MEMORANDUM

ELLIPTIC | Center on Sanctions & Illicit Finance, FOUNDATION FOR DEFENSE OF DEMOCRACIES

BITCOIN LAUNDERING: AN ANALYSIS OF ILLICIT FLOWS INTO DIGITAL CURRENCY SERVICES

Yaya J. Fanusie and Tom Robinson | January 12, 2018

INTRODUCTION

Bitcoin,[1] the world's first cryptocurrency, long obscured with a reputation as a fringe economic phenomenon, has gone mainstream. The skyrocketing price in late 2017 has made Bitcoin a household name.[2] Proposed in a 2008 white paper by pseudonymous software developer Satoshi Nakomoto,[3] Bitcoin was an attempt to enable peer-to-peer "electronic cash" as an alternative to conventional banking in the wake of the global financial crisis. When released in 2009,[4] the digital currency had a value of less than one U.S. penny per "coin."[5] Now, just nine years later, one bitcoin recently almost reached $20,000,[6] and the cryptocurrency's market capitalization is over $200 billion.[7]

Criminals – often early adopters of new technologies – quickly appreciated that Bitcoin has unique properties that could potentially serve their interest in evading law enforcement.

Yaya J. Fanusie is the director of analysis for the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance (CSIF). Yaya previously spent seven years as both an economic and counterterrorism analyst in the CIA, where he regularly briefed White House-level policy makers, U.S. military personnel, and federal law enforcement. Dr. Tom Robinson is the Chief Data Officer and Co-Founder of Elliptic, the global leader in cryptocurrency forensics and anti-money laundering solutions. Tom has advised government, tax authorities and regulators on cryptocurrencies, and his forensics analysis of cryptocurrency transactions has been used to help secure the convictions of cybercriminals.

1. "Bitcoin" is capitalized when referring to the concept of Bitcoin or the Bitcoin network itself. It is not capitalized when used as a unit of account, e.g. "I sent her 10 bitcoins."
2. Peter Rudegeair and Akane Otani, "Bitcoin Mania: Even Grandma Wants In on the Action," The Wall Street Journal, November 29, 2017. (https://www.wsj.com/articles/bitcoin-mania-even-grandma-wants-in-on-the-action-1511996653)
3. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin, 2008. (https://bitcoin.org/bitcoin.pdf)
4. Satoshi Nakamoto, "Bitcoin v0.1 released," January 9, 2009. (https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html)
5. Samuel Gibbs, "Man buys $27 of bitcoin, forgets about them, finds they're now worth $886k," The Guardian (UK), December 8, 2015. (https://www.theguardian.com/technology/2015/dec/09/bitcoin-forgotten-currency-norway-oslo-home)
6. "Bitcoin (USD) Price," CoinDesk, accessed January 11, 2018. (https://www.coindesk.com/price/)
7. "Cryptocurrency Market Capitalizations," Coin Market Cap, accessed January 11, 2018. (https://coinmarketcap.com/currencies/bitcoin/)

Users of Bitcoin employ pseudonyms rather than names, and it can be transferred without intermediaries and across international borders as easily as sending an email. However, what we know about Bitcoin's illicit use is mainly based on anecdotal evidence, usually without supporting data, analysis of how it is used across geographical regions, or trends over time. While it is impossible to quantify exactly how much bitcoin is used illicitly, analyzing the laundering of bitcoins (where it can be identified) gives insight into criminals' methods for hiding their illicit proceeds.

To provide a more rigorous assessment of Bitcoin and its use in illicit finance, the Center on Sanctions and Illicit Finance, a program at the Foundation for Defense of Democracies, teamed up with Elliptic, a cryptocurrency analytics provider, to study Bitcoin blockchain data and illicit inflows into digital currency services. This study provides insights for policymakers and financial industry leaders who want to better understand illicit finance risks arising from Bitcoin and formulate ways to enhance Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) compliance among cryptocurrency businesses.

A glossary is provided at the end of this document to define unique terms, concepts, and entities relating to the cryptocurrency industry found in this report.

OVERVIEW OF FINDINGS

Through extensive analysis of a narrow data sample of Bitcoin transactions between 2013 and 2016, this study identifies trends in the flow of bitcoins from clearly identified illicit activity to various digital currency conversion services.1 The parameters of the study were purposefully narrow to keep the data manageable, which likely minimized the volume of illicit bitcoins considered for analysis. The amount of observed Bitcoin laundering was small (less than one percent of all transactions entering conversion services), but what is most relevant are the clear patterns we discovered relating to how illicit bitcoins are laundered.

