Working Paper Series
International Trade and Economic Diplomacy
Middlebury Institute of International Studies
Monterey, CA

Cryptocurrency and Risks to Banks, AML, and Sanctions Compliance: A Case Study

Dennis Gable
Assistant VP, GFS-US, BNP Paribas
and Colleague

MA in International Trade and Economic Diplomacy Candidate

April 2021

Abstract

This working case study describes the potential compliance risks cryptocurrencies pose to financial institutions in addition to areas in which banks may expand digital services. Banks' compliance requirements often come at odds with users' appeal to privacy but are necessary for properly monitoring any transgressions or illicit behavior. While many enthusiasts have praised cryptocurrency-related services such as mixing and OTC brokers, many of these processes may pose substantial risks to banks' KYC efforts. Our reviewed cases highlight a number of ways in which actors with pernicious intentions may complicate financial institutions and exchanges' monitoring efforts by obfuscating the source of their laundered or sanctioned funds.

Table of Contents

Abstract:

This working case study describes the potential compliance risks cryptocurrencies pose to financial institutions in addition to areas in which banks may expand digital services. Banks' compliance requirements often come at odds with users' appeal to privacy but are necessary for properly monitoring any transgressions or illicit behavior. While many enthusiasts have praised cryptocurrency-related services such as mixing and OTC brokers, many of these processes may pose substantial risks to banks' KYC efforts. Our reviewed cases highlight a number of ways in which actors with pernicious intentions may complicate financial institutions and exchanges' monitoring efforts by obfuscating the source of their laundered or sanctioned funds.

Introduction:

The growth of cryptocurrency in the international market is continuing to complicate Anti-Money Laundering (AML) and sanctions compliance programs for both the public and private sector. For financial institutions that have decided to avoid adding cryptocurrency to their portfolios, there is a growing risk of business lines using digital currency in violation of United States sanctions in a manner that will implicate the financier. Since the launch of Bitcoin in 2009, cryptocurrency has only grown in market value and diversity. Although there are coins that are considered to be clear front runners, estimates show that there are now thousands of cryptocurrencies available for investment with more being offered everyday. In 2019, cryptocurrency accounted for $237.1 billion up from 128.78 in 2018.[1] While there is a notable volatility in digital currency, it can no longer be denied that it is a growing service. If we

[1] Rudden, Jennifer. "Cryptocurrency Market Value 2013-2019." *Statista*, 6 Nov. 2020, www.statista.com/statistics/730876/cryptocurrency-maket-value/#:~:text=Cryptocurrency%20market%20capitalization%202013%2D2019&text=The%20cumulative%20market%20capitalization%20of. Accessed 8 Nov. 2020.

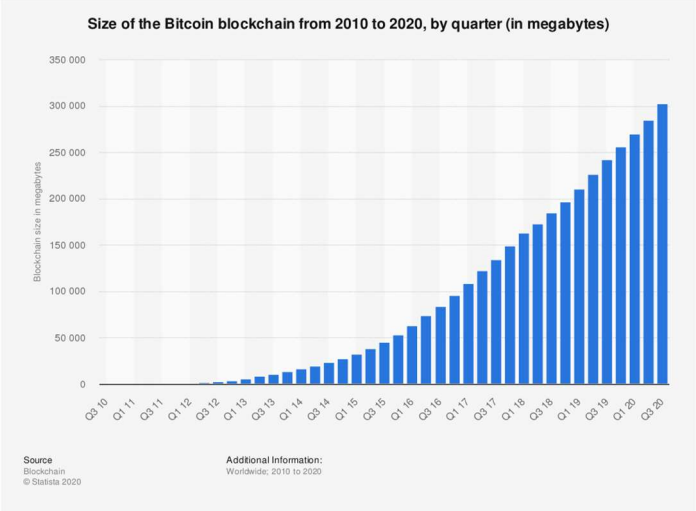
assumed 5% user adoption of crypto in the US currently and calculated revenue growth if user adoption reaches 10% (conservative case), 20% (base case), and 50% (optimistic case) by 2029, resulting exchange revenues would amount to $1.9 billion in the conservative case, $3.8 billion in the base case, and $9.6 billion in the optimistic case.[2]

Bitcoin, the most popular form of cryptocurrency in the world, has shown consistent and impressive growth since its inception in 2009 (See Graph 1). Recently, Bitcoin has risen back to almost $20,000 per coin - nearing its all-time high from 2018. Bitcoin has also shown a steady and significant growth in its usage rate (See Graph 2). As the cryptocurrency market continues to grow in a market capitalization of several hundreds of billions of dollars, many banks and financial service companies have begun offering a wide array of crypto products and have begun to see the mass potential of blockchain technology. Over time, it may even become impossible for financial companies to avoid dealings in digital currency if current growth trends persist.

Graph 1

Graph 2

[2] Shimron, Leeor. "Crypto Exchanges And Bitcoin Are Poised For Massive Growth By 2030." *Forbes*, 20 June 2020, www.forbes.com/sites/leeorshimron/2020/06/20/crypto-exchanges-and-bitcoin-are-poised-for-massive-growth-by-2030/?sh=48280d423f83. Accessed 8 Nov. 2020.



