

Cryptocurrency Crime and Anti-Money Laundering Report

CipherTrace
Cryptocurrency Intelligence
February 2021



About CipherTrace

CipherTrace enables the blockchain economy by protecting cryptocurrency companies and financial institutions from security and compliance risks. Years of research have gone into developing the world's most complete and accurate cryptocurrency intelligence and forensics, covering more than 800 currencies. This visibility into the blockchain and virtual asset businesses helps protect banks and exchanges from cryptocurrency laundering risks, while protecting user privacy. CipherTrace also works with government agencies to bridge the gaps between regulation and the world of cryptocurrencies and blockchain.

CipherTrace is a founding member of TRISA, the leading open-source industry standard to meet the Travel Rule requirement for secure information sharing while protecting cryptocurrency user privacy. TRISA enables cryptocurrency companies to comply with the Financial Action Task Force regulations that will shape the world of cryptocurrencies and bring them to institutional prominence as investment and cross-border payment technologies. Learn about the open-source Travel Rule Information Sharing Architecture at trisa.io.

Table of Contents

- [Highlights..... 6](#)
- [Executive Summary 7](#)
- [2020 Major Trends and Developments 9](#)
 - [\\$3.5 Billion Sent from Criminal BTC Addresses in 2020.....9](#)
 - [One US Exchange Sent More than \\$36.7 Million *Directly* to Criminals in 2020.....9](#)
 - [US Exchanges Sent \\$41.2 Million *Directly* to Criminals10](#)
 - [Over Half of 2020 Crypto Hacks are from DeFi Protocols.....10](#)
 - [DeFi Rug Pulls Emerge as Top Exit Scam.....12](#)
 - [Future of DeFi Hacks, Scams, and Regulation13](#)
 - [FinCEN’s Proposed Rulemaking Creates New Reporting and Record-Keeping Requirements for Transactions to Unhosted Wallets14](#)
 - [Unhosted Wallets Dominate BTC Volume Going to and from US Exchanges 16](#)
 - [Potential Implications of the Proposed Rule..... 17](#)
 - [Difficulty in determining “cross-border payments” in the virtual asset world 19](#)
 - [1/3 of Cross-Border Bitcoin Volume is Sent to Exchanges with Demonstrably Weak KYC20](#)
 - [US Spotlight 20](#)
 - [Cross Border BTC Volume Around the Globe..... 21](#)
 - [Exchanges Receive Over Half of BTC Payments in 202023](#)
 - [Percentage BTC Volume Sent to High-Risk Exchanges Reaches All-Time Low25](#)
- [Terrorist Use of Cryptocurrency in 202026](#)
 - [DOJ Seizures of Cryptocurrency Donations Puts a \\$2 Million Hole in Terrorist Finances26](#)
 - [French Police Arrest Twenty-Nine in Cryptocurrency Terrorism Financing Scheme27](#)
- [Major 2020 Enforcement Actions.....28](#)
 - [BitMEX Executives Charged with Illegal Operations and Anti-Money Laundering Violations28](#)
 - [Ripple, Execs Face SEC Lawsuit30](#)
 - [FinCEN Fines Operator of Helix Mixer \\$60M for Bitcoin Laundering Scheme Linked to Notorious Dark Markets30](#)
 - [BitGo Enters Into \\$98,830 Settlement with US Treasury Over Multiple Crypto Sanctions Violations32](#)
 - [FBI and German Police Charge Operators of movie2k.to and Seize \\$30 Million in Crypto32](#)
 - [US Attorney's Office Charges Man with Operating Unlicensed ATM Network33](#)
 - [Fifteen Plead Guilty After Implication in International Crypto-Crime Ring.....34](#)
 - [DOJ Charges Founder of “AML Bitcoin” with Money Laundering.....34](#)
 - [SEC Orders Telegram to Return \\$1.2 Billion to Investors, Pay \\$18.5 Million Penalty35](#)

| | |
|--|-----------|
| Chinese Authorities Arrest Over 100 People for Involvement in the PlusToken Ponzi Scheme | 35 |
| US Prosecutors Attempt to Return \$6.5 Million in Crypto to Victims of Ponzi Scam | 36 |
| Centra Tech Inc. Co-Founder Implicated in \$25 Million Scam | 36 |
| \$15 Million in Crypto and Supercars Seized as Chinese Police Bust Arbitrage Scam | 37 |
| Police Arrest BitGrail Boss for His Role in Largest Cyber-Financial Attack in Italy..... | 37 |
| Promoter of Australian Cryptocurrency Lending Scheme Sentenced to 20 Years..... | 38 |
| The US DOJ Seized \$24 Million from a Brazilian Cryptocurrency Investment Scheme | 38 |
| IRS Calls Sentencing of Ukrainian National the First Case of Bitcoin Tax Fraud in US | 39 |
| OKEx Founder "Star" Xu is Being Held in Police Custody | 39 |
| Global Cryptocurrency Money-Laundering Cartel Busted—20 Arrested | 40 |
| Bitcoin Escrow Company CEO Pleads Guilty to Fraud and Embezzlement..... | 41 |
| Crypto Trader Charged with Fraud and Ordered to Repay Over \$6 Million to Investors | 41 |
| Coincheck Hack Proceeds Seized in Japan’s First Official Seizure of Cryptocurrency | 41 |
| Justice Department Charges Airbit Founders with Cryptocurrency Mining Fraud | 42 |
| Malaysian Authorities Arrest Crypto Miners That Stole \$600K+ in Electricity | 42 |
| OCC Hits Bank with First-Ever Enforcement Action for Lack of Crypto AML Compliance | 43 |
| Major Thefts, Scams, and Fraud | 44 |
| Social Media Giant Twitter Compromised by Insiders | 44 |
| Cryptocurrency Exchange KuCoin's Hot Wallets Hacked for Millions | 45 |
| DeFi Hackers Use Complex Attack to Steal \$500,000 From Balancer | 45 |
| Instagram Influencer “Hushpuppi” Hides \$14 Million of Stolen Funds in Bitcoin | 46 |
| New Zealand Police Seize \$90 Million in Investigation of BTC-e Exchange..... | 47 |
| Nexus Mutual CEO Hacked for Over \$8 Million in NXM Tokens..... | 47 |
| \$2.5 Million in Crypto Stolen Through SIM Card Hacks by Irish Man | 48 |
| Argentina’s National Immigration Agency Hacked by Ransomware Group..... | 48 |
| Slovakian Crypto Exchange Eterbase Loses \$1.6 Million in Hot Wallet Hack | 49 |
| Wotoken Ponzi Scheme Defrauds Investors of Over \$1B Worth of Crypto | 49 |
| 2020 Technical Hacks..... | 50 |
| Changes in Global Regulatory Environment | 53 |
| Current Implementation of AML/CTF Regulations Globally..... | 53 |
| FATF—Revised Standards on Virtual Assets 12-Month Review | 54 |
| FATF—Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing | 55 |
| EU—Crypto Businesses Faced with AMLD5 Regulation | 56 |

| | |
|--|------------------|
| US—FinCEN Releases New Proposed Rule Aimed at Closing AML Gaps from Unhosted Wallets | 56 |
| US—FinCEN, OFAC Warn VASPs of Potential Sanctions Violations | 57 |
| US—National Defense Authorization Act for Fiscal Year 2021 (H.R.6395)..... | 57 |
| US—OCC Issues Statement Allowing Banks to Hold Crypto Assets for Customers | 58 |
| US—4th Amendment Does Not Protect Bitcoin Data, Says US Appeals Court..... | 58 |
| US—DOJ Publishes Cryptocurrency Enforcement Framework | 59 |
| UK—FCA Becomes AML and CTF Supervisor for UK Cryptoasset Activities | 59 |
| UK—FCA Issues Notice to UK Cryptoasset Businesses | 60 |
| UK—New National Risk Assessment of Money Laundering and Terrorist Financing | 60 |
| France—Mandatory KYC Rules for All Cryptocurrency Transactions on the Horizon | 60 |
| South Korea—New Tax Targets Crypto Traders..... | 61 |
| South Korea—Plans to Ban Privacy Coins..... | 61 |
| Kyrgyzstan—National Bank Developing New Cryptocurrency Laws..... | 62 |
| Pakistan—Creation of Crypto Framework in the Works | 62 |
| <i>Central Bank Digital Currencies</i> | <i>63</i> |
| BIS—Central Banks Reject Popular Narrative Regarding CBDC Issuance Motives..... | 63 |
| US—National Banks Can Use Stablecoins to Facilitate Payments, OCC Says | 63 |
| US—Federal Reserve Board Governor Announces Co-Op with MIT to Research Digital Currency | 64 |
| The Bahamas—Sand Dollar Sees Retail Use | 65 |
| China—Central Bank Digital Currencies Make Big Strides Forward..... | 65 |
| Sweden—Taking Next Step on CBDC Development..... | 65 |
| Australia—The CBDC Race Heats Up Down Under | 66 |
| Brazil—President of Central Bank Sees CBDCs as the Future of Finance | 66 |
| Private Sector—Citigroup Working with World Governments to Build CBDCs | 66 |
| IOSCO—Global Stablecoins May Be Subject to Securities Regulation | 67 |
| <i>Sanctioned Countries.....</i> | <i>68</i> |
| Russia..... | 68 |
| Iran | 69 |
| North Korea..... | 69 |
| Venezuela | 71 |

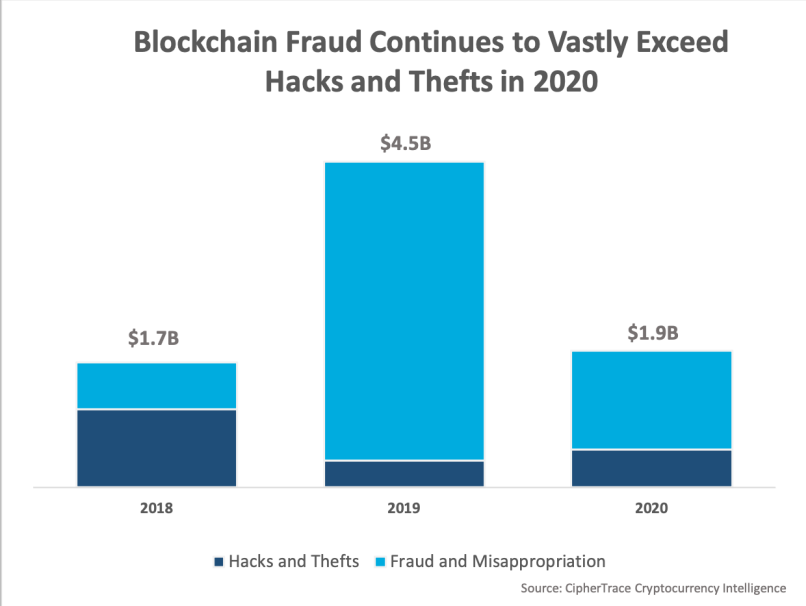
Highlights

Highlights of key findings are as follows:

- As legitimate cryptocurrency use goes up, crypto crime as a percentage goes down. 2020 crypto crime was \$1.9 billion in 2020, down 57% from 2019's \$4.5 billion.
- Decentralized finance (DeFi) is the next major threat vector for fraud and money laundering: half of all thefts in 2020, totaling \$129 million, were DeFi-related hacks and centralized exchange, such as Shapeshift, are transforming into a decentralized exchange (DEX) to avoid KYC requirements.
- Exchange executives face arrest, extradition, and massive fines, as individuals are held personally accountable for money laundering violations.
- Fraud is the dominant cryptocurrency crime, followed by theft and ransomware.
- US exchanges sent \$41.2 million worth of BTC directly to criminals in 2020.
- 84% of the bitcoin moved in exchange-to-exchange transactions was moved cross-border.
- A third of cross-border Bitcoin volume is sent to exchanges with demonstrably weak KYC.
- Forty-one percent of the total cross-border BTC volume sent from US VASPs went to VASPs with demonstrably weak KYC; 50% of cross-border volume received by US VASPs is from exchanges with demonstrably weak KYC.
- Seventy-eight percent of BTC Volume from South Korean VASPs is from exchanges with demonstrably weak KYC.
- FinCEN's proposed rule change to the "Travel Rule" threshold would more than double the number of "Travel Rule" messages needed to be sent by US VASPs.
- Fifty-two percent of BTC payment volume was sent to exchanges in 2020; 40% sent to private wallets.
- The US leads the world in receiving bitcoin, with 19.3% of BTC sent to exchanges globally received by US-domiciled VASPs. Ten percent of all BTC payments were sent to US-domiciled VASPs.
- The percentage of global BTC volume sent to high-risk exchanges was at an all-time low, with a 59% drop from 2019.