We found that darknet marketplaces such as Silk Road and, later, AlphaBay, were the source of almost all of the illicit bitcoins laundered through conversion services that we identify in our study. Bitcoin exchanges received the greatest amount of identified illicit bitcoins out of all conversion services, but they also processed the majority of Bitcoin transactions overall. The conversion services with the highest proportion of Bitcoin laundering within their platforms were mixers and online gambling sites.

Looking at geographic patterns, conversion services based in Europe received the greatest share of illicit bitcoins out of identifiable regions, more than five times as much as North American services. And while Asian conversion services processed the highest share of all incoming Bitcoin transactions in 2015 and 2016, they accounted for a disproportionately small share of Bitcoin laundering during those years. Lastly, a large percentage of conversion services that receive illicit bitcoins appear to conceal their country of operations, making it a challenge to identify the legal jurisdictions responsible for their AML enforcement.

1. Platforms where users convert bitcoin to fiat currency (a bitcoin exchange) or another cryptocurrency (a crypto-exchange) or move the bitcoins to another Bitcoin address accessible to the user. This results in a flow of funds that cannot be viewed or traced directly on the public blockchain. A glossary of definitions is included at the end of the report.

PURPOSE OF THE STUDY

This study aimed to identify where individuals turn in order to cash out or transmit bitcoins (BTC) acquired from illicit entities and to discover typologies for criminals "laundering" bitcoins. A true person-to-person payment using bitcoins will leave a record of that transaction and the addresses involved (analogous to account numbers) in the blockchain. This record can be an effective tool for law enforcement. Therefore, for the purpose of the study, we focus on those platforms and intermediaries that transmit funds on behalf of users by either cashing out bitcoins to a legal tender fiat currency, converting them to another cryptocurrency, or transmitting them to another Bitcoin address in such a way that the flow of funds cannot be viewed and traced directly on the blockchain. We call these platforms "conversion services" and they include virtual currency exchanges, mixers, online gambling sites that accept cryptocurrency, Bitcoin ATMs, and other services.

Money laundering has a precise legal definition which must be adapted for the cryptocurrency context. The U.S. Treasury's Financial Crimes Enforcement Network (FinCen) defines money laundering as the three-step process of making "illegally-gained proceeds (i.e. 'dirty money') appear legal (i.e. 'clean')," by 1) placing dirty money in the legitimate financial system, 2) layering it within additional transactions to obfuscate its origins, and 3) integrating it into the financial system with more transactions so the funds appear licit.2

While legal opinions differ on whether bitcoins technically constitute money,3 we assume in this study that when an individual moves bitcoins from an address associated with illicit activity to a new address, in a way that obscures the original source of funds, or cashes out to fiat currency, it indicates the intent to "cleanse" the bitcoins from their illegal origins. Hence the term "Bitcoin laundering." This form of laundering is not perfectly analogous to fiat currency money laundering because "cleansing" funds in the Bitcoin blockchain requires fewer steps. Moreover, there is not a separate legitimate financial system in which dirty bitcoins are laundered – unless they are cashed out into fiat. Much of the placement, layering, and integration all occurs within one financial ecosystem – Bitcoin.

Still, this study has implications for the formal financial sector. Financial institutions should assess whether they are indirectly enabling money laundering through cryptocurrencies. Compliance professionals assessing financial crime risk should take into account flows of funds originating from cryptocurrencies, both directly and indirectly, and make use of blockchain analysis techniques to verify this risk. The risk is particularly acute for those financial institutions that are providing banking services to cryptocurrency businesses, such as exchanges.

METHODOLOGY

To identify bitcoins moving from illicit entities to conversion services, we used Elliptic's forensic analysis tool, which combines public blockchain data with a proprietary dataset of Bitcoin addresses associated with known entities, to provide visibility into who is transacting with whom in Bitcoin. We reviewed transaction data between 2013 and 2016. We aggregated total volume of bitcoins going into conversion services and also identified the amounts coming directly from addresses flagged by Elliptic as belonging to illicit entities, such as various types of darknet marketplaces, ransomware, and fraudulent activities.

---

2. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "History of Anti-Money Laundering Laws," accessed November 29, 2017. (https://www.fincen.gov/history-anti-money-laundering-laws)

3. Steven Porter, "US judge rules that Bitcoin counts as money," The Christian Science Monitor, September 20, 2016. (https://www.csmonitor.com/Business/2016/0920/US-judge-rules-that-Bitcoin-counts-as-money)

Our study examines transaction data to determine to what extent conversion services are the direct recipients of proceeds of illicit activity, and which of these services are most popular: We observed 214 unique conversion services, including virtual currency exchanges, gambling sites, and mixers (see Table 1). We considered 102 illicit entities and placed them into 6 categories (see Table 2). No private consumer data was accessed during this study. All information came through Elliptic's forensic analysis of the public Bitcoin blockchain, and other public information.

