The difference with them is that a pyramid scheme requires that the initially defrauded person must recruit further investors. While Ponzi schemes are easy to prosecute, a pyramid scheme requires more investigation. The SEC Investor.gov consumer protection site describes them as such:

> Fraudsters frequently promote pyramid schemes through social media, Internet advertising, company websites, group presentations, conference calls, YouTube videos, and other means. Pyramid scheme promoters may go to great lengths to make the program look like a business, such as a legitimate multi-level marketing (MLM) program. But the

[36] https://www.sec.gov/news/pressrelease/2015-271.html
[37] https://www.investor.gov/introduction-investing/investing-basics/glossary/ponzi-schemes
[38] See Corbet, Shaen, Brian Lucey, Larisa Yarovaya, (2018) "Datestamping the Bitcoin and Ethereum bubbles" *Finance Research Letters*, Volume 26, Pages 81-88 for further details on the creation and propagation of bubbles in cryptocurrencies.

fraudsters use money paid by new recruits to pay off earlier stage investors (usually recruits as well). At some point, the schemes get too big, the promoter cannot raise enough money from new investors to pay earlier investors, and people lose their money.

These are some of the hallmarks of a pyramid scheme:

- *Emphasis on recruiting*. If a program focuses solely on recruiting others to join the program for a fee, it is likely a pyramid scheme. Be skeptical if you will receive more compensation for recruiting others than for product sales.
- *No genuine product or service is sold.* Exercise caution if what is being sold as part of the business is hard to value, like so-called "tech" services or products such as mass-licensed e-books or online advertising on little-used websites. Some fraudsters choose fancy-sounding "products" to make it harder to prove the company is a bogus pyramid scheme.
- *Promises of high returns in a short time period.* Be skeptical of promises of fast cash – it could mean that commissions are being paid out of money from new recruits rather than revenue generated by product sales.
- *Easy money or passive income.* There is no such thing as a free lunch. If you are offered compensation in exchange for doing little work such as making payments, recruiting others, or placing online advertisements on obscure websites, you may be part of an illegal pyramid scheme.
- *No demonstrated revenue from retail sales.* Ask to see documents, such as financial statements audited by a certified public accountant (CPA), showing that the company generates revenue from selling its products or services to people outside the program. As a general rule, legitimate MLM companies derive revenue primarily from selling products, not from recruiting members.
- *Complex commission structure*. Be concerned unless commissions are based on products or services that you or your recruits sell to people outside the program. If you do not understand how you will be compensated, be cautious.

All Pyramid Schemes Collapse

When fraudsters attempt to make money solely by recruiting new participants into a program, that is a pyramid scheme, and there is only one possible mathematical result – collapse. Imagine if one participant must find six other participants, who, in turn, must find six new recruits each. In only 11 layers of the "downline," you would need more participants than the entire population of the United States to maintain the scheme. This infographic shows how all pyramid schemes are destined to collapse.[39]

In the case of Garza, while being a *cause célèbre* at the time, it was a relatively straightforward fraud and a classic example of wire fraud. What has made cryptocurrencies novel in the area of fraud is that this involves a new asset class, which has developed rapidly since 2008. The attractiveness of a new technology to bubbles and to outright fraud should not come as a surprise. Recent work on

[39] https://www.investor.gov/protect-your-investments/fraud/types-fraud/pyramid-schemes

bubbles by Quinn and Turner (2020) highlights how historically bubbles are facilitated by new technologies.[40] Bubbles have also been traditionally associated with frauds, facilitated by political or technological conditions that allow a combination or marketability, credit and speculation to ignite an event. The market failures in the form of information asymmetries and moral hazard opportunities brought about by a new technology are well documented, cryptocurrencies being the latest in a long line of such occurrences.[41]

Wire fraud, though a serious crime, typically does not attract a very lengthy custodial sentence. This in part reflects the rationale behind the application of the "kingpin" statute (21 USC § 848) to Ulbricht, which attracts a much more severe penalty. In September 2018, Garza was convicted of wire fraud and sentenced to 21 months imprisonment.