Executive Summary

CipherTrace’s 2020 Cryptocurrency Crime and Anti-Money Laundering Report reveals that in 2020, major crypto thefts, hacks, and frauds totaled \$1.9 billion—the second-highest annual value in crypto crimes yet recorded.



Massive exit scams have dominated cryptocurrency crimes in the last two years. In 2019, the Ponzi scheme PlusToken netted \$2.9 billion with its exit scam— 64% of the year’s major crime volume. 2020 saw WoToken, a similar scheme operated by some of the same people as PlusToken, defraud investors out of \$1.1 billion in its exit scam—58% of 2020’s major crime volume. While major fraud volume saw a significant decrease, it still made up 73% of 2020’s crime total.

While 2019 and 2020 saw a similar number of thefts, hacks, and fraud, the average value¹ taken by criminal actors in 2019 was 160% higher than in 2020, indicating maturity in the crypto space as entities continue to harden systems and take precautions against inside and outside threats. While 2020 did see a large \$281 million hack of cryptocurrency exchange KuCoin, the exchange claims to have already recovered 84% of the stolen funds—something almost unheard of in previous years.

Another factor contributing to this discrepancy is that 2020 was overrun by dozens of DeFi related hacks and scams, which were much smaller in size. Half of all 2020 crypto hacks were of DeFi protocols—a pattern that was virtually negligible in all prior years—and nearly 99% of major fraud volume in the second half of 2020 stemmed from DeFi protocols performing “rug pulls” and other exit scams in a pattern eerily reminiscent of the

¹ This is the average value after excluding the large PlusToken and Wotoken outliers.

2017 ICO craze. In a rug pull, which is similar to a pump and dump, some investors will liquidate the entire DeFi pool, leaving the remaining token holders with no liquidity and unable to trade, wiping out the remaining value.

On the regulatory front, the crypto-sphere has been inundated with new legal attention as regulatory and policy making bodies weigh in on how the space should operate. In the US, FinCEN has proposed two major rule changes to the regulatory obligations banks and virtual asset service providers (VASPs) face when conducting certain virtual currency transactions.

One notice of proposed rulemaking (NPRM) issued in October sought to amend the recordkeeping and Travel Rule regulations to collect, retain, and transmit transfer information on international payments at a much lower threshold. As it stands, financial institutions currently transmit records for any transfers in excess of \$3000. The new rule would see much smaller transfers—anything over \$250—come under the same requirements if the transmittal of funds begins or ends outside the United States. The rule specifically includes cryptocurrency transfers as a class of transactions to which the proposal would apply.

Another NPRM issued in December would require banks and VASPs to verify the identity of their customers, keep records of virtual currency transactions greater than \$3,000, and submit CTR-like reports for virtual currency transactions over \$10,000, if the counterparty in the transaction uses an unhosted (noncustodial) or “otherwise covered” wallet. The NPRM defines “otherwise covered” wallets as wallets held at a financial institution that is not subject to the BSA and is located in a foreign jurisdiction identified by FinCEN as being of primary money laundering concern, such as Burma, Iran, and North Korea.

Upon taking office in January 2021, the Biden administration has declared a freeze on all agency rule-making, pending a review by a department or agency head appointed or designated by the President. While the Trump administration had already extended the unhosted wallet NPRM for 15 days regarding the \$10,000 threshold and 45 days regarding the remaining rules, FinCEN has since extended and consolidated both deadlines to 60 days. There has yet to be an indication that the “Travel Rule” NPRM will get a similar reopening and extension.

It is likely that these rules—or something close to them—will take effect in the first half of 2021, creating significant new crypto compliance requirements and dramatically increasing the sense of urgency felt by banks and VASPs to file crypto CTRs and SARs.

Globally, FATF released their *12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* in June. In it, FATF decided not to revise previous recommendations related to virtual assets or VASPs but has documented the need for future continued direction. Reassessment of progress towards a Travel Rule solution and further guidance is slated for June 2021, at the next 12-month review.

2020 Major Trends and Developments

Cash—anonymous and liquid—has long served as a tool for criminals. Cryptocurrency, with its similar characteristics, may likewise struggle to ever completely shake its bad reputation, despite illicit transactions making up less than 0.5% of Bitcoin’s yearly volume in 2020. Virtual Asset Service Providers (VASPs) are the front line in preventing financial crime and identifying bad actors. However, inadequate anti-money laundering controls at a VASP can end up facilitating the flow of criminal funds around the world. As VASPs continue to mature and adopt stronger security measures, CipherTrace has found that criminals are beginning to set their sights on greener decentralized finance services over their centralized counterparts.

\$3.5 Billion Sent from Criminal BTC Addresses in 2020

Criminally associated bitcoin addresses sent over \$3.5 billion worth of bitcoin in 2020. This figure includes BTC addresses controlled by dark markets, ransomware actors, hackers, and fraudsters. Most of this bitcoin will ultimately need to be laundered by these criminals, meaning it will make its way to an exchange where it can be converted to fiat currency and transferred to a bank.

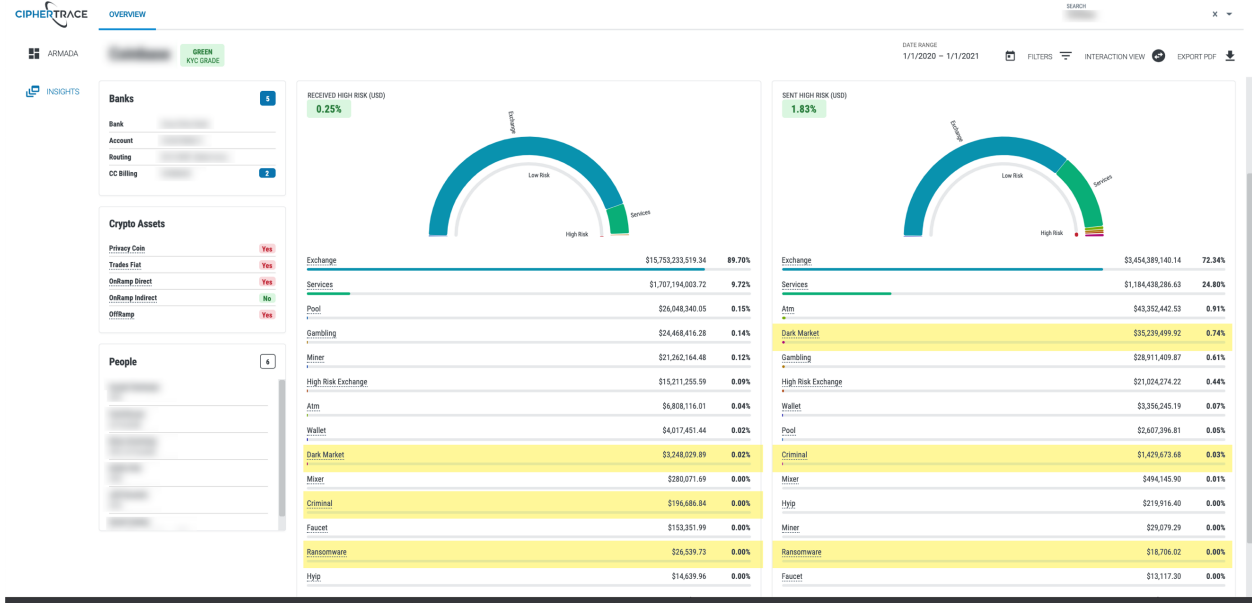
One US Exchange Sent More than \$36.7 Million *Directly* to Criminals in 2020

Using cryptocurrency intelligence tools including CipherTrace Armada, analysts were able to determine that one prominent US exchange received more than \$3.5 million worth of bitcoin *directly* from criminal sources in 2020, despite strong KYC. However, this figure is only a small amount of the criminally sourced funds that actually made it to the exchange; smart criminals will typically create distance between their illicit source of funds and their fiat off-ramp of choice. It is important to note that although the exchange received \$3.5 million worth of BTC directly from criminally associated addresses, exchanges have no way of denying funds before they are received. Even if the exchange sent these funds back, the interaction will still be recorded on the blockchain.

However, this exchange also sent \$36.7 million worth of bitcoin *directly* to criminally associated addresses. These transactions could and should have been stopped by adequate AML software. These outgoing transactions directly to criminal sources highlight the importance of accurate blockchain analytics data. Many criminals don’t typically send directly to and from their criminally linked addresses when transacting with regulated

exchanges, making the \$36.7 million a conservative estimate of funds flowing through the exchange to the pockets of criminals. A vast majority of bad actors will move their funds at least one time. In fact, CipherTrace analysts found that a typical cryptocurrency exchange’s dark market exposure will typically double at two hops out (transactions once removed from the exchange). In the case of this cryptocurrency exchange, dark market exposure more than tripled two hops out, according to CipherTrace data.