LIMITATIONS

This study considers well over half a million bitcoins that moved directly from illicit sources to conversion services in the period 2013-2016. This is not intended to be a comprehensive overview of this type of activity, as we have not sought to identify all illicit sources of bitcoins. However, it covers the majority of known, significant entities of this type.

We have only considered Bitcoin flows directly from illicit entities to conversion services in order to simplify the analysis. Large volumes of illicit funds may pass through intermediate, unidentified entities before being sent to conversion services; however, the focus of this study was not to capture the totality of illicit Bitcoin transactions, but to track the transactions flowing directly from addresses associated with known illicit actors to conversion services. The data set of illicit transactions does not include flows which may originate from intermediary addresses.

Our data should not be interpreted to assess or estimate the full amount of illicit Bitcoin transactions which may have occurred on the Bitcoin blockchain. The actual volume of illicit Bitcoin transactions is almost surely to be significantly larger than represented in our sample.

TABLE 1

NUMBER OF CONVERSION SERVICES CONSIDERED, BY TYPE	
Bitcoin ATM Operator	1
Bitcoin Exchange	120
Crypto-Exchange	14
Gambling Service	60
Mixer	8
Multi-Service	11
Grand Total	214

TABLE 2

NUMBER OF ILLICIT ENTITIES CONSIDERED, BY TYPE	
Bitcoin ATM Operator	1
Bitcoin Exchange	120
Crypto-Exchange	14
Gambling Service	60
Mixer	8
Multi-Service	11
Grand Total	214

BITCOIN LAUNDERING TRENDS 2013-2016

ILLICIT ENTITIES GROWING

The number of illicit entities observed sending bitcoins to conversion services has risen over time. From Table 3, we see a five-fold increase in the number of significant illegal entities operating between 2013 and 2016.

TABLE 3

NUMBER OF ILLICIT ENTITIES CONSIDERED, BY TYPE					
	2013	2014	2015	2016	Total Unique Entities
Darknet Marketplace	5	9	18	16	30
Darknet Services	2	1	2	4	6
Darknet Vendor	1	3	7	13	16
Fraud Activity	2	11	11	10	26
Ponzi Scheme	0	3	1	2	5
Ransomware	2	5	7	15	19
Grand Total	12	32	46	60	102

DARKNET MARKETS ARE KEY SOURCE OF ILLICIT FUNDS

Illicit activity originated overwhelmingly from darknet marketplaces, as can be seen below in Table 4. Examples of darknet marketplaces, which became popular sites to buy and sell illegal drugs and a multitude of other illicit items and services, are Silk Road, shut down in 2013, and AlphaBay, shut down in July 2017.[11]

TABLE 4

ORIGIN OF ILLICIT BITCOINS ENTERING CONVERSION SERVICES, BY ILLICIT ENTITY TYPE					
	2013	2014	2015	2016	All years
Darknet Marketplace	99.44%	97.51%	98.43%	80.42%	97.36%
Darknet Services	0.03%	0.41%	0.00%	0.06%	0.11%
Darknet Vendor	0.00%	0.01%	0.21%	0.63%	0.12%
Fraud Activity	0.08%	1.84%	0.20%	0.86%	0.60%
Ponzi Scheme	0.00%	0.02%	0.27%	2.28%	0.25%
Ransomware	0.44%	0.22%	0.89%	15.75%	1.56%
Grand Total	100%	100%	100%	100%	100%

11. Andy Greenberg, "The Biggest Dark Web Takedown Yet Sends Black Markets Reeling," Wired, July 14, 2017. (https://www.wired.com/story/alphabay-takedown-dark-web-chaos/)

Only a small number of entities account for the majority of illicit activity in our sample. Nine of the 102 illicit entities were the source of more than 95 percent of all laundered bitcoins in our study. All nine were darknet marketplaces. Table 5 shows their activity from 2013-16. In 2016, a rise in bitcoins laundered from ransom and Ponzi schemes came from the Locky RansomWare attack[11] and the OneCoin scheme,[12] respectively, signaling an increase in this type of activity that continued into 2017.

TABLE 5

ORIGIN OF ILLICIT BITCOINS ENTERING CONVERSIONS SERVICES: LARGEST SOURCES					
Name	2013	2014	2015	2016	All Years
Abraxas	-	0.00%	8.99%	-	3.00%
Agora	0.02%	42.43%	47.89%	0.05%	26.30%
AlphaBay	-	0.00%	9.38%	46.65%	6.26%
Evolution	-	8.35%	10.09%	-	5.40%
Middle Earth Marketplace	-	0.05%	5.59%	-	1.88%
Nucleus Market	-	0.01%	13.6%	31.21%	6.63%
Sheep Marketplace	8.42%	-	-	-	3.00%
Silk Road	89.89%	-	-	-	32.03%
Silk Road 2.0	1.03%	40.50%	-	-	10.21%
Total	99.37%	91.35%	95.54%	77.92%	94.70%