> On September 13, 2018, Homero Joshua Garza, 33, was sentenced to 21 months of imprisonment in connection with a wire fraud charge brought by the U.S. Attorney for the District of Connecticut. His prison term will be followed by three years of supervised release, the first six months of which Garza must spend in home confinement. Garza, a defendant in a now-concluded, parallel SEC civil fraud action, admitted to running a virtual currency scam in which investors lost millions of dollars.
>
> The SEC's case was resolved last year when the court entered final judgments in June and October 2017, respectively, against Connecticut-based GAW Miners and ZenMiner and their principal, Garza, for bilking investors. According to the SEC's December 1, 2015 complaint, at Garza's direction, GAW Miners and ZenMiner sold shares in a purported bitcoin mining operation; however, neither company had the capability to engage in large-scale mining. As a result, most investors paid for a share of computing power that never existed. Returns paid to some investors came, not from successful mining activity, but from proceeds generated by sales to other investors.[42]

How did this fall within the wire fraud statute? As this was a fraud perpetrated on individuals and firms using the telecommunications network, as opposed to the postal network, which triggers mail fraud (18 U.S. Code § 1341) and the involvement of the US Postal Inspection Service (postal police), it constituted wire fraud under the definition of 18 USC § 1343.

Wire Fraud & Theft

There are some classic examples of theft at work in the cryptocurrency world. One of the more well known examples was led by Eli and Assaf Gigi, who were arrested by the Israeli police in June

[40] Quinn, W., & Turner, J. D. (2020). *Boom and bust: A global history of financial bubbles*. Cambridge University Press.
[41] Quinn, W., & Turner, J. D. (2020). *Boom and bust: A global history of financial bubbles*. Cambridge University Press.
[42] https://www.sec.gov/litigation/litreleases/2018/lr24281.htm

2019. This was a combination of a phishing and URL hijacking (typosquatting) to tricking victims into providing login information and installing virtual wallet management software that was ultimately designed to steal their cryptocurrency.[43] The volume of the theft is in dispute but it could be between tens of million to 100 million USD in value.[44]

The SEC defines this type of phishing activity as such:

> "Phishing" involves the use of fraudulent emails and copy-cat websites to trick you into revealing valuable personal information — such as account numbers for banking, securities, mortgage, or credit accounts, your social security numbers, and the login IDs and passwords you use when accessing online financial services providers. The fraudsters who collect this information then use it to steal your money or your identity or both.
>
> When fraudsters go on "phishing" expeditions, they lure their targets into a false sense of security by hijacking the familiar, trusted logos of established, legitimate companies. A typical phishing scam starts with a fraudster sending out millions of emails that appear to come from a high-profile financial services provider or a respected Internet auction house.
>
> The email will usually ask you to provide valuable information about yourself or to "verify" information that you previously provided when you established your online account. To maximize the chances that a recipient will respond, the fraudster might employ any or all of the following tactics:
>
> Names of Real Companies — Rather than create from scratch a phony company, the fraudster might use a legitimate company's name and incorporate the look and feel of its website (including the color scheme and graphics) into the phishy email.
>
> "From" an Actual Employee — The "from" line or the text of the message (or both) might contain the names of real people who actually work for the company. That way, if you contacted the company to confirm whether "Jane Doe" truly is "VP of Client Services," you'd get a positive response and feel assured.
>
> URLs that "Look Right" — The email might include a convenient link to a seemingly legitimate website where you can enter the information the fraudster wants to steal. But in reality the website will be a quickly cobbled copy-cat — a "spoofed" website that looks for all the world like the real thing. In some cases, the link might lead to select pages of a legitimate website — such as the real company's actual privacy policy or legal disclaimer.
>
> Urgent Messages — Many fraudsters use fear to trigger a response, and phishers are no different. In common phishing scams, the emails warn that failure to respond will result in your no longer having access to your account. Other emails might claim that the company

[43] https://posta.co.il/article/389501/
[44] https://ciphertrace.com/wp-content/uploads/2019/08/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q2-1.pdf

> has detected suspicious activity in your account or that it is implementing new privacy software or identity theft solutions. This type of crime is relatively commonplace on the internet.[45]