US Exchanges Sent \$41.2 Million *Directly* to Criminals



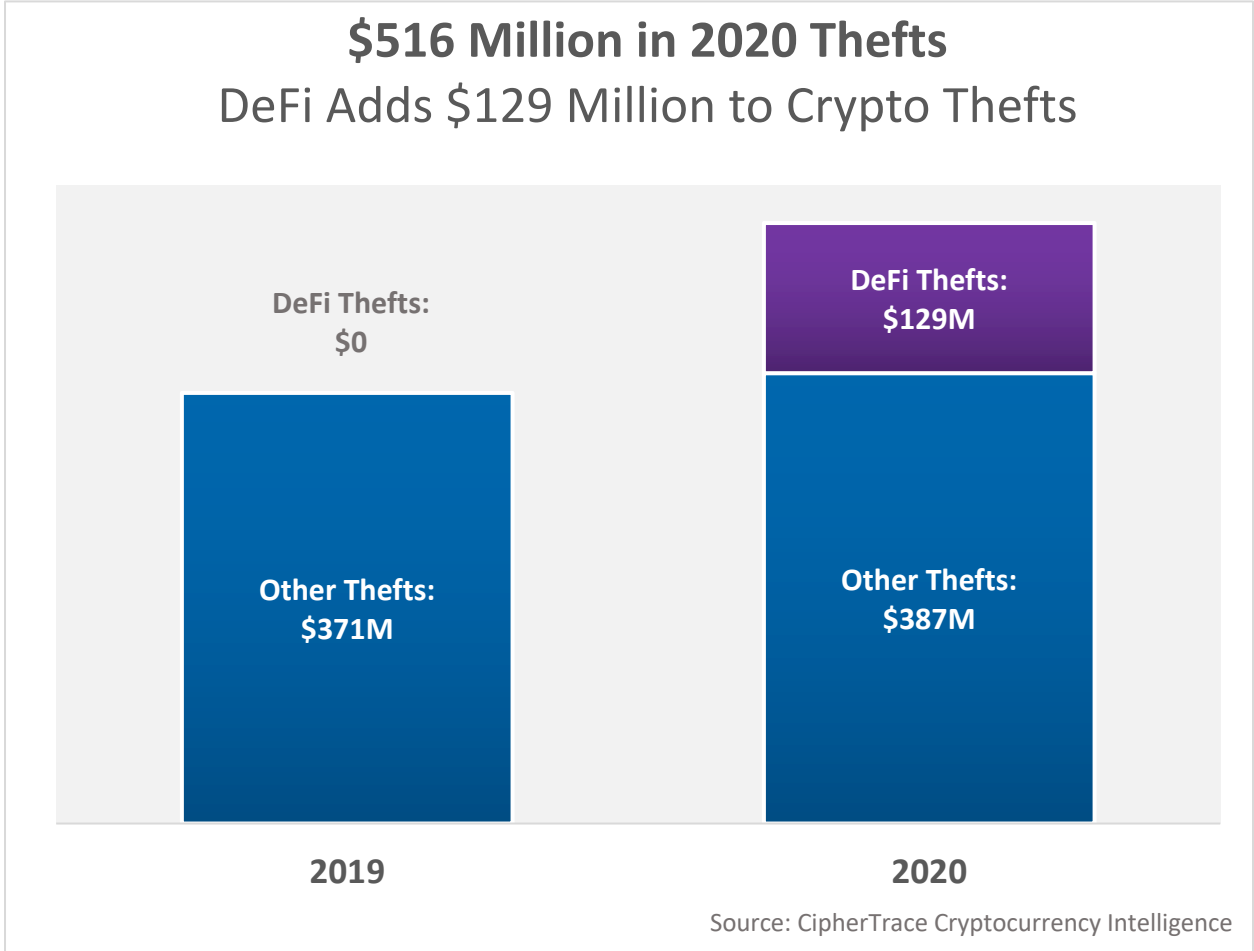
Source: CipherTrace Armada

US exchanges as a whole received \$8.4 million worth of bitcoin *directly* from criminal addresses and sent \$41.2 million worth of bitcoin *directly* to criminally associated addresses.

Over Half of 2020 Crypto Hacks are from DeFi Protocols

The USD value locked in DeFi has grown exponentially in 2020, thereby creating potential new money laundering risks as hacked DeFi protocols make up the majority of crypto thefts in 2020. According to CoinGecko, by the end of December 2020, DeFi had already locked \$19.8 billion—23% of Ethereum’s total market capitalization. This figure equates to more than a 1000% increase from the \$1.7 billion held in DeFi at the start of 2020. This exponential boom eclipses the 70% increase from the start of 2019, when the

DeFi market cap was only \$1.0 billion, to the beginning of 2020. Like the altcoin boom before it, the exponential explosion of capital and lack of regulatory clarity have attracted criminal actors to DeFi, ultimately resulting in the most DeFi hacks in a year to date.



Altogether, over 50% of all 2020 thefts were DeFi hacks, equating to about \$129 million—a little over 25% of the hacked volume for the year. Conversely, in 2019, the DeFi hack volume was virtually negligible. Individual DeFi thefts ranged widely, from a couple hundred thousand to tens of millions of dollars’ worth of crypto tokens. CipherTrace assesses the average DeFi hack in 2020 to be worth roughly \$6 million.

Even 2020’s largest theft, the \$281 million hack of the centralized exchange KuCoin, ultimately involved DeFi as criminals attempted to launder the stolen funds through one of the largest decentralized exchanges in the world—Uniswap. It’s clear that DeFi has become one of the fastest growing trends in the crypto industry. As such, it is important to be vigilant to its money laundering risks. Decentralized exchanges often don’t collect KYC

information on their users and have no way of freezing funds like a centralized exchange; sometimes, this power lies with the individual DeFi projects themselves.

Notable DeFi hacks in 2020 included:

- bZx
- Akropolis
- Axion Network
- Balancer
- Bancor DEX
- Bisq
- Cheese Bank
- COVER
- Eminence.Finance
- Harvest Finance
- Lendf.Me
- Obyn
- OUSD
- Pickle Finance
- Uniswap
- Value DeFi
- WarpFinance
- wLEO

DeFi Rug Pulls Emerge as Top Exit Scam

While DeFi hacks had been on the rise since as early as Q1 2020, the end of the year brought new challenges to DeFi as rug pulls and exit scams began to proliferate, reminding many crypto veterans of the “pump and dump” schemes popular at the height of the ICO boom. In the second half of 2020, nearly 99% of major fraud and misappropriations volume stemmed from DeFi protocols performing rug pulls and exit scams.

Rug pulls are similar to exit scams; both involve insiders taking off with a majority, if not all, of users’ funds. While often used interchangeably, exit scams are more often linked to established entities or projects unexpectedly closing down (“exiting”), taking user funds with them. For example, in November 2020, the DeFi project SharkTron appeared to have conducted an exit scam with \$10 million in user funds, closing its website and leaving users in the dark.

A rug-pull, on the other hand, is a specific type of exit scam that involves “pulling the rug” out from under investors (users) by selling the majority of the DeFi pool, thereby draining liquidity from a specific token. Rug pulls are often accomplished through intentional back doors written into smart contracts. In the case of DeFi project Compound.Finance, a hidden backdoor written into the smart contract allowed developers to pull \$10.8 million from the project’s liquidity pools in November 2020. DeFi project Unicats performed a similar rug pull in October, draining the entirety of its users’ funds.

In our research, CipherTrace found several incidents of DeFi rugpulls and exit scams in 2020. Unfortunately, due to a lack of definitive data, we were not able to verify each incident. Unverified incidents are not included in our overall data pool for analysis.


Notable examples of DeFi rug pulls and exit scams in 2020 included:

- Compound.Finance
- Emerald Mine
- Lv.Finance
- SharkTron
- Unicats
- Yfdex.Finance
- Amplyfi.money (unverified)
- Burn Vault Finance (unverified)
- Minions Farm (unverified)
- Unirocket (unverified)

This trend is likely to continue into 2021 without proper audits of smart contracts, continued education of investors, and relevant regulations on these new risk vectors.

Future of DeFi Hacks, Scams, and Regulation

DeFi protocols are permissionless by design, meaning they often lack regulatory oversight, and anyone in any country can access them with little or no KYC required. As a result, we have seen DeFi become a haven for money launderers in the last months of 2020.



“[DeFi Projects] are likely subject to various laws already, including securities law, potentially banking and lending laws—definitely AML/CTF laws.”

-Valerie Szczepanik, SEC

It appears regulators are beginning to pay closer attention to DeFi and associated compliance requirements. The unaudited smart contracts on which many DeFi projects rely often have vulnerabilities that bad actors can exploit. As Olaf Carlson-Wee, the founder and CEO of Polychain Capital, said on a September 8 episode of Unchained, “I do think it scares me a little bit how much capital is being dumped into contracts that are unaudited. I think that getting security audits is, overall, an important part of maturing any one of these systems.” As DeFi continues to grow, it’s plausible to expect that DeFi projects could fall under the scope of global regulators. FATF already considers decentralized exchanges to be VASPs, and FinCEN applies the same regulatory consideration to DEXs that it does to bitcoin ATMs, regardless of whether they operate for profit.

The US Securities and Exchange Commission staff has noticed DeFi projects that have been subject to vulnerabilities, hacks, attacks, fraud, and manipulation. At the September 18 Parallel Summit, the SEC’s Crypto Czar Valerie Szczepanik said, “When you are

running [Defi] things on code and you are putting it out in the wild, you are missing a step there where you may want to test the code, you may want to audit the code, you may want to have some peer review of the code. To send it out live right away without those protections is risky.”

“Don’t feed into the hype that surrounded the ICO market,” warned Val. “Hype leads to fraud; it can lead to bad implementations of code and insufficient testing. If the industry takes the time to get it right and engages with regulators to help them do so, then all the good stuff will percolate to the top and you will have the benefits that come with the promise of distributed ledger technology.”

Val said “we’ve seen structures that purport to enable users to lend money, earn interest, borrow money, exchange, take positions; these are all financial activities, and they are likely subject to various laws already, including securities law, potentially banking and lending laws—definitely AML/CTF laws.”

The EU, meanwhile, has introduced Markets in Crypto-Assets (MiCA), a proposed regulation which, if passed, will ban decentralized exchanges from trading with any European Union citizens if they are not incorporated as a legal entity and have their registered office in a Member State.

FinCEN’s Proposed Rulemaking Creates New Reporting and Record-Keeping Requirements for Transactions to Unhosted Wallets

On December 18, 2020, the US Department of Treasury issued a notice of proposed rulemaking (NPRM) that will require financial institutions subject to the BSA to verify the identity of their customer, keep records of convertible virtual currency (CVC) transactions greater than \$3,000, and submit CTR-like reports for CVC transactions over \$10,000, if the counterparty in the transaction uses an unhosted (noncustodial) or “otherwise covered” wallet. The NPRM defines “otherwise covered” wallets as those wallets that are held at a financial institution that is **not subject to the BSA** and is **located in a foreign jurisdiction** identified by FinCEN as being of primary money laundering concern, a list that includes Burma, Iran, and North Korea.

These rules were proposed under the Trump administration. In January 2021, the incoming Biden administration declared a freeze on agency rulemaking, which includes these proposed changes. However, the freeze is only temporary, pending review by a department or agency head appointed or designated by President Biden. While the Trump administration had already extended the unhosted wallet NPRM for 15 days regarding the \$10,000 threshold and 45 days regarding the remaining rules, FinCEN has since extended

and consolidated both deadlines to 60 days. There has yet to be an indication that the “Travel Rule” NPRM will get a similar reopening and extension.

Many BSA officers felt that the regulation of unhosted wallets was inevitable, and that the proposed rules are a reasonable response to the current and future money laundering risk posed by the potentially large unmonitored flow of funds to and from unhosted wallets. The proposed rule will be expensive to implement and it is anticipated that these costs will be passed on to users.

If adopted, the new rule will further enforce the requirement for VASPs, as well as banks engaged in crypto transactions, to be able to identify whether a counterparty is another VASP or not, and if so, where that VASP is domiciled. Current regulations already impose this burden on VASPs under the Travel Rule, with additional rules now set for certain transactions to unhosted wallets and otherwise covered jurisdictions, closing AML gaps not covered by Travel Rule regulations. CipherTrace blockchain analytics tools can help your institution determine if a counterparty address belongs to a hosted, unhosted, or “otherwise covered” wallet, which is the crux of the new proposed rule.

The new rule also requires that VASPs aggregate cryptocurrency transactions over a 24-hour period to report transactions over \$10k and identify any signs of structuring. Crypto and cash transactions do not need to be combined when aggregating. CipherTrace is uniquely capable to help VASPs and banks aggregate multi-chain aggregation payments and leverage predictive analytics to identify structuring.