As can be seen in Table 5, almost all of the illicit funds in our sample came from one or two of these nine sources in most years. For example, in 2013, 89.89 percent of all illicit funds in our sample came from the Silk Road darknet marketplace (shut down by law enforcement in 2013). 2016 represents the low point of the sample, with only 78 percent of money laundering coming from these nine marketplaces. The criminal ecosystem for Bitcoin was becoming less dominated by a few key players. This is likely due to the shutdown of popular darknet drug sites like Agora and Evolution,[3] as well as to the broader dispersal of illicit sources in our study

EXCHANGES, MIXERS, AND GAMBLING SITES ARE NOTABLE LAUNDERING DESTINATIONS

In 2016, Bitcoin exchanges received over 50 percent of the bitcoins entering conversion services from AlphaBay, the most popular darknet marketplace active during that year (see Table 6).

11. "Three US hospitals hit by ransomware," BBC News (UK), March 23, 2016. (http://www.bbc.com/news/technology-35880610)
12. Samburaj Das, "UK Authority Warns Against Using OneCoin," CryptoCoinsNews (Norway), September 27, 2016. (https://www.cryptocoinsnews.com/uk-authority-warns-using-onecoin/)
3. Andy Greenberg, "Agora, the Dark Web's Biggest Drug Market, Is Going Offline," Wired, August 26, 2015. (https://www.wired.com/2015/08/agora-dark-webs-biggest-drug-market-going-offline/)

TABLE 6

DISTRIBUTION OF LAUNDERED BITCOINS ORIGINATING FROM ALPHABAY, BY CONVERSION SERVICE TYPE			
	2015	2016	All years
ATM	0.07%	0.07%	0.07%
Bitcoin Exchange	56.39%	52.05%	54.22%
Crypto-Exchange	0.70%	0.48%	0.59%
Gambling	26.63%	13.59%	20.11%
Mixer	7.89%	28.99%	18.44%
Multi-Service	8.32%	4.82%	6.57%
Grand Total	100.00%	100.00%	100.00%

As Bitcoin exchanges are the services with the highest volume of Bitcoin activity in general, they unsurprisingly account for the largest share (45 percent) of total Bitcoin volume laundered during the four years (see Table 7).

TABLE 7

DISTRIBUTION OF LAUNDERED BITCOINS, BY CONVERSION SERVICE TYPE					
	2013	2014	2015	2016	All years
ATM	0.00%	0.00%	0.03%	0.05%	0.01%
Bitcoin Exchange	61.79%	23.22%	41.34%	59.40%	45.43%
Crypto-Exchange	0.17%	0.32%	0.64%	0.30%	0.37%
Gambling	10.86%	43.48%	31.56%	12.21%	25.79%
Mixer	24.97%	26.54%	19.27%	24.20%	23.40%
Multi-Service	2.20%	6.44%	7.16%	3.84%	5.00%
Grand Total	100.00%	100.00%	100.00%	100.00%	100.00%

According to our study, the total percentage of identified "dirty bitcoins" going into conversion services was relatively small. Only 0.61 percent of the money entering conversion services during the four years analyzed were verifiably from illicit sources, with the highest proportion (1.07 percent) seen in 2013 (see Table 8). As mentioned in "Limitations," the 0.61 percent figure should be considered a lower-bound estimate, as we are unlikely to have identified all illicit activity in Bitcoin. The true percentage of Bitcoin laundering is likely to be higher.

Bitcoin exchange services received roughly 75 percent of all incoming (licit and illicit) Bitcoin entering conversion services in our study. Although mixers account for a small amount of Bitcoin transactions, they have a higher propensity to being used for laundering bitcoins. From 2013-15, over 20 percent of mixers' incoming transactions came directly from illicit sources, with a sharp drop in 2016 that mirrored an across-the-board decline in the proportion of illicit transactions in our study (see Table 8). It is likely that illicit bitcoins fell as a percentage of total volume entering conversion services due to the cryptocurrency's increasing popularity as a speculative investment as well as new laundering techniques. The drop may also reflect better AML/CFT compliance by conversion services, including the use of blockchain analysis services to determine customers' source of funds.