In the US context these behaviours, most especially when conducted via business emails will attract the following charges: 18 U.S.C. § 1956(h): Conspiracy to Engage in Money Laundering; 18 U.S.C. § 1 349 : Conspiracy to Commit Wire Fraud, Mail Fraud, and Bank Fraud ; 18 U.S.C. § 1343: Wire Fraud; 18 U.S.C. § 1344(2) : Bank Fraud ; 18 U.S.C. § 1956(a) (1) (B) (i) : Money Laundering; 18 U.S . C. § 1957: Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity ; 18 U.S.C. §§ 1960(a), (b) (1) (A), (b) (1) (B), (b) (1) (C): Operating an Unlicensed Money Transmitting Business; 18 U.S.C. § 2232(a) : Destruction of Property to Prevent Seizure; 18 U. S.C . § lOOl(a) (2): False Statements; 18 U.S.C. § 1028A(a) (1): Aggravated Identity Theft; 1 8 U. S . C. § 2(a): Aiding and Abetting; 1 8 U.S.C. §§ 981 and 982 and 28 U. S . C. § 2461(c): Criminal Forfeiture.[46]

These phishing thefts and their related BEC (business email compromise) and EAC (email account compromise) attacks have triggered more transnational law enforcement coordination. These types of crimes typically are frauds, identity thefts or other forms of illicit money transfers that fall within the remit of existing statutes relating to fraud and anti-money laundering. As anti-money laundering requires international coordination, financial crime and cybercrime specialists have coordinated transnationally to respond. The US Department of Justice in the 2018 Operation Wire Wire and the 2019 Operation reWired worked with several international law enforcement agencies in Nigeria, Turkey, Germany, Ghana, France, Italy, Japan, Kenya, Malaysia, and the United Kingdom as well as the newly created Internet Crime Complaint Center (IC3) of the FBI. These coordinated actions resulted in a total of 355 arrests across these countries for these types of frauds, thefts and money laundering activities.[47]

Wire Fraud & ICOs

Wire fraud comes into its own in the context of the Initial Coin Offering. The CFTC has focused in particular on this area with the following warning to investors:

> SEC and CFTC staff have recently observed investment scams where fraudsters tout digital asset or "cryptocurrency" advisory and trading businesses. In some cases, the fraudsters claim to invest customers' funds in proprietary crypto trading systems or in

[45] https://www.sec.gov/reportspubs/investor-publications/investorpubsphishinghtm.html
[46] https://www.justice.gov/usao-cdca/pr/massive-international-fraud-and-money-laundering-conspiracy-detailed-federal-grand-jury
[47] https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds; https://www.justice.gov/opa/pr/74-arrested-coordinated-international-enforcement-operation-targeting-hundreds-individuals; https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019; https://www.ic3.gov/

> "mining" farms. The fraudsters promise high guaranteed returns (for example, 20-50%) with little or no risk.[48]

The CFTC goes further to say:

> Purchasing virtual currencies on the cash market – spending dollars to purchase Bitcoin for your personal wallet, for example – comes with a number of risks, including:
>
> - Most cash markets are not regulated or supervised by a government agency;
> - Platforms in the cash market may lack critical system safeguards, including customer protections;
> - Volatile cash market price swings or flash crashes;
> - Cash market manipulation;
> - Cyber risks, such as hacking customer wallets; and/or
> - Platforms selling from their own accounts and putting customers at an unfair disadvantage.
>
> It's also important to note that market changes that affect the cash market price of a virtual currency may ultimately affect the price of virtual currency futures and options.[49]

These are not idle threats. One of the most fertile grounds for fraud in cryptocurrencies is the initial coin offering.

In recent years, the largest volume of crypto crimes by value has involved Initial Coin Offering (ICO) scams and Ponzi schemes, such as the OneCoin scam perpetrated by 'Cryptoqueen', Ruja Ignatova.[50] It has been estimated that 25% of ICOs are fraudulent[51], while an analysis of 2017 ICOs by Tokendata found that 46% had either failed at the funding stage, cut and run with investors' money, or simply faded away.[52] The gold rush mentality of investment in cryptoassets makes consumers of ICOs an easy target for fraud.

Nonetheless, most reports to law enforcement agencies of crypto currency crimes involve extortion. Extortion scams typically involve 'sextortion', theft of data, or more recently, Covid-19 related threats.[53] 'Sextortion' spam schemes, using a threat to reveal compromising images or videos to a victim's contacts, increasingly leverage crypto currencies for payment demands. Asking for payments in Bitcoin 'cuts the spamming supply chain to its bare minimal as there is no need to develop sophisticated techniques to monetize the scheme. Indeed, the upper-tail of the supply chain is butchered...there are no URL redirections and bulletproof hosting to deal with, credible websites to maintain, or business partners to find' (Paquet-Clouston et al, 2019).