Understanding FinCEN’s Proposed Rule Change for Unhosted CVC Wallets

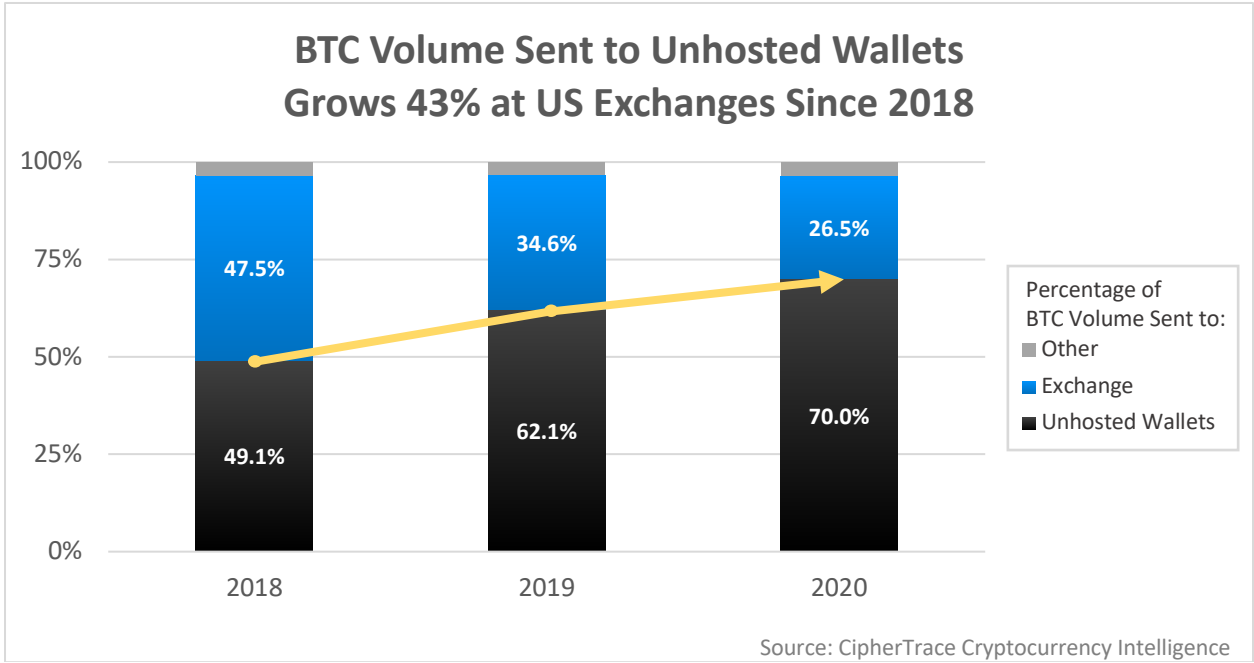
| Banks/VASPs must: | For transactions to/from unhosted or otherwise covered wallets* | | For transactions to/from hosted wallets at either a BSA-regulated financial institution or a foreign financial institution** | |
|---|---|------------------|--|------------------|
| | tx \$3,000+ | \$10,000+/24 hrs | tx \$3,000+ | \$10,000+/24 hrs |
| Verify customer’s identity | ✓ | ✓ | TRAVEL RULE | ✗ |
| Collect, at a minimum, the name and physical address of each counterparty | ✓ | ✓ | TRAVEL RULE | ✗ |
| Retain records on customer’s transaction and counterparty | ✓ | ✓ | TRAVEL RULE | ✗ |
| CTR-like reporting | ✗ | ✓ | ✗ | ✗ |

**“Otherwise Covered” wallets are wallets that are held at a financial institution that is not subject to the BSA and is located in a foreign jurisdiction identified by FinCEN as jurisdictions of primary money laundering concern including Burma, Iran, and North Korea.

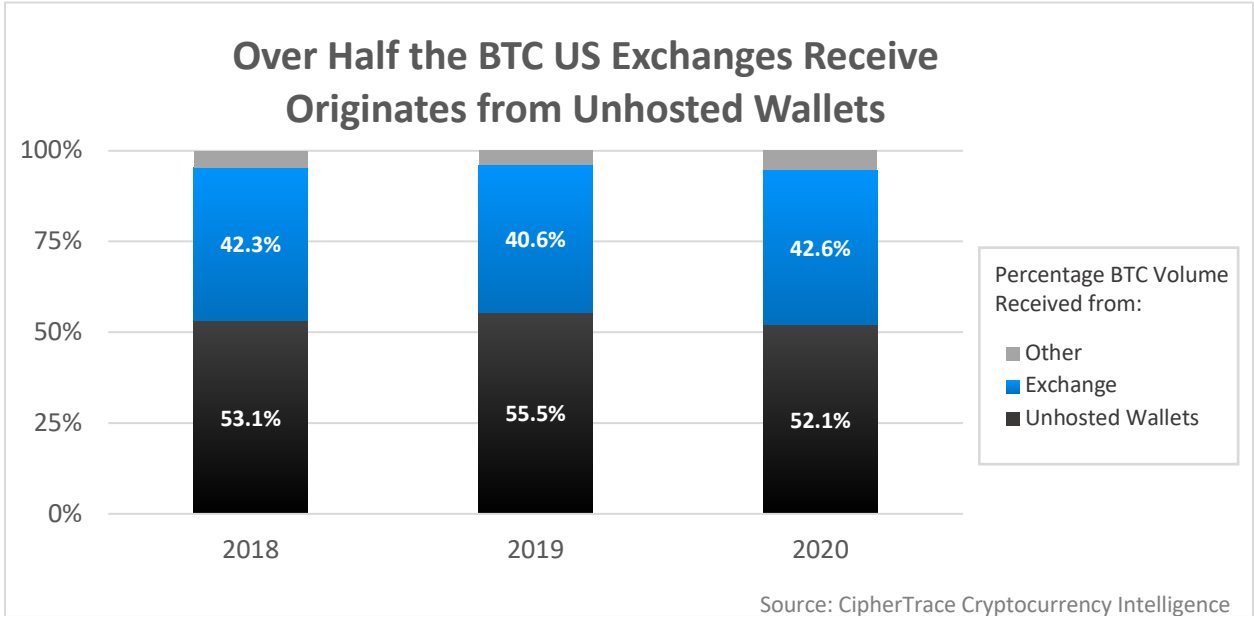
** in a jurisdiction that is not on the Foreign Jurisdictions List

Unhosted Wallets Dominate BTC Volume Going to and from US Exchanges

In 2020, 70% of US Exchanges' outgoing bitcoin volume was sent to unhosted wallets; 52.1% of incoming BTC volume came from unhosted wallets.



By comparison, only about 26.5% of the outgoing BTC volume sent by US exchanges went to other exchanges, and about 42.6% of incoming BTC volume came from other exchanges.



Potential Implications of the Proposed Rule

Blockchain analytics solutions enable crypto exchanges to identify risky transactions involving unhosted wallets. VASPs can follow the funds trail through unhosted wallet addresses, obtaining insights about exposure to high-risk addresses and counterparties. This transparency enables insights about risks associated with unhosted cryptoasset wallets that is impossible to obtain when dealing in fiat currencies or cash.

These proposed requirements are essentially just the application of cash rules (cash and electronic funds transfers) financial institutions have long complied with, now applied to certain virtual asset transactions. However, from an investigatory standpoint, the proposed rule will likely run criminal activity to more hidden corners of the blockchain, which will severely hamper the success of investigations. Instead of using exchanges, criminals will likely move towards unregistered P2P exchanges to keep off the radar. Most investigations are successful when cryptocurrency hits a regulated exchange; by forcing criminal activity out of the exchanges, investigators will lose one of their most powerful tools for tracking, tracing and identifying criminals and their activity.

US “Travel Rule” Rule Making Applies to Virtual Currencies and Lower Threshold Could Double the Compliance Triggers for US VASPs

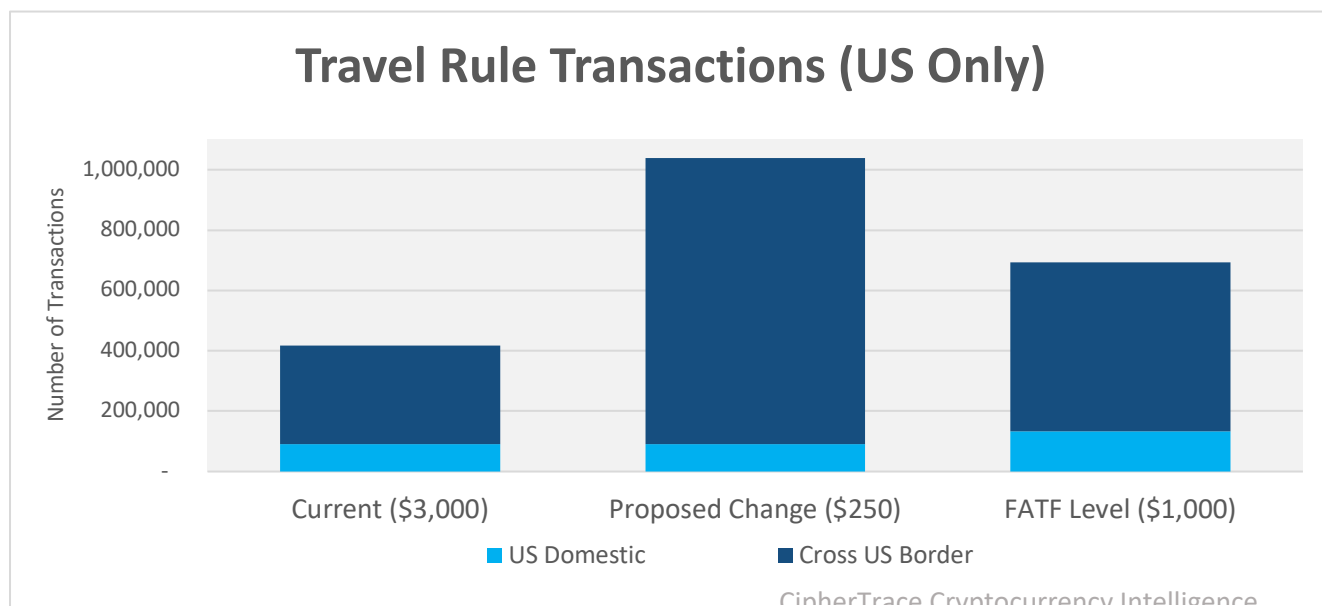
On October 23, the Financial Crimes Enforcement Network (FinCEN) and the Federal Reserve Board proposed a rule change that would require financial institutions, including banks and cryptocurrency exchanges, to collect, store, and transfer information on international payments at a much lower threshold.

Currently, financial institutions must store and forward records for transfers of funds abroad in excess of \$3000. The new rule would see much smaller transfers—anything over \$250—come under the same requirements. Notably, the rule specifically includes cryptocurrency transfers as a class of transactions to which the proposal would apply.

