An Analysis of Bitcoin's Use in Illicit Finance

By Michael Morell
with Josh Kirshner and Thomas Schoenberger

April 6, 2021

Preface

New technologies almost always come with both significant benefits for society as well as negative externalities. It is the role of government officials to make policy that allows the benefits to flourish while protecting us from the downsides. As I saw firsthand in my 33-year career at the Central Intelligence Agency, the process our government uses to get this balance right can often be frustratingly slow, but it has ultimately and typically met the challenge.

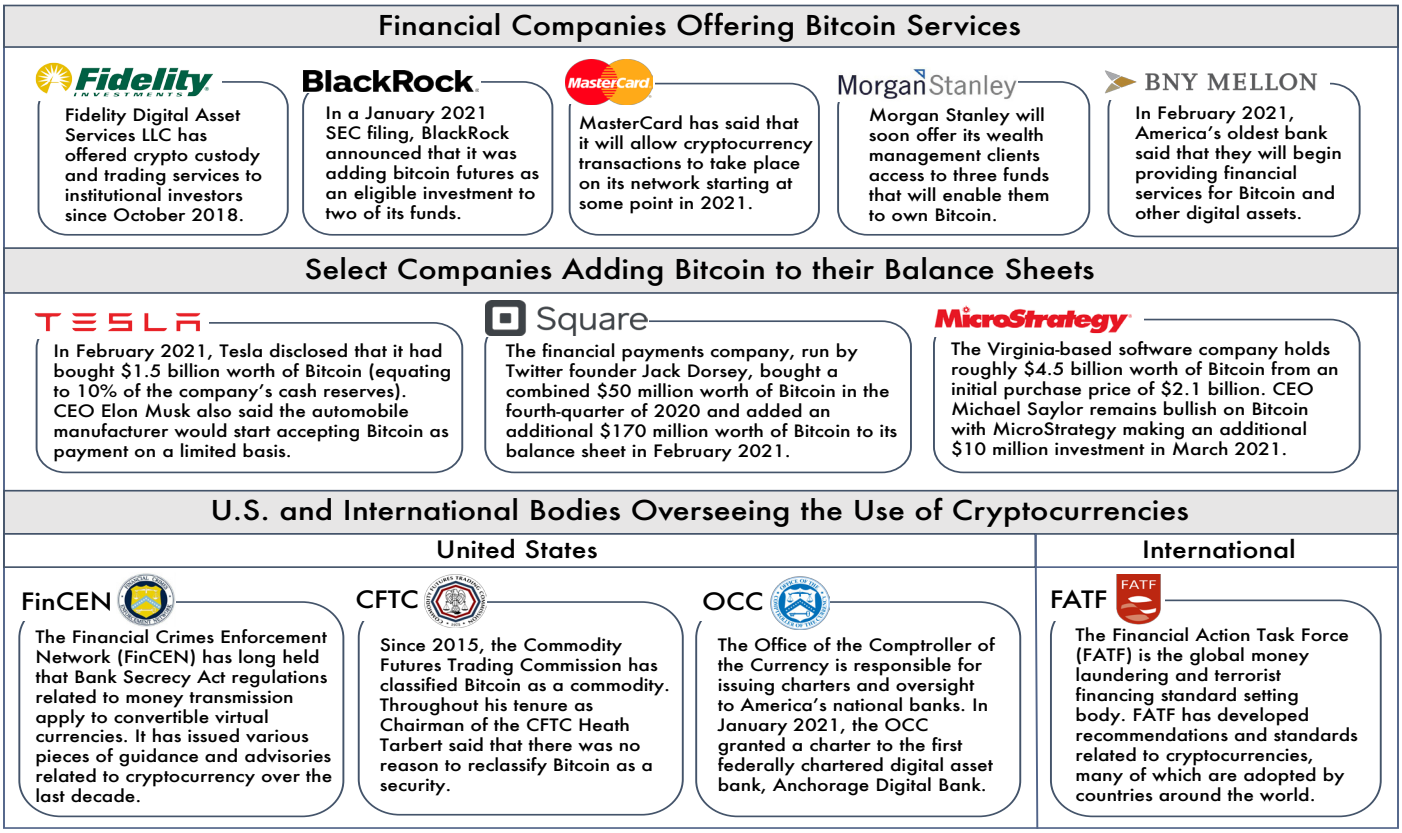
One example is how our government has adjusted to technological advances in financial and payment networks while simultaneously safeguarding vital systems. Online banking was introduced in 1994, but it was not until 1999, with passage of the Uniform Electronic Transfers Act (followed by passage of the federal E-SIGN Act in 2000), that standards were put in place to establish the legality of electronic documents and signatures. Adoption of online banking grew substantially as these laws were enacted and as a regulatory framework took shape to match what were then considered revolutionary technological advancements.

Today, the rapid adoption of blockchain technologies, and the cryptocurrencies they support, are on their way to revolutionizing global financial and payment systems. And, as expected, we are beginning to see a balancing between innovators and regulators, with prominent voices weighing in— some touting cryptocurrency as the future of finance and others raising concerns about the illicit finance implications of the cryptocurrency ecosystem.

Having devoted my career to protecting and advancing the national security interests of the United States, I recognize the importance of ensuring that technological advancements related to critical industries are accompanied by smart, informed, and timely adjustments to regulatory frameworks, policies, and laws. Those who safeguard our nation simply must have the right tools to do their jobs. Period.