TABLE 8

PERCENTAGE OF ALL INCOMING TRANSACTION VOLUME ORIGINATING FROM ILLICIT ENTITIES, BY CONVERSION SERVICE TYPE					
	2013	2014	2015	2016	All years
ATM	-	0.07%	0.02%	0.02%	0.02%
Bitcoin Exchange	1.01%	0.37%	0.34%	0.09%	0.37%
Crypto-Exchange	0.17%	0.06%	0.09%	0.00%	0.04%
Gambling	0.69%	3.76%	3.58%	0.57%	2.01%
Mixer	22.57%	29.26%	24.07%	2.81%	16.03%
Multi-Service	0.15%	0.45%	0.46%	0.06%	0.28%
Grand Total	1.07%	1.04%	0.64%	0.12%	0.61%

GEOGRAPHICAL BREAKDOWN

Our study accounts for incoming transactions to conversion services from five continents, Oceania, and unknown jurisdictions. We used "unknown" when it was not possible to identify the service's home country of operations. Some of these services may have concealed their home base locations intentionally. Though services often have offices and operations in multiple countries, our study considers country of incorporation or the acknowledged headquarters office to specify the service's jurisdiction.

HIGHER LAUNDERING AMOUNTS IN EUROPE AND UNSPECIFIED JURISDICTIONS

The highest amounts of bitcoins were consistently laundered through conversion services domiciled in unknown jurisdictions (see Table 9). In the identified jurisdictions, European conversion services received the highest numbers of illicit bitcoins. There appeared to be relatively little going into conversion services domiciled in Africa.

TABLE 9

ILLICIT PERCENTAGE OF INCOMING TRANSACTIONS TO CONVERSION SERVICES, BY REGION					
	2013	2014	2015	2016	All years
Africa	-	-	0.01%	0.00%	0.00%
Asia	0.28%	0.02%	0.02%	0.00%	0.05%
Europe	1.35%	0.52%	0.88%	0.30%	0.77%
North America	0.39%	0.39%	0.41%	0.03%	0.26%
Oceania	0.07%	0.67%	1.35%	0.40%	0.97%
South America	0.17%	0.07%	0.18%	0.04%	0.11%
Unkown	2.24%	5.28%	4.90%	0.91%	3.19%
Grand Total	1.07%	1.04%	0.64%	0.12%	0.61%

By comparing the percentage of all transactions versus the percentage of illicit transactions going through services on each continent, we can get a sense of where there may be an outsized proportion of illicit activity. In Tables 10 and 11, Asia dominates the conversion service usage in 2015-16 (with over half of our transactions going through conversion services in Asia in those years). However, only 1.61 percent and 1.21 percent of all laundering went through Asia in those years. Thus, though most bitcoins were entering Asian conversion services (within which, China dominates) in those years, only a very small proportion of illicit bitcoins appears to have been laundered there. One plausible explanation for this may be that capital controls in China, in particular, restrict the ability to move fiat currency out of the country, making Chinese conversion services less attractive for transferring illicit funds.

The same cannot be said of Europe. Roughly a quarter of all incoming transactions went into Europe in 2015 and 2016, but 38 percent and 57 percent of all illicit transactions, respectively, went to European services during those years. Thus, Europe hosted a disproportionate amount of illicit activity.

TABLE 10

DISTRIBUTION OF TOTAL BITCOIN VOLUME INTO CONVERSION SERVICES, BY REGION					
	2013	2014	2015	2016	All years
Africa	0.00%	0.00%	0.09%	0.26%	0.11%
Asia	27.59%	21.95%	52.07%	52.56%	42.97%
Europe	34.37%	43.91%	27.81%	22.86%	29.76%
North America	17.27%	19.95%	12.85%	19.14%	16.88%
Oceania	0.00%	0.14%	0.22%	0.11%	0.13%
South America	0.13%	0.20%	0.24%	0.22%	0.20%
Unkown	20.64%	13.86%	6.72%	4.85%	9.94%
Grand Total	100.00%	100.00%	100.00%	100.00%	100.00%

European and unknown jurisdictions combined account for a roughly constant proportion of the overall Bitcoin laundering activity, between 86 and 93 percent (see Table 11).

Fewer than 10 percent of all transactions overall passed through unknown jurisdictions (Table 10), while 52 percent of illicit laundering went through them (Table 11). While 43 percent of all transactions went through Asia, only 3 percent of all illicit transactions went through Asia.

TABLE 11

DISTRIBUTION OF ILLICIT BITCOIN VOLUME INTO CONVERSION SERVICES, BY REGION					
	2013	2014	2015	2016	All years
Africa	0.00%	0.00%	0.09%	0.00%	0.00%
Asia	7.14%	0.51%	1.61%	1.21%	3.29%
Europe	43.31%	21.90%	38.31%	56.65%	37.33%
North America	6.26%	7.42%	8.19%	5.28%	7.12%
Oceania	0.00%	0.09%	0.47%	0.35%	0.20%
South America	0.02%	0.01%	0.07%	0.07%	0.04%
Unkown	43.27%	70.07%	51.36%	36.44%	52.03%
Grand Total	100.00%	100.00%	100.00%	100.00%	100.00%

HIGH-RISK CONVERSION SERVICES

Through the study, it is clear that certain types of conversion services have higher propensities to receive bitcoins from illicit sources, making them higher AML risks. In general, mixers and online gambling sites have the biggest bitcoin laundering problem – they process far and away the highest proportion of dirty bitcoins (see Table 8).