Decreasing the threshold to collect, retain, and transmit information on the transmittals of funds that “begin or end outside the United States” would increase the number of transactions that trigger Travel Rule thresholds every year by a factor of at least 2.5, according to CipherTrace analysis.

| Monthly US Transactions | | | | Number of "Travel Rule" Messages Required by | | Transactions at FATF Threshold (\$1,000) | |
|-------------------------------------|----------------|------------------|------------------|--|-----------------|--|-----------|
| Region | txs over \$250 | txs over \$1,000 | txs over \$3,000 | Current | Proposed Change | US | Other |
| US Domestic | 15,921 | 11,016 | 7,510 | 7,510 | 7,510 | 11,016 | |
| US Cross-Border | 79,011 | 46,780 | 27,295 | 27,295 | 79,011 | 46,780 | |
| International (Non-US) | 392,952 | 260,439 | 178,664 | | | | 260,439 |
| Global | 487,884 | 318,235 | 213,469 | | | | |
| Monthly Travel Rule Messages | | | | 34,805 | 86,521 | 57,796 | 260,439 |
| Annual Travel Rule Messages | | | | 417,660 | 1,038,252 | 693,552 | 3,125,268 |

Source: CipherTrace Cryptocurrency Intelligence



According to CipherTrace data, US VASPs would have had to have sent over 34,000 messages during the month of October 2020 in order to comply with the current US Travel Rule threshold of \$3,000. Over 27,000 of these messages—around 78%—would have been cross-border in nature, meaning the sending or receiving VASP was domiciled outside of the United States. This translates to over 417,000 messages a year at the current threshold.


Lowering the threshold to \$250 would push the number of required travel rule messages to be shared and stored per year to over one million. At this lower threshold, cross-border transactions make up 83% of all travel rule triggers for US VASPs.

If the US were only to lower its threshold to FATF's de minimis standard of \$1,000, then the number of transactions that would trigger compliance would increase by a factor of 1.7 every year. Intermediary banks or financial institutions are also required to transmit this information to other banks or nonbank financial institutions in the payment chain. The proposed rule change acknowledges that cryptocurrency can be transferred without third-party bank involvement but states that, in reality, many users rely on hosted wallets and exchanges to transact.

Difficulty in determining “cross-border payments” in the virtual asset world

FinCEN's proposed rule change is based on transactions that “begin or end outside the United States.” These transactions are defined by whether a financial institution “knows or has reason to know that the transmitter, transmitter's financial institution, recipient, or recipient's financial institution is located in, is ordinarily resident in, or is organized under the laws of a jurisdiction other than the United States or a jurisdiction within the United States.”

Due to the cross-border nature and global reach of virtual assets and VASPs, compliance with this definition would be difficult to enforce, especially given many VASPs are registered in multiple jurisdictions around the world. A financial institution would only have “reason to know” that a transaction begins or ends outside the United States to the extent that such information was shared when receiving the transmittal order or collected from the transmitter—assuming he or she even knows the true extent of the cross-border nature of their transaction.



“Countries should treat all VA transfers as cross-border wire transfers, in accordance with the Interpretative Note to Recommendation 16 (INR. 16), rather than domestic wire transfers, based on the cross-border nature of VA activities and VASP operations.”

-Financial Action Task Force


It is for this reason that the FATF decided in its June 2019 virtual asset guidance that “countries should treat all VA transfers as cross-border wire transfers, in accordance with the Interpretative Note to Recommendation 16 (INR. 16), rather than domestic wire transfers, based on the cross-border nature of VA activities and VASP operations.”

Over One Third of Cross-Border Bitcoin Volume is Sent to Exchanges with Demonstrably Weak KYC

In 2020, cross-border bitcoin transactions constituted 84% of all VASP outflow volume globally. Over one-third—36%—of this cross-border BTC volume went to VASPs with weak or porous KYC procedures.

US Spotlight

A deeper look into the inflows and outflows of VASPs by jurisdiction revealed that 98% of the outgoing BTC volume from US VASPs is from exchanges with strong KYC procedures. When analyzing US VASPs outbound transaction volume for 2020, CipherTrace researchers found that 24% of the BTC volume sent to Virtual Asset Service Providers went to VASPs with demonstrably weak KYC. Of the 24% of outgoing exchange-to-exchange volume, 98% was cross-border. Comparatively, only 44% of the outgoing exchange-to-exchange volume to exchanges with strong KYC was cross-border.

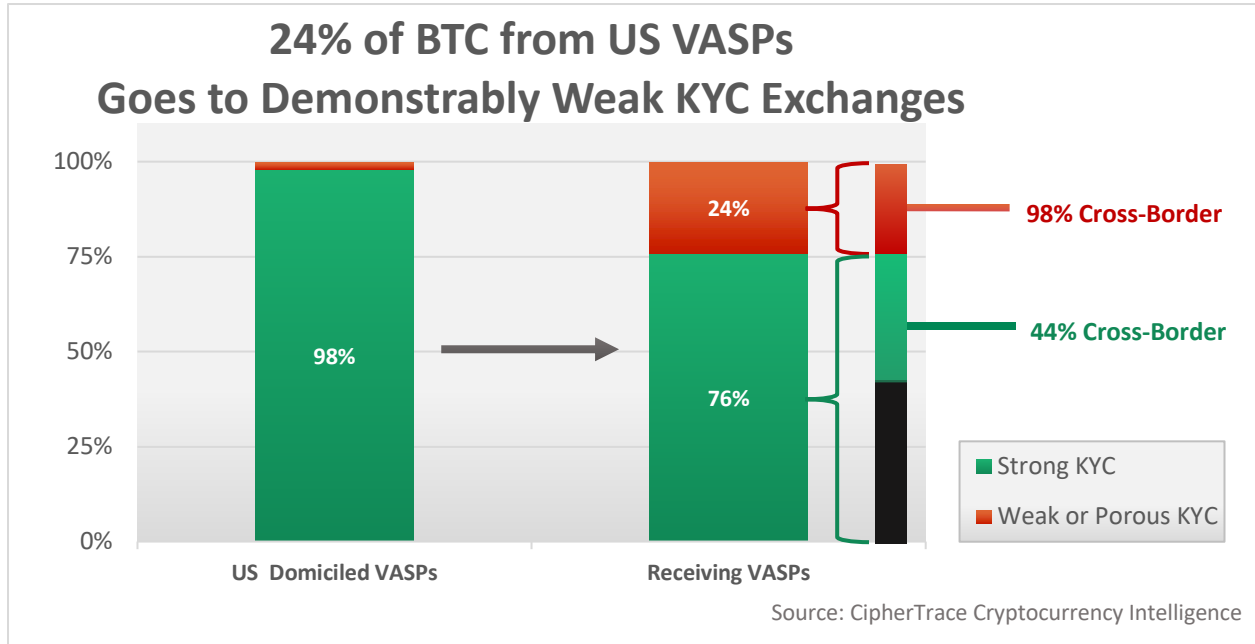


... CipherTrace found that 58% of the exchange-to-exchange BTC volume was cross-border, with 41% of the total cross-border volume being sent to VASPs with weak or porous KYC.

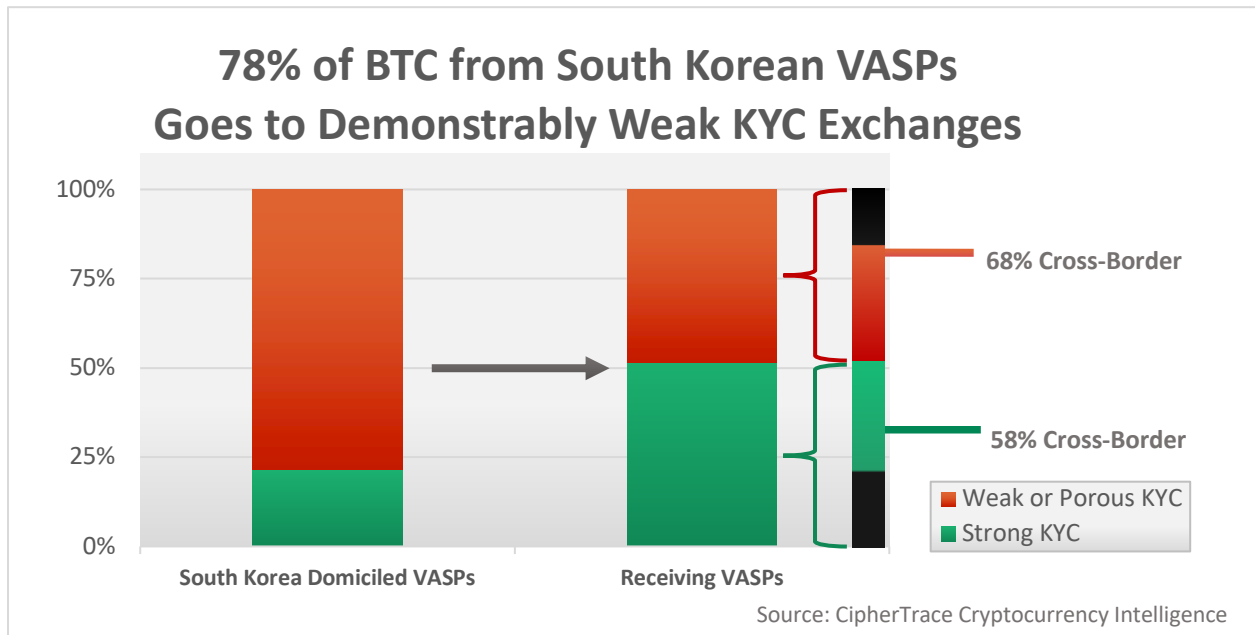
In total, when looking at the outflows of US VASPs, CipherTrace found that 58% of the exchange-to-exchange BTC volume was cross-border, with 41% of the total cross-border volume being sent to VASPs with demonstrably weak KYC.

Inversely, when looking at the inflows of US VASPs, 74% of their inbound exchange-to-exchange BTC volume was cross-border. Of this cross-border volume, 50% originated from crypto exchanges with demonstrably weak KYC practices.

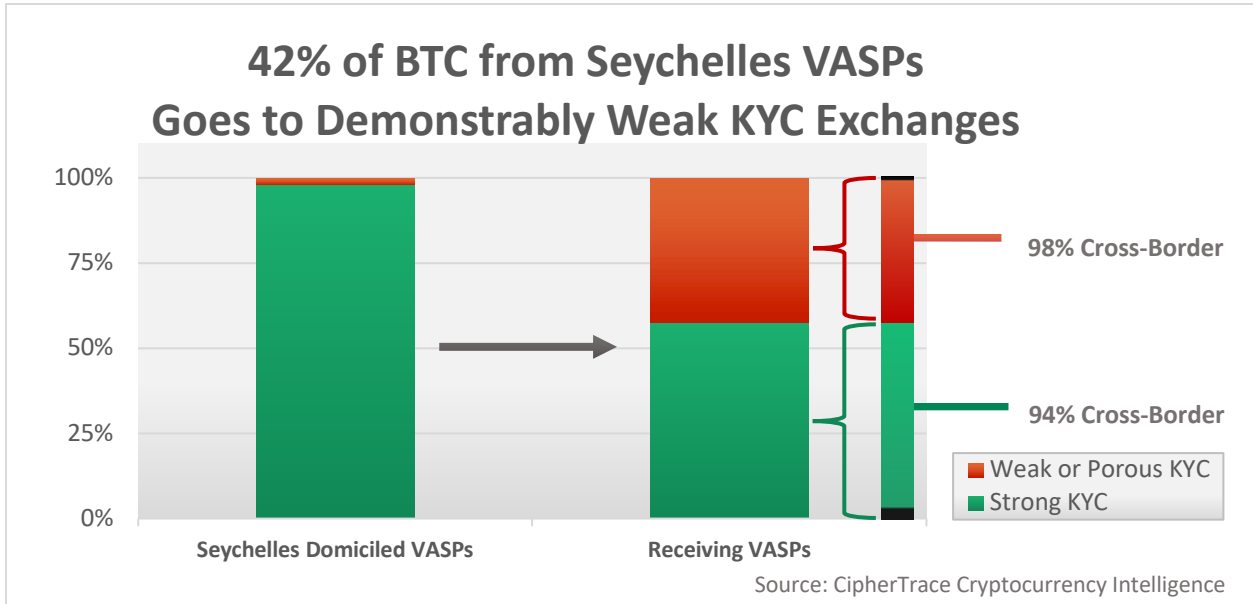
The high percentage of cross-border volume going to and coming from weak or porous VASPs severely complicates the purpose of “Travel Rule” regulations. These KYC-deficient VASPs likely won’t collect or retain the information law enforcement needs to move on any actionable intelligence.