It is against this backdrop that I, and two of my colleagues from Beacon Global Strategies, conducted an analysis regarding the degree of illicit activity associated with cryptocurrencies in general and Bitcoin in particular. The project was sponsored by a group of leading cryptocurrency innovators and investors. The terms of the engagement were that I would "call it as I see it," with objectivity and transparency, just as I had done throughout my career as an intelligence analyst. I am hopeful that this analysis will help advance a healthy and fact-based dialogue as policymakers determine how to best ensure that these financial innovations serve the national interest.

Image: Visual Generation - stock.adobe.com



Introduction

So far, 2021 has been a year of significant developments and milestones for Bitcoin. Its price surpassed $60,000 for the first time in its history.[1] Major corporations, from Tesla to Square to MicroStrategy, are adding it to their balance sheets.[2] Large banks are providing Bitcoin-related services, with Morgan Stanley saying it will soon offer access to three Bitcoin funds for its wealth management clients.[3] Canada has approved Bitcoin exchange traded funds (ETFs).[4] There is growing momentum for Bitcoin's emerging use as a store of value.

Yet there is a common belief that the Bitcoin market is rife with illicit activity, with many holding this belief pointing to several high-profile incidents. When the illicit Silk Road darknet market (DNM) was shut down in 2013, more than 26,000 Bitcoin were seized by the FBI.[5] AlphaBay, formed in 2014 and widely viewed as an heir to Silk Road, was shuttered by international authorities in 2017 after building a customer base of over 400,000, with transactions conducted largely in Bitcoin.[6] The 2017 WannaCry ransomware attack that infected more than 200,000 computers worldwide required payment in Bitcoin.[7] Bitcoin was even used to help fund some of those involved in the insurrection at Capitol Hill on January 6.[8]

The conventional wisdom on this issue has been reinforced by public statements from senior government officials on both sides of the Atlantic who have suggested that Bitcoin is used primarily for illicit activities. Eye-catching media reports, like a recent Buzzfeed article titled, "Secret Documents Show How Terrorist Supporters Use Bitcoin – And How the Government is Scrambling to Stop Them," add weight to such remarks.[9]

In undertaking our analysis, we consulted a diverse group of experts in the fields of cryptocurrency technology and investment, financial services, payment systems, global intelligence and security, financial regulation, and law enforcement. We interviewed executives from major blockchain analytics firms, former senior Treasury Department officials, a senior official from the Commodity Futures Trading Commission (CFTC), and a former CIA intelligence analyst, as well as academics, venture capital investors, former federal prosecutors, and a former leader in the banking industry. We also consulted studies from the U.S. Department of Justice; the Financial Crimes Enforcement Network (FinCEN); the Financial Action Task Force (FATF); major blockchain analytics firms; the Brookings Institution; RAND Corporation; BAE Systems; and the Foundation for the Defense of Democracies.

Sigal Mandelker, former Acting Deputy Secretary of the Treasury and Under Secretary of the Treasury for Terrorism and Financial Intelligence, as well as a former Department of Justice official and prosecutor, gave us a significant amount of her time to tap into her wealth of experience on the issue.

Image: Rickard B. Levine/Zuma Press

I began this work expecting that I would find a set of facts supporting the conventional wisdom on this issue. After all, I believed that Bitcoin and other cryptocurrencies are a largely anonymous way to transfer funds anywhere in the world nearly instantaneously. And I assumed that those officials who have raised concerns about the use of Bitcoin in illicit activity—with the objective of ensuring regulatory vigilance—must be among the best-informed experts on this issue.

However, based on our research and discussions with industry experts, I have confidence in two conclusions:

- The broad generalizations about the use of Bitcoin in illicit finance are significantly overstated.

- The blockchain ledger on which Bitcoin transactions are recorded is an underutilized forensic tool that can be used more widely by law enforcement and the intelligence community to identify and disrupt illicit activities. Put simply, blockchain analysis is a highly effective crime fighting and intelligence gathering tool.