---

[48] https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/watch_out_for_digital_fraud.html

[49] https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/understand_risks_of_virtual_currency.html

[50] Bartlett, 2019

[51] Bank of International Settlements, 2018

[52] Sedgwick, 2018

[53] Europol, 2020

Cybercriminals also target victims using ransomware, demanding payment in privacy coins such as Monero, the largest privacy coin by market capitalisation. The ransomware-as- service model, Sodinokibi, otherwise known as REvil, has adopted Monero as its preferred payment for ransoms from victims. It has been behind major ransomware attacks, such as that levelled against Travelex on New Year's Eve, 2019.[54]

Thefts from individual and enterprise wallets have also multiplied in recent years, as crypotassets become valuable targets for cybercriminals. In 2018, high profile thefts included Coincheck ($540 million stolen) and Zaif ($60 million stolen) in Japan, and Bithumb ($32 million stolen) in South Korea.[55] In 2019, there were ten publicly confirmed hacks of exchanges where criminals stole crypto currencies, resulting in thefts of €240 million worth of assets,[56] and then in September 2020, in another large exchange hack, more than $275 million worth of cryptocurrency was stolen from the KuCoin exchange. The perpetrators of the KuCoin hack used Decentralised Finance (DeFi) protocols to launder the stolen tokens. The hackers used decentralised apps known as decentralised exchanges or DEX apps, which allow users to buy, sell and swap different tokens built on a specific blockchain directly between one another's wallets. Users can undertake these currency swaps without providing KYC (know-your-customer) information or recording the trades in an order book as they would on a standard cryptocurrency exchange.[57]

'Cryptojacking' - in which the computer processing power of a victim is hijacked to mine crypto currencies - has also emerged as a new form of cybercrime in recent years. Targets involve both connected devices and cloud infrastructures. One popular coin mining service, Coinhive, was extensively targeted by cryptojackers after its launch on 2017 to mine the Minero cryptocurrency and divert funds to themselves. It was closed down in 2019, precipitating a substantial drop in cryptojacking hits. Cybercriminals have also increasingly targeted cloud infrastructures, exploiting application programming interfaces (APIs) and container management platforms to mine cryptocurrencies.[58]

Illicit activity on the dark web was initially disrupted by the Covid-19 pandemic in 2020.
The value of dark web transactions declined in the Spring of 2020, in tandem with the fall in the price of Bitcoin and other cryptocurrencies. After this brief fall, the value of dark web market revenues then recovered but the disruption to global supply chains and postal services consolidated purchasing, as consumers stockpiled: overall revenue was up in 2020, but total transfers to dark web markets were down.[59] One recent study of the impact of Covid-19 on dark web drug markets analysed 262 self-reported submissions of illicit drug transactions and found after March 21, 2020, the share of drugs supply shipments that had issues or failed increased rapidly and represented a

[54] Haworth, 2020
[55] HM Treasury, FCA and Bank of England, 2018
[56] Europol, 2020
[57] Chainanalysis, 2020a
[58] ENISA, 2020
[59] Chainanalysis, forthcoming, 2021

majority of all shipments. At the peak of the market disruption, the successful deliveries represented only 21% of all transactions.[60]

Law enforcement activity has been stepped up against dark web traders and this too may account for consolidation in illicit markets. In the US, the Department of Justice created a Joint Criminal Opioid and Darknet Enforcement (J-CODE) team to leverage federal and international partnerships to combat online drug sales. J-CODE has conducted major enforcement operations, such as Operation Disarray and Operation SaboTor, which have shut down dark web accounts used for illegal activity. Agents executed 65 search warrants, seizing more than 299 kilograms of drugs, 51 firearms, and more than $7 million, including $4.504 million in cryptocurrency.[61]