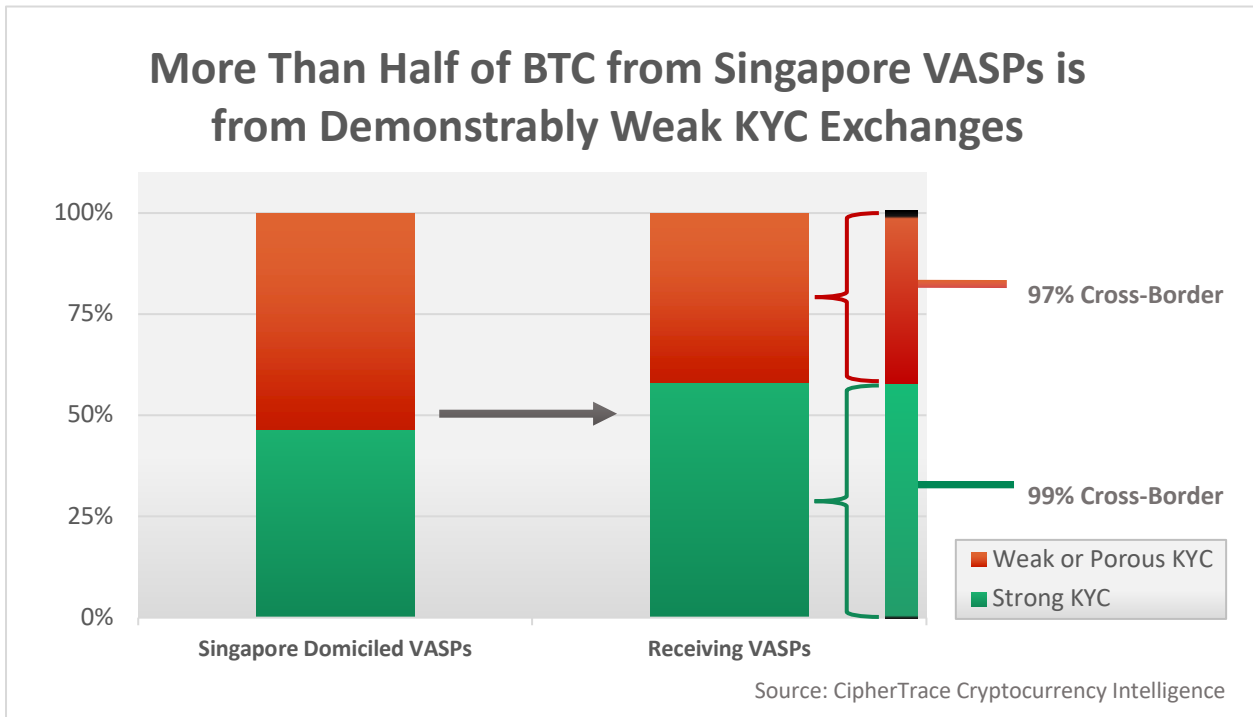
Cross Border BTC Volume Around the Globe



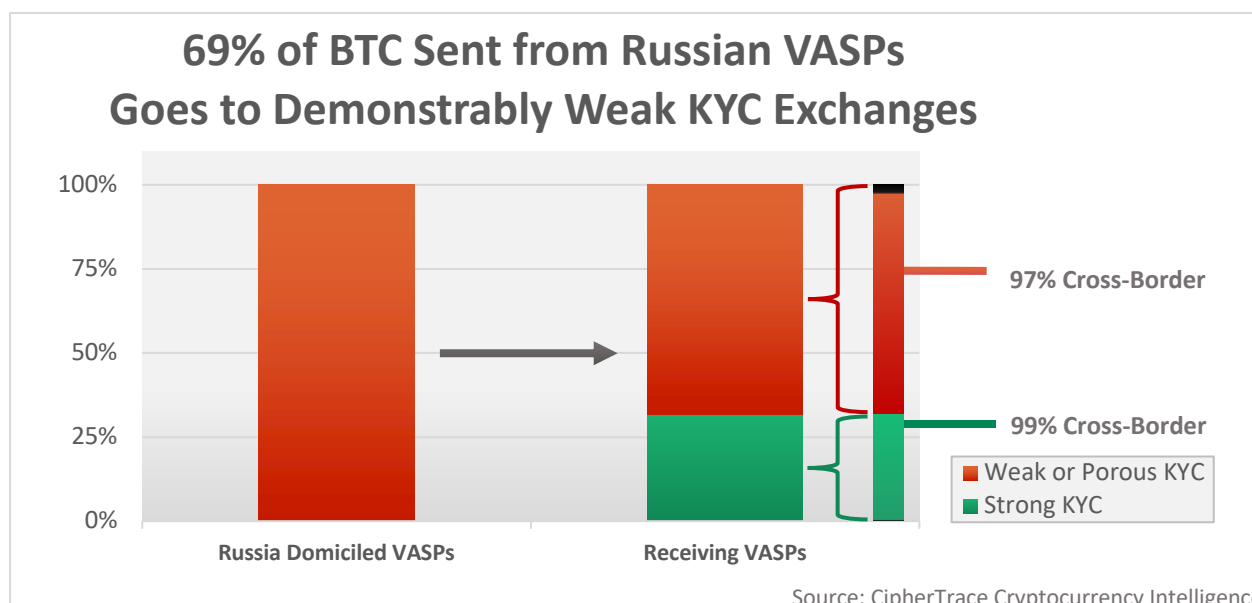
When looking at the outflows of South Korean-domiciled VASPs, CipherTrace found that 63% of the exchange-to-exchange BTC volume was cross-border, with 53% of the total cross-border volume being sent to VASPs with demonstrably weak KYC.



When looking at the outflows of Seychelles-domiciled VASPs, CipherTrace found that 96% of the exchange-to-exchange BTC volume was cross-border, with 51% of the total cross-border volume being sent to VASPs with demonstrably weak KYC.



When looking at the outflows of Singapore-domiciled VASPs, CipherTrace found that 98% of the exchange-to-exchange BTC volume was cross-border, with 49% of the total cross-border volume being sent to VASPs with demonstrably weak KYC.



When looking at the outflows of South Korean VASPs, CipherTrace found that 98% of the exchange-to-exchange BTC volume was cross-border, with 49% of the total cross-border volume being sent to VASPs with demonstrably weak KYC.

Effective KYC protocols are a vital part of any AML program. Understanding KYC processes of counterparty institutions can help financial institutions better understand and manage your risks and prevent money laundering. However, it's one thing to have strong KYC guidelines on paper and another to implement them. By analyzing and probing the KYC processes of more than 800 VASPs in 80+ countries, CipherTrace was able to geographically locate where weak and porous KYC could be exploited by money launderers, criminals, and extremists.

To learn more about average KYC scores by region, check out our *2020 Geographic Risk Report: VASP KYC by Jurisdiction* here: <https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/>

Exchanges Receive Over Half of BTC Payments in 2020

Over half—52.3%—of BTC payment and transfer transaction volume was sent to exchanges in 2020; 40% of payment volume was sent to private wallets.

For this analysis, CipherTrace has identified payment and funds transfers by filtering out blockchain data within the same entity (for example, any transactions from Binance to Binance). This filtering eliminates a large chunk of blockchain data that represents internal transactions within virtual asset entities that skew the overall picture of where crypto funds

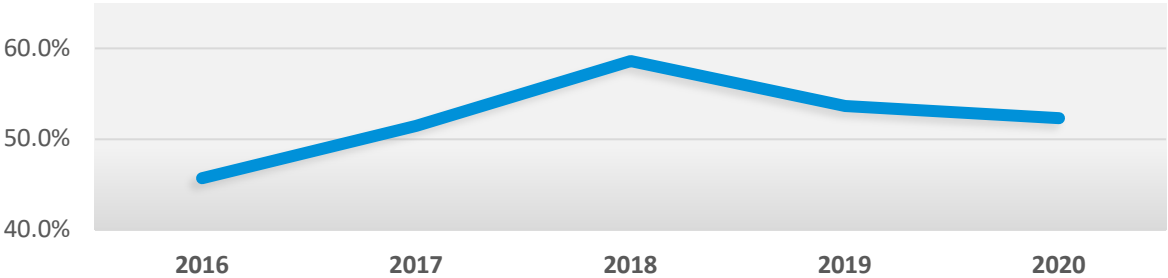
move. By removing this data, analysts can get a better idea of payment flows on the blockchain, rather than analyzing the entire, unfiltered pool of blockchain data.

Likewise, CipherTrace has also filtered out criminals sending funds back to themselves (e.g. peel-chains) and private wallet-to-private wallet transactions as these, too, can artificially inflate the data. In private wallet-to-private wallet transactions, it is impossible to know when individuals are moving funds to different accounts under their control, or engaging in P2P trading.

...while the overall global percentage of BTC volume received by exchanges appears to be dropping, the actual amount of BTC sent to exchanges has increased between 2019 and 2020 by more than 6.3 million BTC, worth roughly \$150 billion.

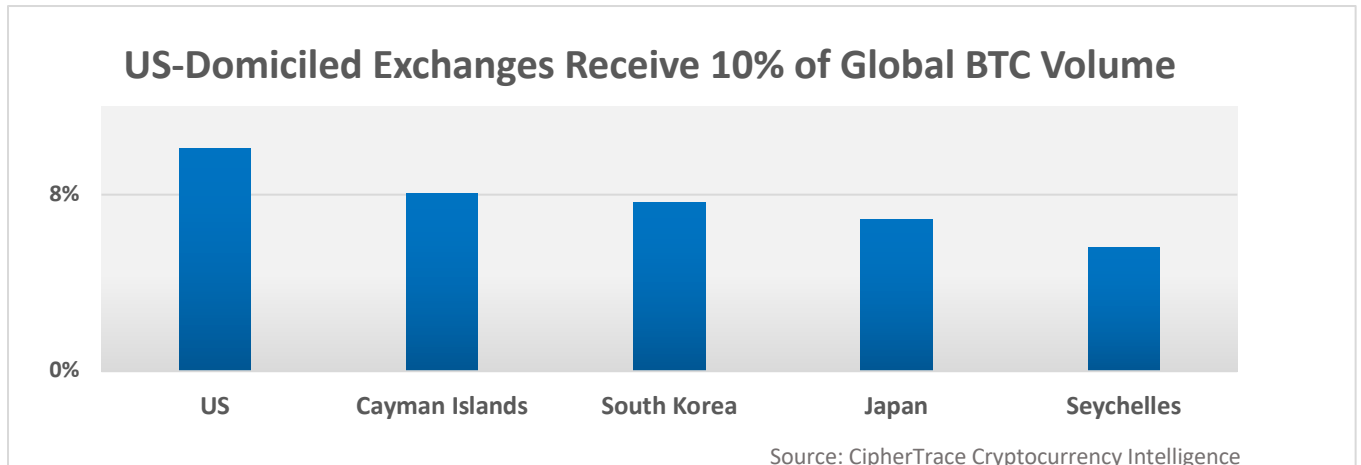
However, while the overall global percentage of BTC volume received by exchanges appears to be dropping, the actual amount of BTC sent to exchanges has increased between 2019 and 2020 by more than 6.3 million BTC, worth roughly \$150 billion. Together, these trends likely mean that, while exchanges continue to grow in popularity, BTC is beginning to see more widespread use outside of exchanges.