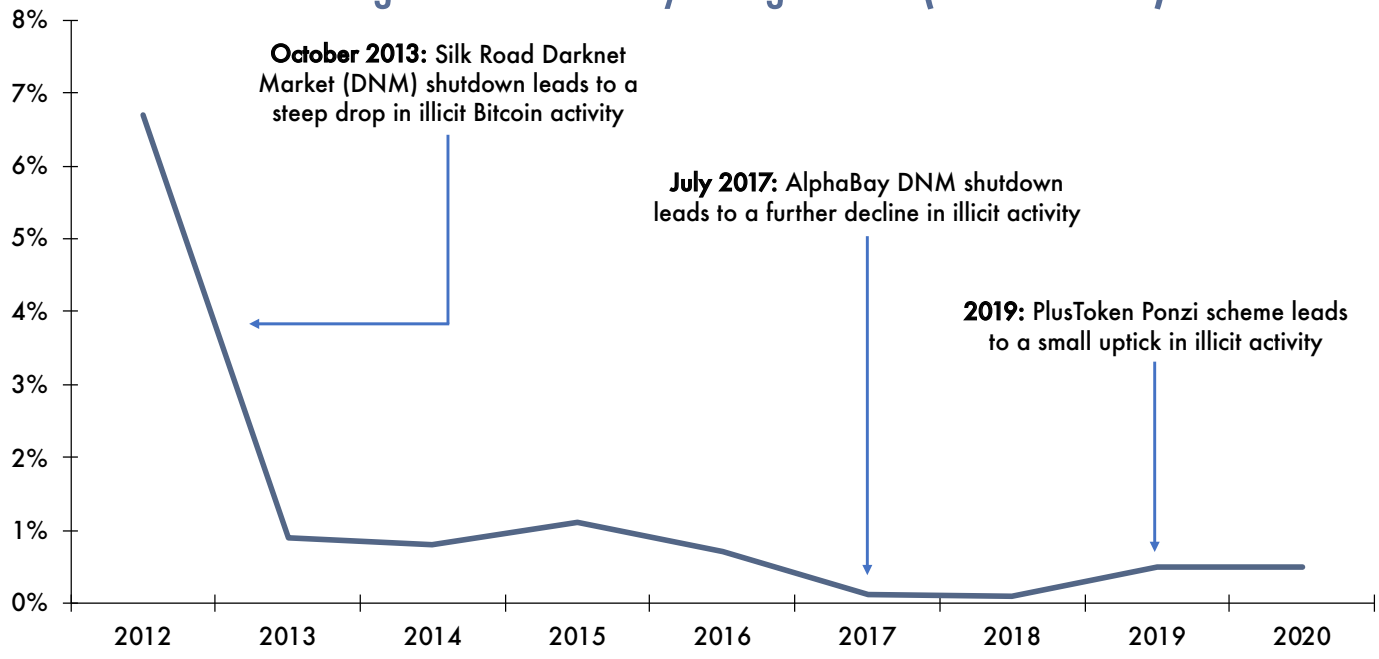
Bitcoin's Use in Illicit Activity is Relatively Limited

It is true that cryptocurrency, like other new technologies and innovations, has attracted the attention of illicit actors. And not surprisingly, just as Bitcoin is the most commonly held cryptocurrency, it is also the coin most often found in DNM wallets by a wide margin.[10] The fact that Bitcoin is being used by illicit actors is likely the basis of recent and widely reported comments by government and regulatory officials. But digging deeper, their statements center on two assertions: First, that Bitcoin is used "frequently" or "primarily" for illicit financial transactions, and second, that the use of Bitcoin in such transactions is growing.

Notwithstanding such statements, a senior executive at a major cryptocurrency analytics firm told us that the common belief that Bitcoin is both primarily and increasingly used for purposes of illicit finance is "uninformed and not based on data" and that "there are no numbers and no methodologies" supporting it.

According to a recent study by blockchain analytics firm Chainalysis, illicit activity among all cryptocurrencies as a percent of total cryptocurrency activity from 2017 to 2020 was less than 1 percent.[11] For Bitcoin specifically, blockchain analytics firm CipherTrace estimates that illicit activity makes up less than 0.5 percent of total transaction volume.[12]

Percentage of Illicit Activity Using Bitcoin (2012 – 2020)



Sources: Chainalysis 2018 Crypto Crime Report; ChipherTrace Cryptocurrency Crime and Anti-Money Laundering Report, February 2021

Meanwhile, estimates of illicit activity in the economy as a whole, overwhelmingly conducted through traditional financial intermediaries and with traditional fiat currencies, are on the order of 2 to 4 percent of global GDP. Indeed, FinCEN's Bank Secrecy Act (BSA) database contains over 300 million Suspicious Activity Reports (SARs), with an additional 20 million added each year.[13] Not all these SARs equate to illicit activity in the traditional banking system, but many do.

A former CIA analyst added credence to the above estimates, telling us that, due in part to the difference in overall volume, most illicit activity still takes place in the traditional banking system and not via cryptocurrency. A 2020 BAE Systems report, commissioned by SWIFT, further noted that "identified cases of laundering through cryptocurrencies remain relatively small compared to the volumes of cash laundered through traditional methods".[14]

> "[I]dentified cases of laundering through cryptocurrencies remain relatively small compared to the volumes of cash laundered through traditional methods."

All of this together suggests a broader point—that the illicit use of cryptocurrencies in general and Bitcoin in particular, as a share of total market activity, is certainly not higher than it is in the traditional banking system and is most likely less.

Of course, the data collected by the blockchain analytics firms is based on illicit activity that they actually see; the estimates do not attempt to quantify the size of illicit activity that they cannot see and analyze.