The blockchain analysis firm, Chainalysis, has recently speculated that crypto crime might evolve in a number of ways in the near term.[62] Following the shutdown in 2019 of Bestmixer.io - one of the three largest cryptocurrency mixer services – Chainalysis speculates that criminals may search for alternatives to third party custodial mixers such as wallets that offer native mixing functionality, similar to 'CoinJoin' wallets like Wasabi. Criminals may also begin to use chain hopping as an alternative to third-party mixing, swapping types of cryptocurrency one for another in quick succession, most often at low-KYC exchanges, in order to obscure the movement of funds. In addition, privacy coins like Monero that increase user anonymity by using an obfuscated public ledger rather than a fully public one like Bitcoin's, may also become preferred currencies for criminals; exchanges that accept privacy coins 'will need to collaborate with regulators, law enforcement, and one another to establish frameworks for investigations of criminals who use privacy coins'. Finally, the criminal use of non-custodial, decentralized exchanges like the Bisq network, which allow peer-to-peer exchanges, will continue to grow. Criminals using such exchanges may also 'benefit from upcoming Bitcoin protocol changes like Taproot and Schnorr Signatures, which make the complicated smart contract-based transactions carried out on P2P exchanges look identical to standard transactions on the blockchain'.[63] This analysis of changing criminal practices using cryptocurrencies is consistent with those of international law enforcement agencies such as Europol. They are likely to make law enforcement investigations more complex.[64]

Policy Responses

Anti-Money Laundering and Counter-Terrorism Financing

[60] Bergeron, Décary-Hétu and Giommoni, 2020
[61] Federal Bureau of Investigations, 2019
[62] Chainanalysis, 2020b
[63] Chainanalysis, 2020b
[64] Europol 2020

A central plank of recent governmental responses to the use of cryptocurrencies in criminal activities has been to extend anti-money laundering and counter-terrorist financing legislation to exchanges and wallet providers. In the European Union, the 5th Anti-Money Laundering Directive (5AMLD) defines cryptocurrency exchanges and wallet providers who own private keys of their clients as obliged entities, mandating them, inter alia, to a proper identification of their clients. It defines cryptocurrency as a *"digital representation of value that can be digitally transferred, stored or traded and is accepted by natural or legal persons as a medium of exchange".* Each of the European Union's member states was required to transpose 5AMLD into domestic law by January 2020 and infraction proceedings have been launched by the European Commission against those that had not done so. Individual countries were given a large degree of flexibility when transposing the directive, but it has nonetheless contributed to harmonisation of legislation in the European Union.[65]

Law enforcement agencies believe will make crypto currencies less attractive and vulnerable to some criminals but may also increase the perceived legitimacy and use of virtual assets.[66] In practical terms, 5AMLD now means that crypto-fiat currency exchanges and crypto wallet providers are considered to be financial institutions, subject to the same anti-money laundering and counter-terrorism financing requirements as traditional financial institutions. They are legally required to register their businesses with public authorities in the EU and to implement transparent, Know-Your-Customer (KYC), Customer Due Diligence (CDD) and Suspicious Activity Reporting (SAR). They must pass identifiable user information, such as names and addresses, to Financial Intelligence Units if requested to do so.

At the global level, the Financial Action Task Force (FATF) is the inter-governmental body which sets international standards to prevent money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. Founded in 1987 by the G7 to combat money laundering and terrorist financing, it now has 39 members and a global network of nine regional bodies that extends its reach to 200 countries. In 2018, the FATF set out amendments to its global standards to place anti-money laundering and counter-terrorism financing requirements on virtual assets and virtual asset service providers (VASPs).[67] Its so-called 'travel clause' requires countries to ensure that:

> '(b) R.16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to beneficiary VASPs and counterparts (if any), and make it available on request to appropriate authorities. It is not necessary for this information to be attached directly to virtual asset transfers. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities. Other requirements of R.16 (including monitoring of the

[65] Europol, 2020: 18
[66] National Crime Agency, 2020
[67] FATF, 2020

> availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R.16.[68]

The FATF will also take action to blacklist countries that fail to implement crypto asset regulatory regimes. Blacklisting by the FATF has serious consequences, since it reduces access to the global financial architecture.[69]

Multilateral action to regulate cryptoassets and crypto asset providers has been matched by cooperation between law enforcement agencies – particularly in the major financial centres of the US, the EU and Japan. Cooperation between the public and private sectors is also critical to law enforcement strategies. In the USA, the Internal Revenue Service (IRS) has recently offered grants up to $625,000 to tech companies to help develop ways of tracing cryptocurrency transactions. Its goal is to develop transaction tracking tools, predictive analytics and new algorithms and source code that would enable IRS agents to keep their tracking capabilities up to date.[70]