The bitcoin blockchain is a distributed database that contains a continuously-growing and tamper-evident list of all Bitcoin transactions and records since the date of its initial release in January of 2009.[3]

Even if traditional financial institutions have decided to avoid dealing in emerging industries such as crypto directly, they may still be vulnerable to its risks if they have failed to develop adequate systems to monitor their exposure. According to a LexisNexis report, in 2019, approximately $2.3 billion in Bitcoin was used for illicit purposes.[4] With the frequency with which illicit actors transfer crypto to fiat currency and vice versa, many banks may remain unaware of their clients (or their clients' clients) dealings. Without any proper analytics technology in place, financial institutions may very well succumb to inadvertently laundering money or conducting business with sanctioned entities through digital currency. In response to the 2018 implementation of the petro by the Venezualen government, the Department of Treasury announced its commitment to holding digital currency to the same standard of compliance as fiat currency and that "U.S. persons (and persons otherwise subject to OFAC

[3] "Bitcoin Blockchain Size 2010-2019 | Statista." *Statista*, Statista, 2010, www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/.
[4] "Sanctions Compliance for Banks in the Age of Crypto-Assets." *Financial Crime In Focus*, 5 June 2020, blogs.lexisnexis.com/financial-crime-in-focus/sanctions-compliance-for-banks-in-the-age-of-crypto-assets/. Accessed 11 Nov. 2020.

jurisdiction) must ensure that they block the property and interests in property of persons named on OFAC's SDN List or any entity owned in the aggregate, directly or indirectly, 50 percent or more by one or more blocked persons, and that they do not engage in trade or other transactions with such persons."[5] U.S. federal law draws no distinction in how cryptocurrency and other assets should be treated and monitored with respect to sanctioned entities. All institutions and financial service companies must maintain the same standard of due diligence when processing transactions.

Criminal Uses of Cryptocurrency

Sanctions Violations:

The nature of cryptocurrency allows coin owners to send funds through thousands of wallets with almost instant settlement - at least with far greater speed than traditional wire transfers. While the movement of most cryptocurrencies is relatively easy to track with access to publicly distributed ledgers, transactions often remain pseudonymous as identifying the entity behind an address can be far from straightforward. An owner can even structure crypto into smaller amounts and distribute funds across several addresses and "one time use" wallets to make tracking more difficult.[6] A bank that does not have blockchain analytics software in place to monitor cryptocurrency transactions tied to its financed business lines could easily overlook

[5] "| U.S. Department of the Treasury." *Home.Treasury.Gov*, 19 Mar. 2018, home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626. Accessed 8 Nov. 2020.
[6] "Sanctions Compliance for Banks in the Age of Crypto-Assets." *Financial Crime In Focus*, 5 June 2020, blogs.lexisnexis.com/financial-crime-in-focus/sanctions-compliance-for-banks-in-the-age-of-crypto-assets/. Accessed 11 Nov. 2020.

the potential downstream financing of sanctioned entities. Privacy coins - an option preferred by privacy enthusiasts and illicit actors alike - afford the user complete anonymity.[7] They provide users with hidden balances and wallet addresses that render their funds virtually untraceable. While many may prefer privacy coins such as Monero or Zcash for perfectly legitimate reasons, privacy coins are very attractive tools for entities looking to launder money or evade sanctions. When a financed business line decides to conduct business with a sanctioned entity, they need only falsify the invoice as the cryptocurrency is reported only as sent from a wallet. Therefore, no explanation or documentation is required to support the transfer of money as it is simply recorded from digital wallet to digital wallet. If the bank does not have adequate digital currency oversight controls in place, there will be no reason to investigate the transaction.

Malware and Ransomware:

Cryptocurrency is completely decentralized and digital. Though these aspects serve as a primary appeal of digital currency, they simultaneously expose crypto to digital theft through the use of ransomware and malware. For clarity, "ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid."[8] Individuals with pernicious intent may use various tactics to avoid KYC detection and redirect digital currency to alternate wallets that will eventually be converted into fiat currency. Whether a financial institution deals in cryptocurrency or not, if its customers hold cryptocurrency in exchanges with inadequate security, such institutions may be susceptible to risk.

---

[7] Privacy coins are unique cryptocurrencies that allow a user to gain total anonymity when making blockchain transactions. The identity of users and the origins of their transactions are completely protected.ShapeShift. "What Are Privacy Coins?" *Medium*, 4 Mar. 2020, medium.com/shapeshift-stories/what-are-privacy-coins-6df8622ebf76#:~:text=Privacy%20coins%20are%20unique. Accessed 11 Nov. 2020.

[8] CISA. "Ransomware | CISA." *www.Cisa.Gov*, 2020, www.cisa.gov/ransomware. Accessed 11 Nov. 2020.

Department of Treasury response to Cryptocurrency:

On 15 July 2019, Treasury Secretary Mnuchin discussed the need for cryptocurrency regulation and plans to better understand the threat it poses to national security: "Cryptocurrencies, such as Bitcoin, have been exploited to support billions of dollars of illicit activity like cybercrime, tax evasion, extortion, ransomware, illicit drugs, and human trafficking. Many players have attempted to use cryptocurrencies to fund their malign behavior. This is indeed a national security issue."[9] He also described how providers and distributors of cryptocurrency are now held to the same standard of AML/KYC compliance measures as traditional finance institutions. At the time, the Facebook "Libra" was the primary focus of Congress as it was poised to become a new domestically based cryptocurrency. Now, the Libra has become completely rebranded due to the regulations and controls established by the Federal government, but the Libra's rebranding and legal issues demonstrate how seriously the government is taking the illicit use of cryptocurrency. Mnuchin has established the Financial Stability Oversight Council (FSOC Group) composed of FinCEN, the Fed, OCC, CFTC, CFPB, and the SEC. "The Financial Stability Oversight Council has a clear statutory mandate that creates for the first time collective accountability for identifying risks and responding to emerging threats to financial stability."[10] Threats to financial stability now include the illicit use of cryptocurrency. The solution is currently to have transmitters of cryptocurrency comply with Bank Secrecy Act (BSA) obligations and register with FinCen - placing responsibility on exchanges to keep up with emerging methods of money laundering and cyber theft throughout

[9] "White House Press Briefing by Treasury Secretary Steven Mnuchin on Regulatory Issues Associated with Cryptocurrency | U.S. Department of the Treasury." *Treasury.Gov*, 22 Oct. 2019, home.treasury.gov/news/press-releases/sm731.