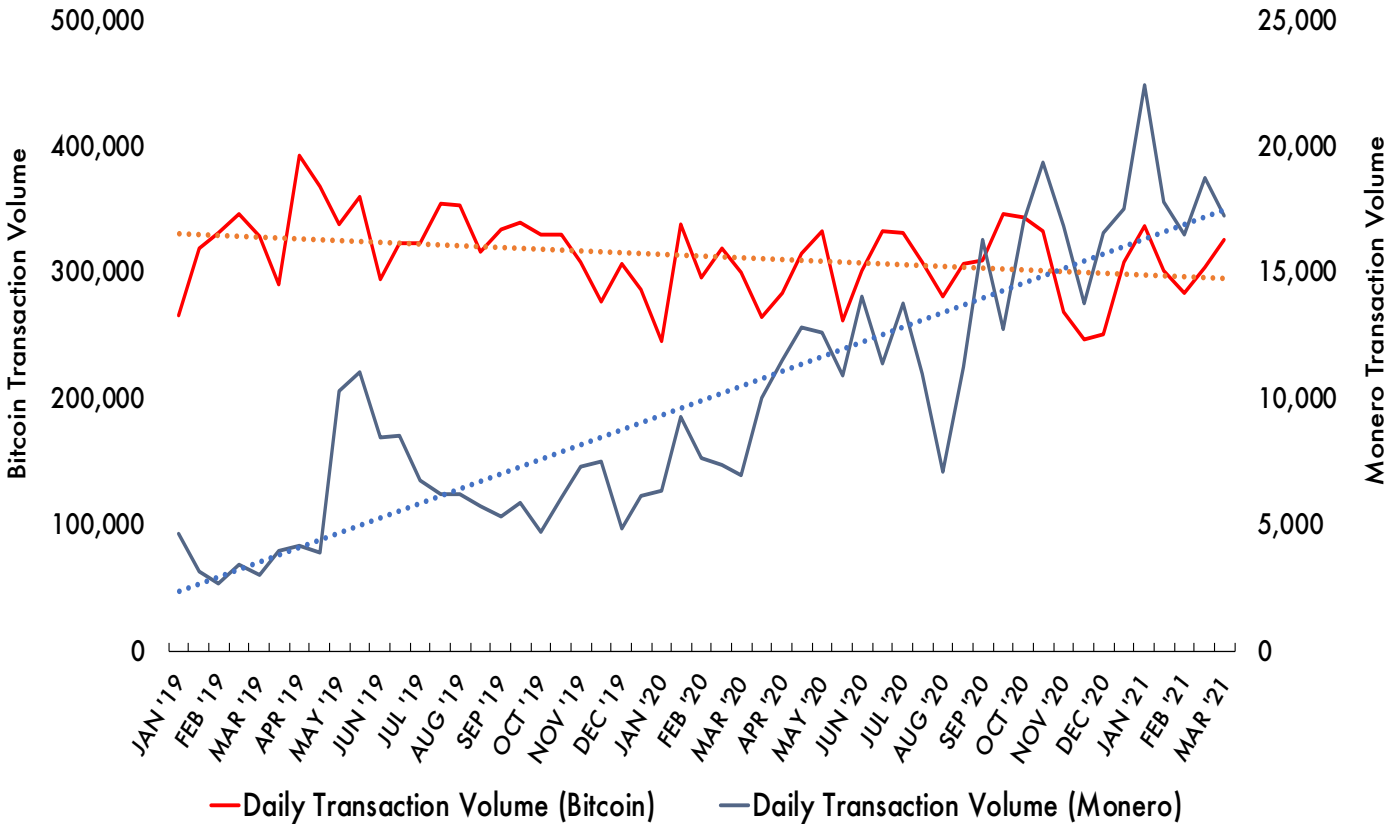
However, the firms we spoke with believe the unseen illicit activity is relatively small. One said it believes that it sees most illicit activity, while another estimates that unseen activity is no more than what they do see. And, while it is true that we don't know what we don't know in the cryptocurrency market, the same is true of illicit activity in the banking system and in cash, as evidenced by the lack of firm estimates for these payment systems.

According to the Chainalysis study, the two most significant types of illicit activity are those related to "simple" scams and purchases on the dark web. Ransoms for ransomware attacks are difficult to measure, but data suggest it is the fastest growing category of cryptocurrency crime, while terrorist-related activity and payments related to sanctions evasion remain quite small.[15]

On the key issue of terrorist financing, the former CIA terrorism expert believes that the hype is much greater than the reality and that cryptocurrency is not yet an important platform for terrorist organizations. He added that cryptocurrency crowdfunding efforts of such groups have typically brought in only a few thousand dollars before being shut down.* A 2019 study by the RAND Corporation further concluded that terrorist use of cryptocurrencies is minimal and that no current cryptocurrency provides a terrorist group what it would need to be a significant user.[16]

* The Department of Justice's 2020 Cryptocurrency Enforcement Network report stated that "while terrorist use of cryptocurrency is still evolving, certain terrorist groups have solicited cryptocurrency donations running into the millions of dollars via online social media campaigns."

Comparison of Daily Transaction Volumes: Bitcoin vs. Monero



Source: BitInfoCharts.com

However, the former CIA terrorism expert also noted that some groups are beginning to use more sophisticated cryptocurrency anonymizing techniques to conceal their flow of funds, which is a key development to monitor.

As noted earlier, Bitcoin is by far the largest cryptocurrency used in illicit flows. However, two major cryptocurrency analytics firms have concluded that this is due to Bitcoin's dominance in the market and, therefore, its accessibility, not because it has attributes that make it more attractive to illicit users. Bitcoin represents more than 60 percent of the total market capitalization of cryptocurrencies, with over 4,000 other cryptocurrencies comprising the remaining 40 percent.[17]

And while Bitcoin is the cryptocurrency most used in illicit activity, other cryptocurrencies are used far more often for illicit purposes as a share of their total transactions. One major cryptocurrency analytics firm executive said that, for Anonymity-Enhanced Cryptocurrencies ("AECs" or "privacy coins"), such as Monero, which use built-in protocols to hide information about transactions, illicit activity as a percent of total transaction volume is "far larger" than it is for Bitcoin.