Regulating Cryptocurrencies

The current regulatory environment for cryptocurrencies has been hampered by the "turf war" that has existed in the past between different regulatory and law enforcement agencies. An overview of the challenges facing the regulatory response to cryptocurrencies has been provided by Fletcher, Larkin and Corbet (2021), most usefully in Table 1 of that paper.[71] An exclusively US overview is provided by Hughes (2017), which is slightly outdated due to developments made by the new IC3 division of the FBI. [72]The US Library of Congress Global Legal Research Directorate has provided an international overview of the regulation of cryptocurrencies in their *Regulation of Cryptocurrency Around the World* (2018).[73] Similar attempts at a global overview of regulation exist from Chcohan (2019) on ICOs.[74] The work by the Library of Congress is slightly outdated, having only been compiled in 2018 with no obvious mechanism for continuous updating but it is, at present, the only global overview of the regulation and treatment of cryptocurrencies. The evolution of private law has created a domain where cryptocurrencies are in the process of creating a space for these new assets. The power of private law has been outlined by Pistor (2020) in

---

[68] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html

[69] Kfir, 2020

[70] Rautmare, 2020

[71] Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance*, *56*, 101387.

[72] Hughes, S. D. (2017). Cryptocurrency Regulations and Enforcement in the US. *W. St. UL Rev.*, *45*, 1.

[73] https://www.loc.gov/law/help/cryptocurrency/world-survey.php

[74] Chohan U.W. (2019) Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. In: Goutte S., Guesmi K., Saadi S. (eds) Cryptofinance and Mechanisms of Exchange. Contributions to Management Science. Springer, Cham. https://doi.org/10.1007/978-3-030-30738-7_10

creating new forms of property rights and the implications of carving out new public protections of the private sphere and the subsequent shifting of risk.[75] In the case of cryptocurrencies, this assignment of risk is a genuine concern. Zoli (2020) presents four options for regulatory responses on the part of governments:

> The first, and most extreme, approach would be to prohibit the activity itself and sanction those who exercise it, where the risk posed to society is considered unacceptable. It is already evident that in the case of crypto-assets, this approach will not be applied, as there are clear social benefits to crypto-assets.
>
> The second approach would be the introduction of a new regulatory regime which ensures that the risk is borne by those responsible for the activity within our legal system. The aim of such a new regulatory regime would be, first, to recognise the indigenous features of crypto-assets and their digital ecosystem; secondly, to identify existing legislative/regulatory barriers under EU and national law; and lastly, to harmonise existing practices or legislative regimes in order to ensure a level playing-field when it comes to legal certainty and investor protection. This is the approach that has been recently adopted by Chinese legislators. China has established three internet courts in Hangzhou, Beijing and Guangzhou. These courts will hear "internet-related cases" online, all of which are located in the most flourishing and prosperous area of China's internet industry.62 In September 2018, the Supreme People's Court ruled that evidence authenticated with Blockchain technology is considered binding in legal disputes, declaring that internet courts should recognise digital data that is submitted as evidence if relevant parties have collected and stored this data via Blockchain with digital signatures, reliable timestamps and hash value verification or via a digital deposition platform, and can prove the authenticity of such technology used.
>
> The third possible approach that could be applied by the legislator is a sort of "benign neglect", where activities are acknowledged but not regulated (this is applied to gambling debts in some jurisdictions, for example). Rights could not be enforced under this approach. Obligations arising from these activities would be "natural obligations": that is to say, the legal system does not recognise or support the enforcement of a certain obligation, but if the obligation is performed, the legal system will not allow a reversal of the transaction on the basis of unjust enrichment. The "benign neglect" approach could be applied to all relationships related to decentralised crypto-assets, as long as they do not jeopardise any important societal values.

[75] Pistor, K. (2020). *The code of capital: How the law creates wealth and inequality*. Princeton University Press.

> The fourth approach, which is often deployed on activities entailing a considerable amount of risk, would be to impose an insurance obligation on the network or their participants. This would address the difficulties in identifying a responsible actor (especially in a decentralised network) and demonstrating their negligence, and would allow the rights of individuals who have been deprived of their crypto-assets or have suffered other damages to be enforced.[76]

Over the past two years a greater degree of cooperation between US agencies and international law enforcement bodies has been manifest, as seen by Operation Wire Wire and Operation reWired. These operations, along with the continued policy coordination by the FATF are indicative of the transnational strategic response to cryptocurrencies and the speed at which law enforcement agencies are responding to the perceived risk of this new asset class.