[10] "About FSOC | U.S. Department of the Treasury." *Home.Treasury.Gov*, home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/about-fsoc. Accessed 17 Nov. 2020.

the market. With the help of the other departments included in FSOC, FinCen now has greater oversight on all cryptocurrency exchanged in and outside of the United States.

Case Study Objective:

The objective of our research is to identify instances in which risks have manifested and how, more generally, these cases pose challenges to the banking industry. Does cryptocurrency present an opportunity or threat to bank's clearing and settlement services? Blockchain technology has been touted as a promising potential method to strengthen banks' AML systems. At the same time however, we know that cryptocurrencies have been used effectively to evade sanctions. We also know that there has been significant theft via cyber crime. So to look at the threats to financial institutions we must also understand how cryptocurrency will be used by banks as products. Once we understand the products that banks may eventually employ, we will understand what risks can be posed by incidents that have already occured.

Cryptocurrency is growing in market share every year. It is only a matter of time before financial institutions begin dealing in this digital currency directly. Nevertheless, there is still considerable uncertainty regarding how banks will profit from the growing technology and which products they will offer clients. First, we must look at the different types of cryptocurrency. There are essentially three types of cryptocurrency that should concern a bank. There is a coin, a token, and a privacy coin. The coin is the standard unit of currency that is maintained in a blockchain and is available to the public for purchase and exchange. Coins can be tracked via blockchain to and from wallet to wallet and generally provide the user with a level of anonymity. The token is similar, but only designed for a single type of use like a bus pass, or rewards card. The privacy coin is used to give the user total anonymity. It can not be tracked and

there is no identified origin or destination. Privacy coins will likely be a red flag for any financial institution. The token will likely be the premier product for most banks. In 2019, J.P. Morgan, released a digital coin (token) equal to the dollar for internal use.[11] A second option will likely be the crypto IRA. There are already opportunities to roll a 401K into a BitCoin supported IRA. The IRA is just one of several investment options as cryptocurrency has proven to be very speculative. A final option for banks is to serve as a digital currency exchange. A bank could offer an additional level of security for a fee to conduct transactions between crypto and fiat currency.

With the products identified, we will now overview potential threats to financial institutions that may develop as a result of carrying such products as part of their portfolio. The Department of Treasury has taken a firm stance to maintain strict regulations on the use of cryptocurrency, so traditional finance institutions must understand what the risks are. In this case study we look at cryptocurrency cyber crime in various forms: a crypto exchange hack, avoidance of sanctions, an elaborate ponzi scheme, and other pertinent cryptocurrency issues for financial institutions. In order to assess these threats we have chosen the Yinyin and Jialong crypto exchange theft case, The DOJ v. Mexican drug cartel crypto-laundering case, PlusToken: Anatomy of a Crypto Ponzi Scheme, and the Microsoft employee BitCoin theft case.

$100m Heist From Hong Kong Crypto Exchange

In 2018, two Chinese nationals, Tian Yinyin and Li Jiadong, were charged with laundering over $100 million of cryptocurrency stolen from a Hong Kong-based cryptocurrency exchange. The original hack reportedly began as a member of the Lazarus Group deceptively

[11] "J.P. Morgan Creates Digital Coin for Payments." *Www.Jpmorgan.com*, www.jpmorgan.com/solutions/cib/news/digital-coin-payments. Accessed 18 Nov. 2020.

posed as a customer, using a fake persona and social media profile, and targeted an employee of the crypto exchange with the aim of forging a working relationship. Once gaining the trust of the employee, the individual began sending emails containing pernicious malware attachments, attachments that would then infect the exchange's computer systems upon opening. After infecting the system, it was relatively simple for the North Korean conspirators to steal the estimated hundreds of million dollars worth of virtual currency. In an effort to prevent law enforcement from tracing the money, the stolen funds were then passed through hundreds of transactions and divided into several smaller amounts to reduce the likelihood of raising any suspicion.

Though Lazarus is a highly skilled cyber-hacking group, the North Korean hackers required the help of professional money launderers to successfully cash out the illicit proceeds.[12] After sending the stolen cryptocurrency to hundreds of single-use wallets on the Hong-Kong exchange, the money was then sent to accounts Yinyin and Jiadong had created at a separate crypto exchange. The two Chinese nationals - thought to be professional money launderers - used fake identity documents to circumvent the exchange's poor KYC defenses. In the layering stage of the scheme, the funds were passed on through a number of additional transactions to intermediary wallets in an effort to further obfuscate the funds' original source. Eventually, the cryptocurrency reached exchange accounts that were controlled by Yinyin and Jiadong and linked to their bank accounts. Less than a week after the original hack, Tian Yinyin linked a bank account at China Guangfa Bank to his accounts at both crypto exchanges. Li Jiadong linked his account at the first crypto exchange to bank accounts he controlled at nine different Chinese

[12] O'Neill, Patrick Howell. "North Korean Hackers Steal Billions in Cryptocurrency. How Do They Turn It into Real Cash?" *MIT Technology Review*, MIT Technology Review, 10 Sept. 2020, www.technologyreview.com/2020/09/10/1008282/north-korea-hackers-money-laundering-cryptocurrency-bitcoin/.

banks (Agricultural Bank of China, Everbright Bank, China CITIC Bank, CGB, China Minsheng Bank, Huaxia Bank, Industrial Bank, Pingan Bank, and Shanghai Pudong Development Bank). Yinyin and Jiadong used their various bank accounts and a cryptocurrency exchange that allows conversion to fiat currency to complete the final integration stage of their money laundering scheme. The proceeds of the hack, in this way, reached a number of accounts the perpetrators set up and controlled at various banks. The banks however, remained completely unaware of the reality that they were facilitating sanctions evasion through cryptocurrency.