There is also mounting evidence that illicit activity is flowing away from Bitcoin and toward AECs. The 2020 RAND report referenced above noted such a shift from Bitcoin to cryptocurrencies with stronger anonymity.[18] The prominent DNM "White House Market" has moved to accepting Monero exclusively.[19] Similarly, the ransomware group, Sodinokibi, no longer accepts Bitcoin as payment and will only take Monero.[20] Growing use of AECs for illicit activity was further highlighted in an October 2020 advisory issued by FinCEN that stated, "[illicit actors] are increasingly requiring or incentivizing victims to pay in AECs that reduce the transparency of [cryptocurrency] financial flows, including ransomware payments, through anonymizing features". The advisory added that "[s]ome ransomware operators have even offered discounted rates to victims who pay their ransoms in AECs."[21]

Blockchain Technology is a Powerful Forensic Tool

Blockchain technology is a powerful but underutilized forensic tool for governments to identify illicit activity and bring criminals to justice. One expert on the cryptocurrency ecosystem called blockchain technology a "boon for surveillance."

A currently serving official at the CFTC added that it "is easier for law enforcement to trace illicit activity using Bitcoin than it is to trace cross-border illegal activity using traditional banking transactions, and far easier than cash transactions."

> "[It] is easier for law enforcement to trace illicit activity using Bitcoin than it is to trace cross-border illegal activity using traditional banking transactions, and far easier than cash transactions."

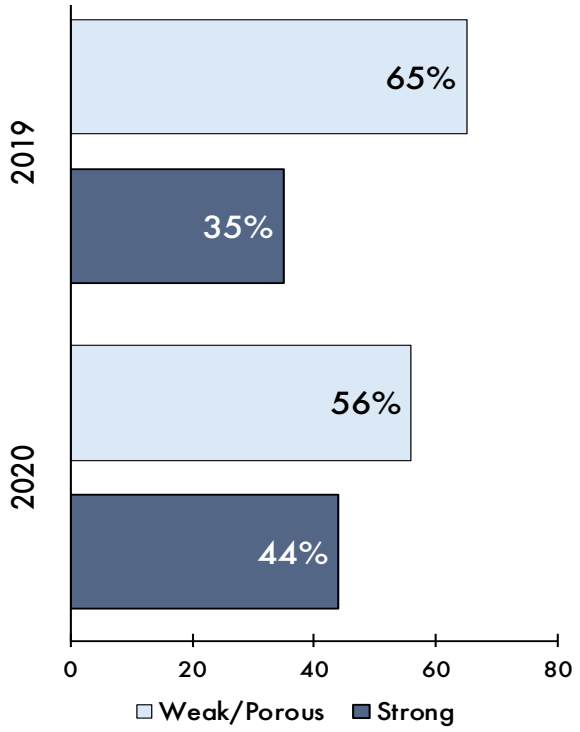
Former senior Treasury official Sigal Mandelker agreed and said that this view is shared by a number of people in this space who have experience working in law enforcement.

In a February 2021 testimony before the House Subcommittee on National Security, International Development and Monetary Policy, former Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes Daniel Glaser stated that, when it comes to transparency in the international financial system and the domestic financial system, "crypto-currencies provide enhanced opportunities in certain ways for law enforcement agencies to be able to trace transactions". Glaser added that the U.S. government should "bring [cryptocurrencies] into the system and regulate them in the appropriate way."[22]

One expert told us that the chance of catching illicit actors is "magnitudes greater" using blockchain than in the traditional banking sector. Another went so far as to say that "if all criminals used blockchain, we could wipe out illicit financial activity." In fact, its transparent nature led one blockchain analytics expert to compare transactions on blockchain to having the "whole world" be a witness to paying someone $2,000 in a dark alley.[23] Based on our research, I have come to believe that if there was one financial ecosystem for bad actors to use that would maximize law enforcement's chances of identifying them and their illicit activities, it would be blockchain.

Blockchain technology enables this forensic power because it captures every single transaction for all to see—it provides governments and the public at large with a permanent, unchangeable record of transactions. When viewed together with other data derived from the analysis of blockchain analytics as well as traditional law enforcement tools like subpoenas, blockchain technology can allow for the identification of both illicit activity and the identities of end users. The ability to detect illicit activity and identify the perpetrators is not perfect, but it has grown significantly over the last few years.

Percentage of VASPs* with either Strong or Weak/Porous KYC (2019 vs. 2020)



Source: CipherTrace 2020 Geographic Risk Report

Broader enforcement of Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations would further enhance the ability of law enforcement to identify illicit Bitcoin activity.[24] While a growing share of Bitcoin are held on centralized exchanges, CipherTrace reported that 56 percent of global Virtual Asset Service Providers (VASPs)* still have "weak or porous KYC processes".[25] Given this, I expect that further applying KYC and AML regulations, long seen as effective by senior government officials, will help assuage their concerns about Bitcoin transactions.

> "I pay you $2,000 in a dark alley, who are the witnesses to that transaction? Just you and [me], right? With cryptocurrency... the whole world could be the witness."

Decentralized exchanges (DEXs), which typically do not have a central authority on which to apply KYC and AML regulations, are also an emerging challenge. Although DEXs are responsible for only a small portion of overall cryptocurrency transaction volume, their decentralized, mostly open-source nature adds an additional layer of anonymity and thus offers increased opportunities for moving illicit funds.[26]

* Virtual Asset Service Providers (VASPs) are businesses that offer one of the following services: 1) exchange between cryptocurrencies and fiat currencies; 2) exchange between one or more forms of cryptocurrency; 3) transfer of cryptocurrencies; 4) safekeeping and/or administration or cryptocurrencies.