Mixers have consistently processed about a quarter of incoming illicit bitcoins per year. The proportion laundered through exchanges and gambling combined has been roughly constant (66 to 72 percent). Of note, Bitcoin exchanges processed 45 percent of laundered bitcoins, but, as they received much higher volumes, a much lower proportion of their activity is illicit (see Table 7).

Looking deeper at mixers and gambling sites, we found that 97 percent of all illicit volume in these two categories is being laundered through just three mixing or gambling services. These same three destinations alone account for almost half of all Bitcoin laundering (comprising most of the volume going into mixers and gambling sites noted in Table 7). One particular service, Helix, became the dominant mixer for Bitcoin laundering by 2016.

Lastly, the exchanges represent another major part of the picture. Our study identified that two EU-based Bitcoin exchanges account for 50 percent of all bitcoins laundered through exchanges, while the remaining 118 exchanges account for the other 50 percent.

SUMMARY

Our study, the first of its kind, indicates that while most types of conversion services have received some bitcoins from illicit activity, the vast majority of the funds they receive do not appear to be illicit. However, two types of services in particular – mixers and online gambling services – do receive a high proportion of illicit bitcoins and thus, are significant concerns for Bitcoin laundering.

It is noteworthy that conversion services based in Europe tend to receive higher rates of illicit bitcoins compared to other regions. Also, it is apparent that services which appear to hide their location have high rates of Bitcoin laundering activity.

RECOMMENDATIONS

The growth of cryptocurrencies and their associated technologies provides great opportunities for firms to develop new business models, for governments to build more efficient and secure information systems, and for the financial inclusion of billions of people who lack easy access to the conventional banking system. Cryptocurrency and blockchain technology represent, potentially, a net positive economic and social gain. At the same time, laundering of cryptocurrencies is a new type of illicit finance methodology. If this new financial technology is going to fulfill its potential, its accompanying illicit risks will have to be managed, as has been done for other types of payment methods that now flourish, such as checks, credit cards, PayPal, etc. The following recommendations are ways in which government officials and members of industry can help to mitigate risk as cryptocurrency adoption rises:

- Financial authorities in all jurisdictions must increase AML enforcement of mixers and online gambling sites. The key to addressing the pattern of Bitcoin laundering observed in this study is for financial authorities to investigate the poor Anti-Money Laundering and Know Your Customer (AML/KYC) practices by businesses transmitting funds without licensure or regulatory compliance. The fact that most mixers and gambling sites hide their location of operations indicates they probably seek to evade the basic regulations in place to uphold transparency and financial integrity standards in most jurisdictions. Since a handful of specific mixers and gambling sites accounted for 97 percent of the Bitcoin laundering on these platforms, targeting them should be a priority for law enforcement. And even when mixers and gambling sites do not publicize their jurisdictions or ownership, investigators can use website domain analysis as well as Bitcoin blockchain forensics to identify the probable owners and administrators of these sites.

- European virtual currency exchanges must improve AML practices. Exchanges transmitting cryptocurrency in Europe should set up stronger procedures to verify customers' identities and the sources of their funds. European regulators must bring Bitcoin businesses, such as exchanges, within the scope of AML legislation. Many large European Bitcoin exchanges do implement robust AML policies. However, this is out of choice rather than obligation, and there are some who choose not to, possibly to attract business from criminals. Although illicit bitcoins are a very small portion of bitcoins received by conversion services overall, Europe had the greatest exposure to laundering, after unknown jurisdictions. Of all the illicit bitcoins entering European conversion services, most were received by exchanges. The EU is tackling this by updating its 2015 Anti-Money Laundering Directive so that its regulations cover virtual currency exchanges and custodian wallet services, but even the updated language has loopholes that could permit significant cryptocurrency laundering. For example, the proposed language extends AML regulatory coverage to "providers engaged in exchange services between virtual currencies and fiat currencies"[1] but does not specify services which may only process transactions between different types of cryptocurrencies. The EU should include "crypto-to-crypto" exchanges under its AML Directive, which would help address the risks which come from people swapping bitcoins for more anonymous cryptocurrencies.