Though FINCEN explicitly requires financial institutions to identify and report any suspicious use of virtual currency (i.e. funds potentially being laundered or evading sanctions), many banks still remain dangerously unaware of how to properly monitor and detect virtual currency-related transactions such as cryptocurrency. While financial institutions screen their customers against sanctions lists across various jurisdictions, tracking customers' exposure to or use of virtual currencies is often far more difficult. In the traditional banking system, when sending fiat currency via wire transfer from a customer to a recipient bank, there is little to no client ambiguity. On the other hand, when cryptocurrencies are sent from one pseudonymous or anonymous address to another, it isn't necessarily obvious where the transacting parties are located or who may be behind the addresses.[13] Blockchains are publicly distributed ledgers recording all transactions; however, in the absence of any blockchain analytics software, the names and locations of entities behind these crypto addresses often remain unknown. As Pyongyang continues to direct efforts toward cybercrime hacks of cryptocurrency exchanges, banks will need to remain cognizant of the risk of unknowingly laundering such proceeds.

[13] Carlisle, David. "Cryptocurrencies & Sanctions Compliance: A Risk That Can't Be Ignored." *Blockchain Analytics for Crypto Compliance*, 16 Oct. 2018, www.elliptic.co/blog/cryptocurrencies-sanctions-compliance-a-risk-that-cant-be-ignored.

Microsoft Employee uses Bitcoin Mixing Service to Conceal Funds

Former Microsoft engineer Volodymyr Kvashuk from Ukraine was sentenced to nine years in prison after being convicted by a jury of five counts of wire fraud, six counts of money laundering, two counts of aggravated identity theft, two counts of filing false tax returns, and one count each of mail fraud, access device fraud, and access to a protected computer in furtherance of fraud.[14] Kvashuk was using the accounts and identities of his colleagues to steal "currency stored value" (CSV) including gift cards. He was a part of the team tasked with the testing and development of Microsoft online retail. Kvashuk used this access to steal (CSV). He would then use a Bitcoin mixing service to disguise the paper trail. Over the course of seven months Kvashuk would process $2.8 million through Bitcoin into his own personal account. Since the back end of the theft occurred only in Kvashuk's account and inside the United States, he decided to file a tax return for the transactions and claimed that it was a gift from his family.[15] During the same time Kvashuk purchased a $1.6 million home and a $160,000 Tesla automobile.

This is the first case prosecuted that involved Bitcoin and tax evasion. Kvashuk made several mistakes in this situation that made an arrest and prosecution relatively easy. A $2.8 million deposit to a personal account in 7 months for an engineer that makes $116,000 per year is extremely suspicious. Kvahuk filing taxes and claiming that all the money was a gift from family was all the reason the IRS would need.

---

[14] "Former Microsoft Software Engineer Sentenced to Nine Years in Prison for Stealing More than $10 Million in Digital Value Such as Gift Cards." *Www.Justice.Gov*, 9 Nov. 2020, www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million. Accessed 27 Nov. 2020.

[15] Haig, Samuel. "Microsoft Employee Sentenced to 9 Years in First U.S. Bitcoin Case Involving Tax Fraud." *Cointelegraph*, 10 Nov. 2020, cointelegraph.com/news/microsoft-employee-sentenced-to-9-years-in-first-u-s-bitcoin-case-involving-tax-fraud. Accessed 27 Nov. 2020.

> *In July 2019, law-enforcement agents searched Kvashuk's lakefront home in Renton. Kvashuk purchased the home using approximately $1.675 million in criminal proceeds in April 2018. Inside the home, agents found numerous records that incriminated Kvashuk, such as: (1) an electronic document that contained Kvashuk's working notes during the criminal scheme, including the email addresses and other log-in information for the compromised test accounts; (2) screenshots of 5x5 codes, which had been purchased using the compromised test accounts and displayed on Kvashuk's computer monitor at the time of purchase; (3) files that that tracked numerous 5x5 codes that had been purchased using the compromised test accounts; and (4) proof that Kvashuk had installed tools on his digital devices that anonymized aspects of his internet activity.*[16]

Kashuk had tipped off the IRS with massive deposits to a personal account, and filed a fake tax return while making lavish purchases. The evidence in his home was the confirmation that investigators needed to uncover the use of cryptocurrency. It was mistakes in the physical world that gave Kashuk away and tipped off the authorities to the use of Bitcoin. The cryptocurrency became evidence after the crime was revealed. If the crime had been executed with more discipline, it is unlikely that Bitcoin mixing in order to launder money would have been the evidence that exposed the criminal.

What is interesting here is what part the Bitcoin mixers played in the crime and how conspicuous that aspect actually was. "Bitcoin Mixers, also known as Bitcoin Tumblers, are services that sever the connection between the user's old and new address by mixing their BTC

---

[16] "Ex-Microsoft Dev Gets 9 Years in Prison Over $10M Theft Involving Bitcoin Mixing." *CoinDesk*, 10 Nov. 2020, www.coindesk.com/ex-microsoft-employee-prison-bitcoin-mixing-crime. Accessed 27 Nov. 2020.

with other users in the mixing pool, thereby disassociating the original coins with the owner."[17] This is technology built into cryptocurrency to increase the anonymity of the user. A mixer service will take your coins and mix them with other users' coins so when you get them back, it is unknown where the coins initially came from. These services can also break coins up into fractions and combine them with other broken coins that help hide the origins of the coin when it is issued back out. It is unlikely that law-enforcement could have caught Kvashuk based on his Bitcoin activities. If Kvashuk exercised discipline in his deposits and purchases, it would have been very difficult for authorities to detect any criminal activity. Even before he decided to use Bitcoin, Kvashuk was under suspicion by fellow employees and Microsoft for the transactions that he was conducting while at work. Clearly, Kvashuk was not a capable criminal and unfamiliar with the fundamentals of effective money laundering. He would have likely been apprehended and sentenced even without the use of Bitcoin. However, this case introduces us to another layer of mixing that can obfuscate potential fraud and tax evasion for a more savvy criminal. One can deliver funds through cryptocurrency using a wallet number as the only form of identification and employ mixers as an additional layer of anonymity. Combined with proper integration, the use of cryptocurrency can become very difficult to detect.