Therefore, DEX operations will remain a challenge for government regulators, particularly with regard to their use in facilitating transactions between more anonymous "unhosted" wallets.[27]

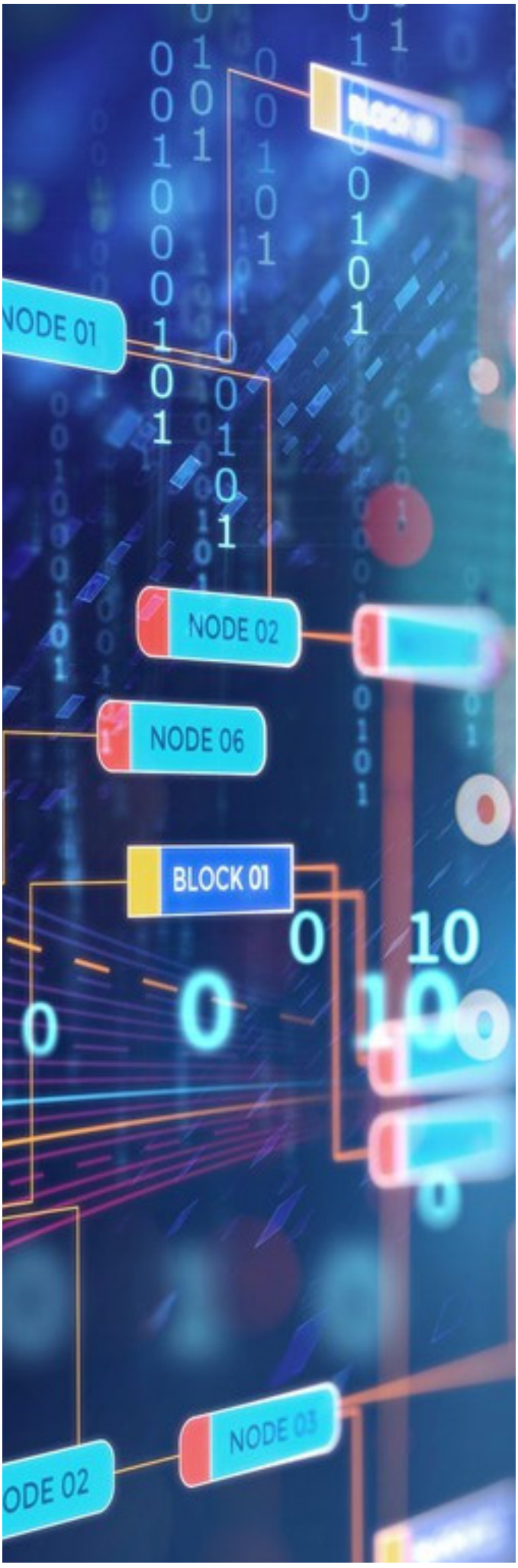
Like other illicit activities, such as the use of performance enhancing drugs in athletics, authorities are constantly working to catch up to new masking techniques used by illicit actors. In the case of cryptocurrency, blockchain analytics firms are developing new forensic tools to counter the use of technologies that create more anonymity—like privacy coins, mixers, tumblers, layering, and chain-hopping.

For example, in September 2020, Chainalysis was awarded a $625,000 grant from the IRS to develop Monero-tracking software.[28] Last November, CipherTrace also filed two patents for technologies related to tracing Monero transactions after working with the U.S. Department of Homeland Security.[29] Finally, in December 2020, cryptocurrency forensics software was even able to reliably trace stolen Bitcoin that had been passed through several coin mixers.[30]

Blockchain forensics can be used in multiple ways by law enforcement and intelligence services. First, it can be used as an investigative tool in existing cases; law enforcement can use the blockchain to uncover the illicit activity of the target of an investigation (and identify other potential bad actors linked via the blockchain to that target). Second, by using artificial intelligence algorithms developed from patterns of how illicit actors behave in the ecosystem, it can identify previously unknown bad actors. To this end, the blockchain allows law enforcement to adopt a much more sophisticated proactive network strategy to identify illicit activity.

All of the experts we consulted believe that governments have been slow to recognize the forensic power of blockchain technology. This lag reflects a lack of awareness at senior and working levels, as well as the challenges understanding and working with the extreme complexity of the computer science associated with blockchain forensics. While there is a growing cadre of government officials who have successfully used blockchain analytic tools to prosecute bad actors and seize illicit proceeds, relatively few current government employees have the skills to use this technology to its full potential.

One expert went even further, saying that the biggest threat involving cryptocurrencies is not illicit finance but rather that governments do not yet fully understand the power of blockchain as a tool for law enforcement and intelligence agencies.



However, the expert also noted that awareness of this power is beginning to expand as governments engage with the three major blockchain analytic firms, Chainalysis, CipherTrace, and Elliptic. Beyond the United States, blockchain forensics are being used by government agencies in Europe, Japan, and South Korea.