1. Council of the European Union, "Interinstitutional file:2016/0208 (COD)," December 19, 2017, page 52. (http://data.consilium.europa.eu/doc/document/ST-15849-2017-INIT/en/pdf)

- Law enforcement should not only target darknet websites, it should expose their vulnerabilities. Shutting down such sites and prosecuting their administrators is not a sufficient long-term approach to combating darknet commerce. Typically, new underground sites arise to take their places and inherit their users. The shutdown1 of the AlphaBay and Hansa darknet marketplaces in mid-2017 was in many ways déjà vu, reminiscent of the Silk Road takedown a few years prior. Darknet marketplace disruptions are temporary. Law enforcement should increase customer skepticism about sites' integrity and reduce the perceived security of such platforms by exposing their vulnerabilities publicly. Moreover, the anonymity of these marketplaces gives some cover to police presence and allows them to interact with users. While those users often feel confident operating on the darknet, awareness of lurking law enforcement may increasingly discourage users and reduce the revenue potential of these marketplaces.

- Jurisdictions with established virtual currency AML regulations should share lessons learned with emerging ones. In our study, Asia showed very little Bitcoin laundering despite significant cryptocurrency activity. Africa had very little licit or illicit conversion service activity. Yet, it should not be expected that low rates of Bitcoin laundering will remain low as these markets grow. To mitigate the rise of illicit activity as virtual currency businesses pop up in newer jurisdictions, financial authorities in Europe and the U.S. should meet with their African, Asian, and South American counterparts to learn about their experiences and share best practices. The U.S. Treasury's Financial Crimes Enforcement Network issued guidance in 2013 that brought Bitcoin exchanges in the U.S. under the same financial regulatory guidelines of Money Service Business,2 a model which other jurisdictions should emulate because of the relatively low levels of Bitcoin laundering among North American conversion services. International bodies can support this. For example, the Egmont Group, the informal global network of national Financial Intelligence Units, should reinforce these lessons among its membership. Europol has hosted four conferences looking at the law enforcement implications of virtual currencies,3 mostly attended by EU officials. Outreach should be extended to countries who are in many ways "starting from scratch" in developing basic AML guidelines for the nascent cryptocurrency industry in their countries.

- The U.S. Congress should mandate a National Commission for Digital Currency Preparedness and help develop a national blockchain technology innovation strategy. U.S. officials should be thinking ahead about how this financial technology (fintech) innovation will impact U.S. activity within the global financial system. In addition to mitigating illicit finance risks like criminal money laundering, there will likely be a need to develop strategies to counter state actors aiming to use cryptocurrencies to circumvent U.S., EU, and UN sanctions.4 The commission should study such risks, but also identify opportunities to fully leverage fintech positively for greater economic efficiency and global financial inclusion. The commission's study should inform a broader U.S. strategy for blockchain technology innovation.

---

1. Nathaniel Popper and Rebecca Ruiz, "2 Leading Online Black Markets Are Shut down by Authorities," The New York Times, July 20, 2017. (https://www.nytimes.com/2017/07/20/business/dealbook/alphabay-dark-web-opioids.html)
2. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "FinCen Issues Guidance on Virtual Currencies and Regulatory Responsibilities," March 18, 2013. (https://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities)
3. EUROPOL, "Europol Hosted 4th Conference On Virtual Currencies," July 5, 2017. (https://www.europol.europa.eu/newsroom/news/europol-hosted-4th-conference-virtual-currencies)
4. Nathaniel Popper, Oleg Matsnev, and Ana Vanessa Herrero, "Russia and Venezuela's Plan to Sidestep Sanctions: Virtual Currencies," The New York Times, January 3, 2018. (https://www.nytimes.com/2018/01/03/technology/russia-venezuela-virtual-currencies.html)

CONCLUSION

Because cryptocurrencies are based on easily downloadable, open-source software and a decentralized network, it is unlikely that they will disappear as a digital method of payment option in the near future. Alternative payment methods bring new illicit finance risks when they are introduced to the public, but survive and eventually flourish when safeguards develop to address (but never fully eliminate) their criminal use. Credit cards, online banking, wire transfers, and cash transactions all have been and continue to be used for crime. Academic researchers and government analysts should study the history of legacy payment methods, derive lessons learned, and articulate a framework for how financial regulators should approach risk mitigation. Such research should be consulted by leading thinkers in the cryptocurrency industry, as well as compliance professionals who can best translate a strategic framework into best practices for industry firms.

Bitcoin is the first cryptocurrency, not the only one. In recent years, developers have created new cryptocurrency protocols, such as Zcash, Monero, and Dash, with privacy features that make them more difficult to track using blockchain analysis techniques. Monero, in particular, is seeing increased adoption on darknet markets.1 Better privacy may be a critical feature for legal cryptocurrency use to grow, but this must be balanced with the need for law enforcement to be able to trace transactions in some circumstances.2 In the coming years, cyber crime law enforcement should acquire the technological expertise to combat their illicit use, and regulators should understand the risks posed by this emerging class of more anonymous cryptocurrencies.