The DOJ v. Mexican drug cartel crypto-laundering case

The 2020 case of The United States v. Xizhi Li, Jianxing Chen, Jinguan Li, Eric Yong Woo, Jiayu Chen, and Tao Liu is a very complicated example of how money laundering can be

[17] "Bitcoin Mixer | Best Bitcoin Tumbler | MyCryptoMixer.com." *Mycryptomixer.com*, mycryptomixer.com/.

used to support Mexican Cartel cocaine trafficking. The six men from China used several methods of money laundering to clean money for the Mexican cartels including bulk cash smuggling, use of foreign and domestic bank accounts, and casinos as fronts for a legitimate business. The DOJ has charged all six men with up to 14 crimes ranging from conspiracy to distribute cocaine to money laundering and bribery. The two charges most relevant to our analysis are the attempted identity fraud and bribery. As typically seen in international money laundering, criminals often purchase goods in the U.S. that are then shipped to sell in China or move funds into Chinese accounts to then make purchases in Latin America by drug trafficking organizations.[18] This case differs from typical schemes with the perpetrators' use of cryptocurrency to bribe State Department employees to create fraudulent United States passports.

Each member of the six that were indicted had a role. Tao Liu is the subject of all 14 charges in the indictment including attempted identity fraud and bribery. Tao was tasked to secure fraudulent United States passports from a contact in the State Department.[19] The goal was to exploit a new State Department employee who was charging $150,000 for fraudulent passports by sending funds through cryptocurrency for the employee to then transfer into fiat and deposit in a bank account. The purpose of using cryptocurrency in this case was to avoid the source of the funds being traced back to Tao. If the sender is able to create a one time use wallet under an alias (Tao Li has 8 known aliases) then the source of the funds will be relatively unknown. The acquisition of these passports would allow for easier access to more countries and the ability to receive contracts from a larger pool of drug trafficking organizations.

---

[18] "THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA." *The United States Department of Justice*, The United States Department of Justice, Sept. 2020, www.justice.gov/opa/press-release/file/1328016/download. Accessed 2 Dec. 2020. Pg. 5

[19] Id. 12 Pg. 1

What Tao was not aware of was that the two contacts that he was working with were undercover agents for the DEA. Agent 1 ran as a go between for Tao and the supposed State Department employee. Agent 2 acted as the employee receiving and depositing Tao's money for the fraudulent passports. The first two transactions of $1,000 and $4,000 were sent in cryptocurrency transferred into USD and deposited by Agent 2 into a Bank of America account. This must have earned Tao's trust because the second two transactions of $2,000 and $3,000 were sent directly from a JP Morgan account to the agents Bank of America account.[20] It is unclear if the agents had sufficient evidence from the crypto transfer to prosecute, but the wallet that received the cryptocurrency transfer was controlled by the DEA and the indictment claims that the funds were transferred for the specific purpose of purchasing fraudulent passports.

Though the criminals in this case were caught, it is an excellent example of the importance of KYC with regards to cryptocurrency. If Tao had vetted his source to the State Department more thoroughly, he may have evaded the DEA and likely any other authorities. What remains unclear is the validity of the evidence that the DEA had without the bank to bank transfers. There can be no doubt that Tao used cryptocurrency to send the initial funds, but if all of the transfers had been completed in a similar manner, there is no indication that the DEA would have had a clear picture of the source of the cryptocurrency other than Tao's own admission. These transfers were also conducted with the DEA having complete awareness and control over the receiving account of the cryptocurrency. There is no indication in the indictment if Bank of America knew that the funds deposited in Agent 2's account were from cryptocurrency or otherwise. What this case truly exposes is that financial institutions must

[20] Id. 12 Pg. 18

maintain a heightened KYC program in order to defend against the potential for cryptocurrency to allow money laundering to remain undetected.

However, what these six were indicted for is only part of the story. It has become more common for Mexican cartels to launder money through cryptocurrency as well. It is very easy for criminals to enter multiple accounts under several pseudonyms that do not have to be associated with a real person and transfer large amounts of money across international borders with little interference from authorities. With the use of Bitcoin mixers, the money can be drawn out as fiat currency in China and used to purchase luxury items that are then sent back to Latin America to be sold by the cartels for a profit in what looks like a legitimate business. To make matters worse, there are several businesses that now accept cryptocurrency as payment for services and products without the need to first transfer to fiat currency. Some of these companies are relatively unknown like BitDials or Bitluxuria.[21] There are others much more well known like Microsoft, Home Depot, and overstock. This is just another option for a money launderer to integrate currency to avoid detection. It is unlikely that a criminal would use a company like Home Depot to conduct its business, but the ability to purchase products directly is continuing to grow and there is less need for money launderers to use an exchange to obtain fiat currency. In this case, it is likely that the Mexican cartels were using the Chinese money launderers to exchange fiat currency in the United States for cryptocurrency and then purchasing products in China to ship back to Mexico to ultimately be sold by cartels. Furthermore, it is likely that this was not a part of the indictment as it has not been processed yet by U.S. authorities.

---

[21] Vassanelli, Eleonora. "Money Laundering and Cryptocurrencies: A Case Study of Mexican Drug Cartels." *Crossfire KM*, www.crossfirekm.org/articles/money-laundering-and-cryptocurrencies-a-case-study-of-mexican-drug-cartels. Accessed 4 Dec. 2020.