This gradual recognition helps explain the number of significant legal cases that have been broken through the use of blockchain analysis. In November 2020, the IRS, following assistance from Chainalysis, was able to retrieve $1 billion worth of illicit Bitcoin related to the now-defunct Silk Road DNM.[31]

In the July 2020 breach of Twitter's network, when over 100 high-profile accounts were hacked to promote a scam asking followers for Bitcoin, it took only two weeks for investigators to identify the perpetrators and make arrests. Investigators linked the wallet addresses to user accounts on various forums. Then, using blockchain analytics, they traced stolen funds to various exchanges, worked with those exchanges to identify the users, and matched that user information to the data found on the forums. Notably, investigators identified an individual who never posted anything publicly that could link him to his real-world identity by analyzing transactions between Bitcoin addresses.[32]

Finally, in late 2020, the law firm Kobre & Kim was able to use blockchain analysis to trace and retrieve $32 million in cryptocurrency that had been passed through coin mixers.[33] As the tools that these firms employ grow more sophisticated, illicit actors are finding it increasingly more difficult to conceal their activity.

And as more seizures and arrests are made, we believe illicit actors—who are technology agnostic—will continue to move away from using Bitcoin for money laundering purposes to other avenues that make it easier for them to hide their activities. It will essentially be the counterterrorism equivalent of Usama bin Ladin never again, for the rest of his life, using a phone after learning that the U.S. government could listen to his calls.

Conclusion

In light of the conclusions we have reached, why do we see such alarmist statements and articles about the threat posed by Bitcoin? There are several reasons. First, this is a new technology, and it is complicated to comprehend—people are typically fearful of what they do not understand.

Second, bad news drives perceptions more than good news; in brief, fear makes headlines. A story about a French citizen sending Bitcoin to individuals involved in the insurrection at the U.S. Capitol crowds out stories of the use of blockchain-enabled forensics to solve a crime. We need to reevaluate these sorts of stories by recognizing that it was the transparent nature of the blockchain that allowed law enforcement to so quickly identify the trail of illicit payments, whereas such payments made through the traditional financial system might have proven more difficult to trace.

"[Growing use of blockchain forensics] will essentially be the counterterrorism equivalent of Usama bin Ladin never again, for the rest of his life, using a phone after learning that the U.S. government could listen to his calls."

Finally, Bitcoin and its decentralized nature seem to pose a disruptive threat to traditional financial institutions. The same could have been said for electronic banking and e-signatures 20 years ago, which stirred up significant debate regarding consumer protection and integrity of the financial system. Eventually, traditional financial institutions found ways to successfully incorporate it into their businesses. And any new technology as innovative as blockchain will represent a risk to the established methods of the finance industry. It will be the government's role to identify how to best use and regulate blockchain technology to advance the national interest.

My entire 33-year career at the Central Intelligence Agency was driven by one over-riding mission— presenting objective facts and analysis to policymakers so that they could make the best possible decision for the country. Such facts and analysis help overcome fear, misperception, and narrow interests (as opposed to the national interest). My hope with this paper is not that it will be the final word on the issue of Bitcoin and illicit finance but rather, as I noted in the introduction, that it will lead to a more fact-based discussion of the issue.

- **Michael Morell:** Senior Counselor, Beacon Global Strategies; Former Acting Director, Deputy Director, and Director of Intelligence at the Central Intelligence Agency
- **Josh Kirshner:** Senior Vice President, Beacon Global Strategies; Former Special Assistant to the Under Secretary of State for Arms Control and International Security
- **Thomas Schoenberger:** Associate, Beacon Global Strategies

End Notes

1) Monica, Paul R. La. "Bitcoin Tops the $60,000 Mark." CNN, Cable News Network, 13 Mar. 2021, www.cnn.com/2021/03/13/investing/bitcoin-prices-60000/index.html.

2) Patnaik, Subrat, et al. "A Tesla for a Bitcoin: Musk Drives up Cryptocurrency Price with $1.5 Billion Purchase." Reuters, Thomson Reuters, 8 Feb. 2021, www.reuters.com/article/us-tesla-crypto-currency/a-tesla-for-a-bitcoin-musk-drives-up-cryptocurrency-price-with-1-5-billion-purchase-idUSKBN2A81CG.

3) Manning, Landon. "With Bitcoin On The Rise, Morgan Stanley Joins Institutional Adopters." Nasdaq, 22 Mar. 2021, www.nasdaq.com/articles/with-bitcoin-on-the-rise-morgan-stanley-joins-institutional-adopters-2021-03-22.

4) Helms, Kevin. "Canada Has Approved Two Bitcoin ETFs – First One Starts Trading Today." Bitcoin.com, 18 Feb. 2021, https://news.bitcoin.com/canada-approved-bitcoin-etfs-start-trading/.

5) Kovach, Steve. "Bitcoin Value Plummeting Following The Silk Road Shut Down." Business Insider, 2 Oct. 2013, www.businessinsider.com/bitcoin-value-drops-after-silk-road-shut-down-2013-10.

6) Arghire, Ionut. "Dark Web Market AlphaBay Goes Down." SecurityWeek, 14 July 2017, www.securityweek.com/dark-web-market-alphabay-goes-down.

7) Menn, Joseph. "Hackers Mint Crypto-Currency with Technique in Global 'Ransomware' Attack." Reuters, Thomson Reuters, 17 May 2017, www.reuters.com/article/us-cyber-attack-cryptocurrency-idUSKCN18D00W.

8) "Large Bitcoin Payment Made to Far-Right Individuals before U.S. Capitol Attack: Report." Reuters, Thomson Reuters, 14 Jan. 2021, www.reuters.com/article/us-usa-election-cryptocurrency/large-bitcoin-payment-made-to-far-right-individuals-before-u-s-capitol-attack-report-idUSKBN29J2PM.