Conclusion

Criminality has not changed but evolved to suit the new media available to criminals. To this effect, it is important to note that the Internet and cryptocurrencies are not, by definition, instruments of criminality, in the same way that the Ford V8 was not by definition a "bank robber's assistant" despite Bonnie and Clyde indicating a strong preference for that vehicle. These innovations have facilitated commerce and the development of new investment pathways as well as fostering new applications of these technologies that can be welfare improving for society.

This chapter has tried to highlight how traditional crimes of frauds, narcotics trafficking and theft have evolved to the new context of the Internet, facilitated by the creation of cryptocurrencies, reducing the overall transaction costs of illegal commerce and the moving of stolen funds. Laws and their enforcement are catching up with the changes in the digital marketplace but it is still traditional detective work in conjunction with ICT experts that has undone major criminal enterprises such as the Silk Road. The challenge ahead for law enforcement is to keep up with the "arms race" between law enforcement and criminal enterprises in the ICT space. This also includes state actors as well as non-state actors. In both circumstances, international coordination and cooperation is a necessary condition for success. The role of the FATF and coordinated action on the part of law enforcement agencies has been highlighted above and will need to develop further to protect investors and consumers as well as governments. The elevation of US Cyber Command to a unified combat command by President Obama in 2016 is indicative of the importance of cybersecurity in the future. It is only logical that cryptocurrencies and tokens become important to the strategic control of Cyberspace, a matter now of the utmost interest to central banks and international financial institutions and discussed elsewhere in this volume.

[76] Zilioli, C. (2020). Crypto-Assets: Legal Characterisation and Challenges under Private Law. *European Law Review April*.P 266.

References (Part II)

Federal Bureau of Investigations, Operation SaboTor, Federal Partnerships Key to Dismantling Online Drug Markets, 2019, accessed at https://www.fbi.gov/news/stories/j-code-operation-sabotor-032619

Bank for International Settlements (2018) 'BIS Annual Economic Report', https://www.bis.org/publ/arpdf/ar2018e5.pdf

Jamie Bartlett (2019) *Cryptoqueen: How this woman scammed the world, then vanished* https://www.bbc.co.uk/news/stories-50435014

Andreanne Bergeron, David Decary-Hetu and Luca Giommon (2020), Preliminary findings of the impact of COVID-19 on drugs crypto markets, International Journal of Drug Policy, 2020 Sep; 83: 102870. Published online 2020 Jul 30. doi: 10.1016/j.drugpo.2020.102870

Chainanalysis (2020a), *The KuCoin Hack: What We Know So Far and How the Hackers are Using DeFi Protocols to Launder Stolen Funds,* accessed at https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap

Chainanalysis (2020b) *The 2020 State of Crypto Crime*, accessed at https://go.chainalysis.com/2020-Crypto-Crime-Report.html

ENISA (2020), *Cryptojacking: ENISA Threat Landscape*, accessed at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cryptojacking

Europol (2020) *Internet Organised Crime Threat Assessment*, accessed at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

HM Treasury, FCA and Bank of England, (2018) *Cryptoassets Taskforce: Final Report*, accessed at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf

Isaac Kfir (2020) Cryptocurrencies, national security, crime and terrorism, *Comparative Strategy*, 39:2, 113-127, DOI: 10.1080/01495933.2020.1718983

Jessica Haworth (2020) What is Sodinokibi? The ransomware behind the Travelex attack, *The Daily Swig*, 14th January 2020, accessed at https://portswigger.net/daily-swig/what-is-sodinokibi-the-ransomware-behind-the-travelex-attack

National Crime Agency (2020) National Strategic Assessment of Serious and Organised Crime, accessed at https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file

Paquet-Clouston et al. (2019), Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem, *Advances in Financial Technology* (AFT19), accessed at https://arxiv.org/pdf/1908.01051.pdf

Kai Sedgwick (2018), 46% of Last Year's ICOs have already failed, Crowdfunding, *Bitcoin.com* accessed at https://news.bitcoin.com/46-last-years-icos-failed-already/