PlusToken: Anatomy of a Crypto Ponzi Scheme

After a drop in cryptocurrency scam revenues in 2018, scammers more than tripled their revenue in 2019, raking in an estimated $4.3 billion in cryptocurrency from millions of victims. It's worth noting however, that approximately half of this revenue can be attributed to one scam alone: the PlusToken scheme. Based in China and operating predominantly in Asia, PlusToken was an investment Ponzi scam that promised to reward investors with high rates of return upon purchasing its associated Plus cryptocurrency token. PlusToken attracted millions of its victims by pushing an aggressive marketing strategy with messaging apps like WeChat and Whatsapp through which they promoted lavish promises of 10-30% returns in public groups. Though the vast majority of PlusToken investors were ordinary people without any particularly shrewd background in cryptocurrency, PlusToken scammers were also able to dupe knowledgeable investors with the promise of up to 30% returns.[22] The marketing efforts of the scheme went to extreme lengths: hosting several in-person info sessions, taking out ads in supermarkets, and even taking photos with their founders and Prince Charles of England. Evidently, the PlusToken scammers were no novices when it came to developing a sophisticated marketing campaign that would ultimately grant them an air of legitimacy. To further their perpetuated front as a legitimate company, PlusToken paid some money out to early investors to maintain the illusion of high returns - the foundational characteristic of a Ponzi scam. However, in this particular case, it is slightly more difficult to differentiate between funds moving to duped early investors and transfers sent to addresses under the scammers' control.

---

[22] Sedgwick, Kai. "The 187,000 BTC Scam – Is Plustoken to Blame for Bitcoin's Sell-Off?" *Bitcoin*, 28 Nov. 2019, news.bitcoin.com/is-plustoken-to-blame-for-bitcoins-sell-off/.

Ultimately, about 800,000 ETH and 45,000 BTC out of an estimated total of 180,000 BTC and 6,400,000 ETH can be definitively identified as funds transferred to the scammers own addresses to launder. While about 790,000 ETH has been sitting in a single Ethereum wallet for months (the other 10,000 ETH was cashed out), the flow of the 45,000 BTC seemed far more sophisticated. 20,000 BTC was cashed out, yet the other 20,000 BTC is spread out across more than 8,700 crypto addresses after having been transferred more than 24,000 times. Like other instances of attempts to obfuscate the source of bitcoin funds, many of these 24,000 transactions were self-shuffled or processed through bitcoin mixers in which the funds were split off into various unique addresses and then re-consolidated again. PlusToken first attempted to mix their funds through self-shuffling, a process that resembles a bitcoin mixer; however, the scammers' self-shuffling attempts were severely damaged by reusing addresses and creating deterministic links. The primary goal of mixing is to create a number of different transaction interpretations which make it difficult for an observer to connect input and output addresses. But by using the same addresses pre and post-shuffling, the scammers failed to break such deterministic links making it relatively easy for investigators to track the transaction process. Even worse, following self-shuffling, the outputs were typically consolidated into single addresses of more than 50 BTC and sent to the Huobi exchange after only a few transactions. Even PlusToken's mixing efforts through Wasabi Wallet, a popular bitcoin mixing service, suffered from abnormally high rates of eventual address reuse.[23] Again, when addresses are reused and post-mix outputs are merged together, it becomes relatively easy to track the funds and even easier to conclude common ownership.

[23] ErgoBTC. "Tracking the PlusToken Whale: Attempted Bitcoin Mixing and Its Impact on Wasabi Wallet." *Medium*, 23 Oct. 2019, medium.com/@ErgoBTC/tracking-the-plustoken-whale-attempted-bitcoin-laundering-and-its-impact-on-wasabi-wallet-787c0d240192.

Ultimately, nearly all of the funds that were cashed out moved to the address of a Huobi OTC (Over the Counter) broker to be liquidated. An OTC broker facilitates trades between individual buyers and sellers at a set, negotiated price. Though these brokers are affiliated with an exchange, they operate independently and typically have substantially lower KYC requirements than most exchanges - hence the PlusToken scammers appeal. While many OTC brokers operate completely legitimately for those who don't want to transact on an open exchange, other independent brokers have taken advantage of lower KYC requirements to offer services to those transacting in illicit funds. In fact, some OTC brokers specialize exclusively in laundering money and exchanging dirty cryptocurrency for fiat money. It's worth noting that at the time of the exceedingly large transfers of Bitcoin from PlusToken wallets to Huobi OTC brokers, Bitcoin spot prices experienced heightened volatility and a significant drop in value. Of course, it may be difficult to prove causation in this case, but the substantial increase in supply of Bitcoin at the time of PlusToken liquidations is very likely to have triggered such price drops.

In June 2019, six ringleaders of the PlusToken Ponzi scheme were arrested in Vanuatu. After deceptively drawing in 2.4 - 3 million users and nearly $3 billion dollars of investments, their charade came to a grinding halt. The PlusToken scam represents a prime example of the damage illicit cryptocurrency schemes can inflict on innocent victims. Even beyond direct investors, analyses have demonstrated the significant effects large liquidations of illicitly obtained funds have on cryptocurrency prices. In order to prevent similar schemes from wreaking widespread havoc, regulators and exchanges must continue to take meaningful strides to prevent such pernicious deception and illicit behavior.

Common Risks and Steps Banks Should Take

While there is profound excitement surrounding the emergence and growth of blockchain technology, cryptocurrency transactions remain a threat to the compliance functions of banks and financial service companies alike. Naturally, banks do not need to clear or settle crypto transactions directly for money laundering or sanctions evasion risks to emerge. Banks certainly have robust KYC information; but without proper safeguards, there is little preventing their exposure to cryptocurrency flows and, more importantly, illicit behavior. The absence of proper technology or awareness can make it extremely difficult for traditional banks to track the movement of funds. As the previous case studies have demonstrated, there are a variety of ways in which money laundering and sanctions evasion crypto schemes can either bypass poor compliance systems or successfully obfuscate the true source of funds. Some of the most prominent threats to financial security include OTC brokers, mixing services, and unregulated cryptocurrency exchanges. Many cryptocurrency enthusiasts have praised OTC brokers and mixing services as countermeasures to resist would-be surveillance of their transaction histories. However, as digital privacy is considered by many to be a fundamental right, crypto fungibility and enhanced anonymity prevent financial institutions from differentiating between legitimate users and illicit actors. Naturally, privacy and compliance are two seemingly incompatible, yet important ends that both deserve a reasonable, well-conceived approach. As exchanges and financial service providers make greater strides in monitoring transactions and enforcing KYC requirements, privacy enthusiasts will only continue to seek out alternative ways to protect their anonymity.