9) Templon, John. "Secret Documents Show How Terrorist Supporters Use Bitcoin - And How The Government Is Scrambling To Stop Them." BuzzFeed News, 1 Feb. 10, 2021, www.buzzfeednews.com/article/johntemplon/bitcoin-cryptocurrency-terrorist-financing-janet-yellen.

10) Silfversten, Erik, et al. RAND Corporation, 2020, Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes.

11) "Crypto Crime Summarized: Scams and Darknet Markets Dominated 2020 by Revenue, But Ransomware Is the Bigger Story." Chainalysis, 19 Jan. 2021, blog.chainalysis.com/reports/2021-crypto-crime-report-intro-ransomware-scams-darknet-markets.

12) "Cryptocurrency Crime and Anti-Money Laundering Report, February 2021." CipherTrace, 3 Mar. 2021, ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/.

13) "Prepared Remarks of FinCEN Director Kenneth A. Blanco at Chainalysis Blockchain Symposium." Prepared Remarks of FinCEN Director Kenneth A. Blanco at Chainalysis Blockchain Symposium | FinCEN.gov, 15 Nov. 2019, www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-chainalysis-blockchain-symposium.

14) "New Report Reveals How Cyber Attackers 'Cash out' Following Large-Scale Heists." BAE Systems | Managed Security Services, www.baesystems.com/en-financialservices/insights/news/report-reveals-how-cyber-attackers-cash-out-following-heists.

15) Grauer, Kim, and Henry Updegrave. Chainalysis, 2021, The 2021 Crypto Crime Report.

16) Dion-Schwarz, Cynthia, and David Manheim. RAND Corporation, 2019, Terrorist Use of Cryptocurrencies.

17) "Global Cryptocurrency Market Charts." CoinMarketCap, coinmarketcap.com/charts/; "Cryptocurrency Prices, Charts And Market Capitalizations." CoinMarketCap, 22 Mar. 2021, coinmarketcap.com/.

18) Ibid.

19) Staff, Decrypt. "Bittrex To Delist Privacy Coins Monero, ZCash and Dash in Two Weeks." Decrypt, Decrypt, 1 Jan. 2021, decrypt.co/53012/bittrex-to-delist-privacy-coins-monero-zcash-and-dash-in-two-weeks.

20) Erb, Kelly Phillips. "IRS Will Pay Up To $625,000 If You Can Crack Monero, Other Privacy Coins."
Forbes, Forbes Magazine, 15 Dec. 2020, www.forbes.com/sites/kellyphillipserb/2020/09/14/irs-will-pay-up-to-625000-if-you-can-crack-monero-other-privacy-coins/?sh=32617ccf85cc.

21) Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments. Financial Crimes Enforcement Network (FinCEN), 1 Oct. 2020, www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

22) U.S. House Committee on Financial Services, Subcommittee on National Security, International Development and Monetary Policy, "Dollars Against Democracy" virtual hearing, February 25, 2021.

23) Lee, Seulki, and Corinne Redfern. "Sex Criminals Use Bitcoin. So Do the Police." Foreign Policy, 30 Jan. 2021, foreignpolicy.com/2021/01/30/sex-criminals-use-bitcoin-so-do-the-police/.

24) KYC regulations require financial services companies to acquire sufficient customer information and to perform due diligence. Adequate KYC regulations are integral to AML compliance.

25) Silfversten, Erik, et al. RAND Corporation, 2020, Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes; Clegg, Pamela, and Dave Jevans. CipherTrace, 2020, CipherTrace Geographic Risk Report.

26) Khan, Momina. "DEX Volumes Made up Almost 4% of Centralized Exchange Volumes in July - a Monthly High." The Block, 4 Aug. 2020, www.theblockcrypto.com/linked/73939/dex-volume-ratio-july.

27) Unhosted cryptocurrency wallets are owned and operated by individuals. They do not require a custodian or financial institution in order to conduct transactions.

28) Post, Kollen. "Chainalysis and Texas Firm Win Million-Dollar IRS Contract to Crack Monero." Cointelegraph, Cointelegraph, 30 Sept. 2020, cointelegraph.com/news/chainalysis-and-texas-firm-win-million-dollar-irs-contract-to-crack-monero.

29) Jevans, Dave. "CipherTrace Files Two Monero Cryptocurrency Tracing Patents." CipherTrace, 21 Nov. 2020, ciphertrace.com/ciphertrace-files-two-monero-cryptocurrency-tracing-patents/.

30) "Benjamin Sauter Explains Precedent-Setting Digital Currency Recovery Case." Benjamin Sauter Explains Precedent-Setting Digital Currency Recovery Case | Kobre & Kim - Disputes and Investigations, kobrekim.com/insights/publications/benjamin-sauter-explains-precedent-setting-digital-currency-recovery-case.

31) "United States Files A Civil Action To Forfeit Cryptocurrency Valued At Over One Billion U.S. Dollars." The United States Department of Justice, 5 Nov. 2020, www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us.

32) Barrett, Brian. "How the Alleged Twitter Hackers Got Caught." Wired, Conde Nast, 31 July 2020, www.wired.com/story/how-alleged-twitter-hackers-got-caught-bitcoin/.

33) Ibid.