More than Half of BTC Volume Was Sent to Exchanges



Source: CipherTrace Cryptocurrency Intelligence

While over half of BTC payments volume went to exchanges in 2020, a majority of that volume was from exchanges in five countries: the US, the Cayman Islands, South Korea, Japan, and the Seychelles. US-based exchanges received the most, at 10% of all BTC volume globally—or 19% of all BTC volume received by exchanges.

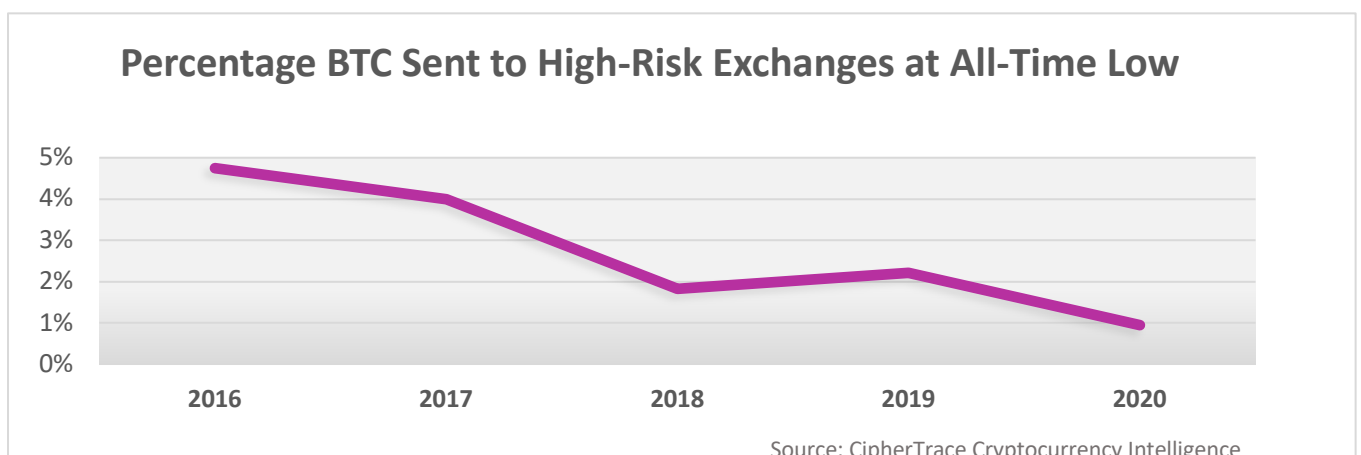


Percentage BTC Volume Sent to High-Risk Exchanges Reaches All-Time Low

2020 saw a 59% drop in the percentage of global BTC volume received by high-risk exchanges. There are several factors that determine when an entity is categorized as a "high-risk exchange." These factors include, but are not limited to, the following:

- they are known bad actors,
- they intentionally try to circumvent AML and KYC measures,
- and/or they are known to regularly fail to cooperate with law enforcement and regulators.

High-risk exchanges are known for being avenues of money laundering. While criminals continue to use high-risk exchanges as fiat off-ramps, CipherTrace investigators continue to see more centralized, mainstream exchanges on the receiving end of criminal funds—albeit often after attempts to obfuscate and distance the funds from their criminal sources through the use of peel chains, mixers, or other obfuscation techniques.




Terrorist Use of Cryptocurrency in 2020

Terrorist organizations and their supporters and sympathizers are continuously looking for new ways to raise and transfer funds without detection or tracking by law enforcement. An asset like cryptocurrency, which allows for the instant, pseudonymized transmission of value around the world with no due diligence or recordkeeping, was bound to catch their eye. Fortunately, the use of blockchain analytics coupled with diligent investigations by law enforcement have resulted in major foiling of terrorist financing networks in 2020.

DOJ Seizures of Cryptocurrency Donations Puts a \$2 Million Hole in Terrorist Finances

On August 13, the US Department of Justice announced the seizure of \$2 million in cryptocurrency from prominent terrorist groups, including al-Qaeda, ISIS, and Hamas. The funds came from cryptocurrency donations the groups solicited online via social media and their own websites.



“It should not surprise anyone that our enemies use modern technology, social media platforms and cryptocurrency to facilitate their evil and violent agendas...”

- Attorney General William Barr

Terrorist groups like these use cryptocurrency to buy weapons, train operatives, and cover international transportation costs. “It should not surprise anyone that our enemies use modern technology, social media platforms and cryptocurrency to facilitate their evil and violent agendas,” said then-Attorney General William Barr.

Authorities conducted their investigation in concert with covert operators. In addition to donations, terrorists garnered funds through fake charity fronts and scams involving the sale of protective supplies related to the coronavirus pandemic, according to IRS’s Don Fort.

Highlighted in the DOJ report was Hamas’s use of bitcoin donations via a Telegram channel run by its military wing, known as the Qassam Brigades. CipherTrace had previously reported on this exact scheme in our Q3 2019 report. While it appears the

operation brought in only the rough equivalent of \$5000 to the terrorist organization, it is important to remember that the cost of carrying out a terrorist attack can be very low.

Jason Blazakis, former director of the Counterterrorism Finance and Designations Office at the US Department of State's Bureau of Counterterrorism, and current director of the Center on Terrorism, Extremism, and Counterterrorism, explained, "[T]errorists don't have to raise a lot of crypto or cash to maintain sanctuary for sleeper cells or, worse yet, the ammunition, guns, and bombs that can maim innocent civilians. While a thousand dollars may not seem like a lot of money, in the hands of the wrong person, it can do all of the above and much more."

French Police Arrest Twenty-Nine in Cryptocurrency Terrorism Financing Scheme

On September 30, 2020, law enforcement arrested 29 French operatives linked to a terrorism financing operation which used cryptocurrency "coupons" in an attempt to obfuscate the source and flow of funds. The French operatives are believed to be affiliated with the Hayat Tahrir Al-Sham organization, an Al-Qaeda affiliate.

The French operatives purchased "hundreds of thousands of euros" worth of cryptocurrency "coupons" from licensed tobacco outlets in France and sent the credentials on the coupons to jihadists in Syria, where the Bitcoin could be redeemed online. France's financial intelligence unit, Tracfin, was able to detect the financial flows from France to Syria after constant surveillance of the group led authorities to several dozen people living in France that "had visited repeatedly, over the past few months, tobacco shops throughout the country to anonymously purchase coupons worth between €10 and €150 [that] were then credited to accounts opened from abroad by jihadists," according to the national anti-terrorism prosecutor's office.

Major 2020 Enforcement Actions

2020 was the year of widespread crypto adoption and price gains, making crypto fraudsters and those in regulatory noncompliance the prime target for enforcement actions. VASPs must adhere to local laws when doing business with their citizens. Aside from deep fines, personal liability and potential jail time loom for those who willfully disregard anti-money laundering laws in many jurisdictions.

BitMEX Executives Charged with Illegal Operations and Anti-Money Laundering Violations

On October 1, the US Department of Justice (DoJ) announced the indictment of four BitMEX executives, charging the group with violating the Bank Secrecy Act (BSA), and conspiring to violate the BSA by "willfully failing to establish, implement, and maintain an adequate anti-money laundering ("AML") program." On the same day, the Commodity Futures Trading Commission (CFTC) filed a civil enforcement action charging five entities and three individuals that own and operate the BitMEX trading platform, including BitMEX CEO Arthur Hayes.

These charges include operating an unregistered trading platform and violating multiple CFTC regulations such as failing to implement AML procedures while generating \$1B USD in transaction fees. The defendants each face up to 10 years in jail and the CFTC's injunction may top \$1.3B USD, making it one of the most expensive AML penalty ever paid by a financial institution.

BitMEX had been under investigation by the CFTC since early 2019 for allowing Americans to trade on their exchange. While the platform claimed to have improved their Customer Identification Program to effectively exclude US persons, the CFTC complaint alleged otherwise. According to the complaint, BitMEX is a maze of corporate entities all owned and controlled by the same people, doing business as the same name. These businesses include: HDR Global Trading Limited, 100x Holdings, ABS Global Trading, Shine Effort, and HDR Services.

According to the CFTC, HDR Global Trading Limited operated the BitMEX trading platform. Despite being incorporated in the Seychelles, "HDR does not have, and never has had, any operations or employees in the Seychelles." Despite being domiciled in the Seychelles, Hayes held his ownership interest in BitMEX entities through a Delaware limited liability company that maintains bank accounts at financial institutions in the US. Despite serving at least 85,000 US customers and managing a large portion of its trading infrastructure from within the US—with half the its employees working from San Francisco or New York offices—BitMEX never registered with the CFTC.

AML Deficiencies and Failure to Report Suspicious Activity

The complaint also claimed that BitMEX not only failed to comply with record keeping obligations, but the company was actively deleted critical customer identification information. In certain cases, these records were deleted “explicitly because a user was found to be located in the US or another restricted jurisdiction.” The DOJ complaint adds that from BitMEX's launch in late 2014 to at least in or about September 2020, the exchange did not file any SARs, failing to report suspected illegal activity on the platform.

Addressing the DOJ indictment, Acting Manhattan US Attorney Audrey Strauss said, “With the opportunities and advantages of operating a financial institution in the United States comes the obligation for those businesses to do their part to help in driving out crime and corruption. As alleged, these defendants flouted that obligation and undertook to operate a purportedly ‘off-shore’ crypto exchange while willfully failing to implement and maintain even basic anti-money laundering policies. In so doing, they allegedly allowed BitMEX to operate as a platform in the shadows of the financial markets. Today’s indictment is another push by this Office and our partners at the FBI to bring platforms for money laundering into the light.”

BitMEX responded to the charges on their website, stating “We strongly disagree with the U.S. government’s heavy-handed decision to bring these charges, and intend to defend the allegations vigorously. From our early days as a start-up, we have always sought to comply with applicable U.S. laws, as those laws were understood at the time and based on available guidance.”

Steps to Improve AML Compliance

In an effort to improve compliance, BitMEX has already taken steps to increase their AML procedures. Since the indictment, BitMEX has hired Malcolm Wright, an associate fellow of the Centre for Financial Crime and Security Studies at the UK's Royal United Services Institute, as the company’s Chief Compliance Officer. Wright will monitor the exchange’s global compliance activities, and directly report to Vivien Khoo, acting interim CEO and COO of BitMEX. It is still unclear as to whether BitMEX had a CCO before Wright.

Upon reevaluating BitMEX’s KYC, CipherTrace has found that the exchange has already improved its practices, moving the exchange from a “porous” (yellow) score since the release of our Geographic Risk Report earlier this month, to a “strong” (green) KYC score. This further corroborates BitMEX’s position on strengthening their compliance procedures, proving the effort to hire a new CCO isn’t in jest.