Beyond the risks posed by OTC brokers and cryptocurrency mixing services, there is a far more basic threat deterring proper crypto due diligence: the widespread number of cryptocurrency exchanges without proper KYC systems in place. In 2020, Ciphertrace

investigated over 800 virtual asset service providers (VASPs) in over 80 countries and found that 56% of VASPs globally have weak or porous KYC protocols.[24] While 56% may be an upgrade from last year's finding that 65% of the most popular crypto exchanges have weak or porous KYC, there are still far too many exchanges with inadequate KYC measures in place. An excessively high percentage of VASPs with poor KYC enables criminals to exploit deficiencies and launder money with relative ease. Ciphertrace also found that approximately 85% of the providers that fail to disclose the country they are registered in have weak or porous KYC. For financial institutions looking to effectively monitor their clients' transaction flows linked to cryptocurrency exchanges, it is imperative to differentiate exchanges with strong KYC from those with inadequate compliance standards. Knowing that a certain exchange does not disclose the country they are registered in should be a jarring AML red flag for any financial service company that comes across such a suspicious provider. A prudent approach to integrating cryptocurrency into a bank's current operations would be to first identify exchanges with robust KYC requirements.

Given the reality that many exchanges are still far behind in their compliance standards, banks should treat crypto exchanges cautiously and ensure clients steer clear of KYC-deficient platforms. While banks, for the time being, generally aim to avoid crypto transactions altogether, generating a proper risk scoring system to identify trustworthy exchanges could gradually make banks more willing to process transactions that would otherwise be restricted by their internal policies. In partnering, to whatever extent, with compliant exchanges, banks could also begin implementing KYT (Know Your Transaction) programs that are better tailored to blockchain

[24] "2020 Geographic Risk Report: VASP KYC by Jurisdiction." *Ciphertrace*, ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/.

technology.[25] A digital ledger enables observers to trace the entire history of crypto transactions, a record that cannot be fabricated or tampered with in any way. As a result, blockchain technology, by its own nature, has tremendous benefits for monitoring transactions and tracing the flow of funds back to its original source. Banks would be able to leverage blockchain technology and a robust KYC/KYT mechanism to monitor flows far more effectively as criminals would simultaneously be less capable of masking their transactions. While criminals' crypto anonymity presents a major threat to financial institutions' compliance functions today, proper implementation of blockchain technology and immutable ledgers may very well revolutionize AML compliance in the decades to come.

In addition to implementing blockchain to the benefit of AML monitoring, banks may also be able to capitalize on the need for cryptocurrency custodian services. Cryptocurrencies and exchanges - as demonstrated in recent years by malicious groups such as Lazarus - often fall victim to fraud, malware, and hacks. As security issues persist, so will the need for proper storage and maintenance of cryptocurrency assets; and banks may be in the best position to offer such solutions. Banks already offer clients exceedingly secure cyber protection for financial holdings and records, so expanding to provide similar services for crypto assets would seem rather reasonable. In July 2020, the Treasury's Office of the Comptroller of Currency (OCC) published an interpretive letter clarifying that all chartered U.S. banks are clear to custody cryptocurrencies.[26] The OCC's opinion certainly provides more certainty to banks that have traditionally made conservative crypto risk assessments. In the future, even greater regulatory assurance can propel banks to capitalize on this emerging, lucrative opportunity. No other

[25] Mogul, Zubin, et al. "How Banks Can Succeed with Cryptocurrency." *Boston Consulting Group*, 5 Nov. 2020, www.bcg.com/publications/2020/how-banks-can-succeed-with-cryptocurrency.
[26] De, Nikhilesh. "The OCC's Crypto Custody Letter Was Years in the Making." *Coindesk*, 18 Aug. 2020, www.coindesk.com/occ-crypto-custody-years.

entities can parallel banks' reputations and track records of providing traditional custodian services, and some estimates even suggest that crypto custody could generate revenue of up to 1% per annum of underlying assets. With regulatory approval and an open digital custody market, the greater risk may not be associated with entering this emerging space but of missing opportunities to do so.

In the end, there are both risks and profitable opportunities that will continue to emerge with the growth and greater adoption of cryptocurrency. Many banks have traditionally remained rather risk-averse when it comes to crypto and have only recently begun expanding into areas in which they believe they can capitalize on potential profit. On the other hand, unwitting exposure to cryptocurrency flows continues to plague many financial service companies. If banks continue to neglect such exposure, they may not become aware of their relation to crypto flows until it is too late. Cryptocurrency does not have to be a wild west endeavor for banks, and greater comfort in dealing with digital assets starts, first and foremost, with addressing one's own exposure.

Works Cited

"U.S. Department of the Treasury." Home.Treasury.Gov, 19 Mar. 2018, home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626. Accessed 8 Nov. 2020.

"About FSOC | U.S. Department of the Treasury." Home.Treasury.Gov, home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/about-fsoc. Accessed 17 Nov. 2020.

Baldwin, David A. "The Sanctions Debate and the Logic of Choice." International Security, vol. 24, no. 3, Jan. 2000, pp. 80–107, 10.1162/016228899560248. Accessed 21 May 2020.

"Bitcoin Blockchain Size 2010-2019 | Statista." Statista, Statista, 2010, www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/.