1. Rachel Rose O'Leary, "Europol Warns Zcash, Monero and Ether Playing Growing Role in Cybercrime," CoinDesk, October 3, 2017. (https://www.coindesk.com/europol-warns-zcash-monero-and-ether-playing-growing-role-in-cybercrime/)
2. Lalita Clozel, "How Zcash Tries to Balance Privacy, Transparency in Blockchain" American Banker, October 31, 2016. (https://www.americanbanker.com/news/how-zcash-tries-to-balance-privacy-transparency-in-blockchain)

ACKNOWLEDGEMENTS

We wish to thank the following people for their constructive input and suggestions on this report: Luke Sully, Shane Shook, and Peter Van Valkenburgh. We are also grateful to David Adesnik, Simone Maini, David Murray, Jonathan Schanzer, Juan Zarate, and Boris Zilberman for substantive edits which helped refine our argument. We would like to thank Abu Adan and Alex Entz for assistance in compiling and analyzing the data set, and Alexandra Gutowski for helping with data visualization. We would like to thank Nicole Salter for copy edits that helped tighten our prose and Erin Blumenthal for her hard work and creative input during production. Also thanks to interns Benjamin Brown and Katie Miedema for assistance throughout the research and drafting process.

DEFINITIONS

Bitcoin Address
A public identifier that takes the form of a long string of alphanumeric digits used to send, receive, and store bitcoins. Because the Bitcoin blockchain is public, anyone with access to the internet can view the balances of Bitcoin addresses and their transaction activity. The owners of the addresses are not always known, but they can sometimes be identified through outside information or blockchain analysis. One user of bitcoin will typically have several Bitcoin addresses with which they receive and send payments, and a Bitcoin wallet, which may be software or a service, will generate addresses, keep track of all generated addresses, and handle security.

Blockchain
A public digital ledger that records verified cryptocurrency transactions. In the case of the Bitcoin blockchain, it lists Bitcoin transactions.

Conversion Services
Platforms where users convert bitcoins to fiat currency (a Bitcoin exchange) or another cryptocurrency (a crypto-exchange) or move the bitcoins to another Bitcoin address accessible to the user. This results in a flow of funds that cannot be viewed or traced directly on the public blockchain.

CONVERSION SERVICE TYPES

Bitcoin ATM Operator
Operators of physical machines that enable the conversion between bitcoins and cash.

Bitcoin Exchange
Online platforms enabling the exchange of bitcoins for fiat currencies.

Crypto-Exchange
Online platforms enabling the exchange of bitcoins for other cryptocurrencies.

Gambling Service
Online gambling services where wagers and payouts are paid in bitcoins. It is often possible to use these services anonymously and limits are not imposed, providing the opportunity to use them to launder funds.

Mixer
An online software service that will swap your bitcoins for ones with a different transaction history – effectively laundering them. Mixers are typically operated anonymously through the darknet.

Multi-Service
Online platforms that offer a range of Bitcoin services, including storage and Bitcoin/fiat brokerage

ILLICIT ENTITY TYPES

Darknet Marketplace
Online marketplaces (usually operating via darknets such as Tor or I2P) connecting buyers with sellers of illicit goods and services, with Bitcoin as the primary means of payment

Darknet Services
Illicit darknet services accepting payments in bitcoins.

Darknet Vendor Shop
Online marketplaces (usually operating via darknets such as Tor or I2P) connecting buyers with a single seller of illicit goods and services, with Bitcoin as the primary means of payment

Fraud Activity
Thefts, scams and other activities involving deceptive practices.

Ponzi Scheme
An investment scheme where investors are promised high rates of return with little risk, where the scheme's facilitators take newcomers' investments and pass along as profits to the earlier investors.

Ransomware
Malware that restricts access to computer systems and demands a Bitcoin payment.

Elliptic is the global leader in detecting and investigating cybercrime involving cryptocurrencies. Elliptic's technology has enabled key advances in investigations into dark marketplace activity, ransomware and cyber extortion, providing evidence that has led to convictions. We also enable companies handling bitcoin to meet their anti-money laundering obligations, by allowing them to confidently perform AML transaction screening.

For more information, please visit www.elliptic.co.

FDD's Center on Sanctions and Illicit Finance (CSIF) provides policy and subject matter expertise in areas of illicit finance, financial power, and economic pressure to the global policy community.

CSIF seeks to illuminate the critical intersection between the full range of illicit finance and national security, including money laundering, terrorist financing, sanctions evasion, proliferation financing, cyber crime and economic espionage, and corruption and kleptocracy. This includes understanding how America can best use and preserve its financial and economic power to promote its interests and the integrity of the financial system. The Center also examines how America's adversaries may be leveraging economic tools and power. For more information, please visit www.defenddemocracy.org/csif.