"Bitcoin Mixer | Best Bitcoin Tumbler | MyCryptoMixer.com." Mycryptomixer.com, mycryptomixer.com/.

CISA. “Ransomware | CISA.” Www.Cisa.Gov, 2020, www.cisa.gov/ransomware. Accessed 11 Nov. 2020.

“Cryptocurrency and OFAC: Beware of the Sanctions Risks.” JD Supra, 24 Jan. 2020, www.jdsupra.com/legalnews/cryptocurrency-and-ofac-beware-of-the-34002/.

De, Nikhilesh. “The OCC’s Crypto Custody Letter Was Years in the Making.” *Coindesk*, 18 Aug. 2020, www.coindesk.com/occ-crypto-custody-years.

“Ex-Microsoft Dev Gets 9 Years in Prison Over $10M Theft Involving Bitcoin Mixing.” CoinDesk, 10 Nov. 2020, www.coindesk.com/ex-microsoft-employee-prison-bitcoin-mixing-crime. Accessed 27 Nov. 2020.

“Former Microsoft Software Engineer Sentenced to Nine Years in Prison for Stealing More than $10 Million in Digital Value Such as Gift Cards.” Www.Justice.Gov, 9 Nov. 2020, www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million. Accessed 27 Nov. 2020.

Haig, Samuel. “Microsoft Employee Sentenced to 9 Years in First U.S. Bitcoin Case Involving Tax Fraud.” Cointelegraph, 10 Nov. 2020, cointelegraph.com/news/microsoft-employee-sentenced-to-9-years-in-first-u-s-bitcoin-case-involving-tax-fraud. Accessed 27 Nov. 2020.

“THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRlCT OF VIRGlNIA.” The United States Department of Justice, The United States Department of Justice, Sept. 2020, www.justice.gov/opa/press-release/file/1328016/download. Accessed 2 Dec. 2020.

“J.P. Morgan Creates Digital Coin for Payments.” www.Jpmorgan.com, www.jpmorgan.com/solutions/cib/news/digital-coin-payments. Accessed 18 Nov. 2020.

Kauflin, Jeff. “Why Everyone In Crypto Is Talking About DeFi.” Forbes, 26 Oct. 2020, www.forbes.com/sites/jeffkauflin/2019/04/26/why-everyone-in-crypto-is-talking-about-defi/#1b8976b5723f.

Konowicz, Deane. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION. 1. REPORT DATE (DD-MM-YYYY) Paper Awards Submission 3. DATES COVERED (From -To). 3 May 2018.

Mogul, Zubin, et al. “How Banks Can Succeed with Cryptocurrency.” *Boston Consulting Group*, 5 Nov. 2020, www.bcg.com/publications/2020/how-banks-can-succeed-with-cryptocurrency.

Post, Kollen. “US Sanctions Strategy and Crypto: The Cracks Are Showing in Iran.” Cointelegraph, 15 Mar. 2020, cointelegraph.com/news/us-sanctions-strategy-and-crypto-the-cracks-are-showing-in-iran. Accessed 21 Oct. 2020.

Ratna, Tanvi. “Iran Has a Bitcoin Strategy to Beat Trump.” Foreign Policy, 24 Jan. 2020, foreignpolicy.com/2020/01/24/iran-bitcoin-strategy-cryptocurrency-blockchain-sanctions/.

Roberts, Jeff. “Crypto Soars Again as Traders Embrace ‘DeFi’ and ’Yield Farming’—but Some See Echoes of the 2017 Bubble.” Fortune, 25 Aug. 2020, fortune.com/2020/08/25/crypto-defi-yield-farming-bitcoin/. Accessed 24 Oct. 2020.

Rudden, Jennifer. “Cryptocurrency Market Value 2013-2019.” Statista, 6 Nov. 2020, www.statista.com/statistics/730876/cryptocurrency-maket-value/#:~:text=Cryptocurrency%20market%20capitalization%202013%2D2019&text=The%20cumulative%20market%20capitalization%20of. Accessed 8 Nov. 2020.

“Sanctions Compliance for Banks in the Age of Crypto-Assets.” Financial Crime In Focus, 5 June 2020, blogs.lexisnexis.com/financial-crime-in-focus/sanctions-compliance-for-banks-in-the-age-of-crypto-assets/. Accessed 11 Nov. 2020.

ShapeShift. “What Are Privacy Coins?” Medium, 4 Mar. 2020, medium.com/shapeshift-stories/what-are-privacy-coins-6df8622ebf76#:~:text=Privacy%20coins%20are%20unique. Accessed 11 Nov. 2020.

Shimron, Leeor. “Crypto Exchanges And Bitcoin Are Poised For Massive Growth By 2030.” Forbes, 20 June 2020, www.forbes.com/sites/leeorshimron/2020/06/20/crypto-exchanges-and-bitcoin-are-poised-for-massive-growth-by-2030/?sh=48280d423f83. Accessed 8 Nov. 2020.

“Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group | U.S. Department of the Treasury.” Home.Treasury.Gov, 2 Mar. 2020, home.treasury.gov/news/press-releases/sm924.

“Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack.” www.Justice.Gov, 2 Mar. 2020, www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack. Accessed 6 Nov. 2020.

Vassanelli, Eleonora. “Money Laundering and Cryptocurrencies: A Case Study of Mexican Drug Cartels.” Crossfire KM, www.crossfirekm.org/articles/money-laundering-and-cryptocurrencies-a-case-study-of-mexican-drug-cartels. Accessed 4 Dec. 2020.

“White House Press Briefing by Treasury Secretary Steven Mnuchin on Regulatory Issues Associated with Cryptocurrency | U.S. Department of the Treasury.” Treasury.Gov, 22 Oct. 2019, home.treasury.gov/news/press-releases/sm731.

“2020 Geographic Risk Report: VASP KYC by Jurisdiction.” *Ciphertrace*, ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/.