Ripple, Execs Face SEC Lawsuit

The US Securities and Exchange Commission filed a lawsuit on December 22 against Ripple, Ripple CEO Brad Garlinghouse, and Chris Larsen, a co-founder of the company, alleging that the firm's sale of XRP constituted an offering of unregistered securities.

Ripple responded to the lawsuit in a Wells Submission—a document where the person or business facing an enforcement actions has the opportunity to present facts and legal arguments to convince the SEC that no action should be brought. In their Wells Submission, Ripple claims that “by alleging that Ripple’s distributions of XRP are investment contracts while maintaining that bitcoin and ether are not securities, the Commission is picking virtual currency winners and losers, destroying U.S.-based, consumer-friendly innovation in the process.” However, bitcoin and ether’s decentralized nature have saved them from SEC enforcement. XRP, on the other hand, is much more centralized.

Many exchanges have suspended or delisted XRP pending the results of the SEC lawsuit. This list includes: Binance.US, Coinbase, eToro, and Bittrex. Some investment firms with XRP positions, such as Greyscale and Bitwise Asset Management, have also liquidated their holdings.

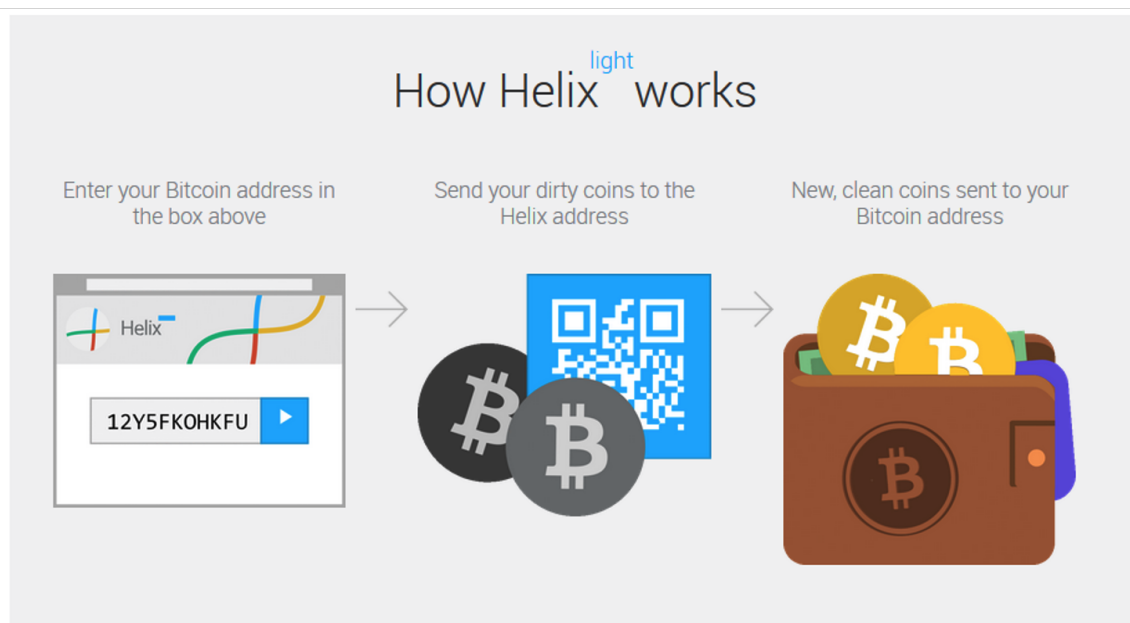
Speaking on an episode of the Pomp Podcast a month prior to the SEC’s decision, Garlinghouse stated he believes that his company would still thrive under a “hypothetical scenario” where XRP is declared a security. Garlinghouse later adds that “more than 90% of RippleNet customers are out of the United States.” However, the lawsuit and subsequent delistings have caused the price of XRP to plummet while most coins remain bullish, affected countless XRP retail holders with no connection to Ripple or the United States.

A virtual pretrial is set for February 22, 2021.

FinCEN Fines Operator of Helix Mixer \$60M for Bitcoin Laundering Scheme Linked to Notorious Dark Markets

In one of the most significant takedowns of a cryptocurrency-anonymizing service, Federal law enforcement authorities arrested Larry Dean Harmon of Akron, Ohio, in February for money laundering. Harmon’s Helix “tumbling” operation moved approximately \$300 million in bitcoin. The Department of Justice alleged that Helix had partnered with now-defunct underground marketplace AlphaBay, which was known for drug dealing and other illegal activities until it was shut down in 2017 by law enforcement.

According to the indictment, Helix made it possible for customers to send bitcoin in a manner that was designed to conceal the transaction and the owner of the bitcoin. Think of a tumbler or “mixer” as being analogous to blender into which you put various types of fruit to make a smoothie. Once the blades spin it is virtually impossible to distinguish the banana from the strawberry. Likewise, once the anonymizing service mixes clean crypto with cryptocurrency that was stolen or used for criminal activities such as selling drugs, it becomes very difficult to trace the bad funds back to the source. “The brazenness with which Helix operated should be the most appalling aspect of this operation to everyday citizens,” said Don Fort, chief of the IRS Criminal Investigation division. “There are bad actors and then there are criminals who facilitate hundreds of other crimes. The sole purpose of Harmon’s operation was to conceal criminal transactions from law enforcement.



- Simple**
1 transaction in,
Many transactions
out
- Speedy**
Cleans coins in 30
minutes
- Easy**
No account needed

Eight months later, on October 19, FinCEN announced a \$60 million civil money penalty against Harmon, for violations of the Bank Secrecy Act (BSA) and its implementing regulations. By accepting and transmitting bitcoin through a variety of means, Harmon operated as an exchanger of convertible virtual currencies. FinCEN found that Harmon

willfully violated the BSA's registration, program, and reporting requirements by failing to register as a MSB, failing to implement and maintain an effective anti-money laundering program, and failing to report suspicious activities.

BitGo Enters Into \$98,830 Settlement with US Treasury Over Multiple Crypto Sanctions Violations

According to a December 30 Enforcement Release by the US Treasury's Office of Foreign Asset Controls, institutional crypto custodian service and wallet operator BitGo failed to prevent persons apparently located in sanctioned jurisdictions from opening accounts and sending digital currencies via its platform.

The release notes that there were 183 apparent violations, adding up to over \$9,000, in transactions sent to the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria. Treasury claims BitGo had reason to know that these users were located in sanctioned jurisdictions based on IP data collected when users log in to the platform, but that BitGo lacked any controls to block users in sanctioned jurisdictions from accessing its services.

Although the statutory maximum civil monetary penalty applicable in these matters is \$53,051,675, OFAC determined that the Apparent Violations constituted a "non-egregious case" and the two parties came to a settlement of \$93,830. The fact that BitGo is a small company, cooperated with OFAC's investigation into the violations, and invested in significant remedial measures in response to the violation were mitigating factors that contributed to the lower settlement amount.

OFAC emphasized in the enforcement action that sanctions compliance obligations apply to all US persons, including those involved in providing digital currency services. This action came two months after OFAC had issued an advisory warning of potential sanctions violations for allowing customers to pay ransomware.

FBI and German Police Charge Operators of movie2k.to and Seize \$30 Million in Crypto

As a result of a joint investigation between the FBI and German authorities, over 25 million euros' worth of cryptocurrency—\$29.6 million worth of Bitcoin (BTC) and Bitcoin Cash (BCH)—was seized from those implicated in the illegal movie streaming site movie2k.to on August 6.

According to the German newspaper Der Spiegel, movie2k.to was one of the largest platforms for the sharing of pirated movies. The site was officially shut down in spring

2013 due to copyright infringement concerns; prior to the shutdown, the site's operators were allegedly able to distribute 880,000 pirated copies of films. One of movie2k.to's operators, who worked as the site's programmer, has been in police custody since November 2019. The programmer has now comprehensively confessed to the charges and is reportedly assisting authorities in their continuing investigations into the second main operator, who remains on the run.

US Attorney's Office Charges Man with Operating Unlicensed ATM Network

On July 22, the US Attorney's office released a statement detailing the guilty plea of a Yorba Linda man, Kais Mohammad, for his involvement in Herocoin—an illegal cryptocurrency business that exchanged up to \$25 million through in-person transactions and a network of Bitcoin ATM kiosks.

According to his plea agreement, Mohammad offered in-person bitcoin-for-cash exchange services, in amounts up to \$25,000. In a typical arrangement, Mohammad generally did not ask about the source of clients' funds and, on many occasions, he knew the funds had originated from criminal activity.

Mohammad also owned a network of Bitcoin ATM-type kiosks located in a network of malls, gas stations, and convenience stores across the greater LA area. These kiosks allowed customers to buy bitcoin with cash, or to sell bitcoin in exchange for cash.

According to his plea agreement, Mohammad knowingly decided not to register Herocoin with the US Treasury Department's Financial Crimes Enforcement Network (FinCEN). He also reportedly refused to develop an effective anti-money laundering program and failed to file currency transaction reports for suspicious exchanges.

While bitcoin ATMs have been known to service criminals and scammers in the past, the global regulatory landscape is tightening for crypto ATM operators. New legislation has been created in countries around the world specifically to regulate businesses that swap crypto for cash, requiring them to obtain KYC information on all transactions over a certain threshold. This KYC information gathering and record keeping is also a critical step in complying with Travel Rule regulations that crypto ATM operators must abide by. These regulations are critical for governments to prosecute and stop those using bitcoin to launder illegal funds.

Fifteen Plead Guilty After Implication in International Crypto-Crime Ring

On June 16th, Vlad-Călin Nistor—the owner of crypto exchange CoinFlux—and 14 of his associates entered guilty pleas for their involvement in an international cryptocurrency scam. According to the U.S. Department of Justice, this crime ring was responsible for fraudulent online auctions used to launder money through Nistor’s cryptocurrency exchange, where they would exchange cryptocurrency for fiat and then deposit the funds into bank accounts under the names of CoinFlux employees and family members.

Regarding the investigation, Assistant Attorney General Brian Benczkowski of the Justice Department’s Criminal Division commented, “Today’s modern cybercriminals rely on increasingly sophisticated techniques to defraud victims, often masquerading as legitimate businesses.” He continued, “These guilty pleas demonstrate that the United States will hold accountable foreign and domestic criminal enterprises and their enablers, including crooked bitcoin exchanges that swindle the American public.”

The real danger, though, may come from other nation-state actors who seek to replicate this behavior by using cryptocurrency exchanges to cover their tracks. Attorney General Benczkowski highlighted this danger in his press release, stating that, “this time [a cryptocurrency exchange] was being used by criminal fraudsters, but there are definitely parallels in what we’ve already seen from nation-state actors.”

DOJ Charges Founder of “AML Bitcoin” with Money Laundering

On June 22, the US Department of Justice charged the CEO of NAC Foundation and founder of AML Bitcoin, Marcus Andrade, with wire fraud and money laundering. The SEC announced parallel criminal actions against Andrade for conducting a fraudulent, unregistered offering of AML Bitcoin and defrauding investors.

The SEC alleged NAC Foundation raised nearly \$5.6 million from more than 2,400 investors by selling tokens that could later be converted to AML Bitcoin. The AML Bitcoin Whitepaper portrayed the token as superior to the original bitcoin because it allegedly had anti-money laundering, anti-terrorism, and theft-resistant technology built into the coin, which would reside on NAC’s own “privately regulated public blockchain.” However, the SEC’s complaints allege that none of these capabilities actually existed.

Kristina Littman, Chief of the SEC Enforcement Division’s Cyber Unit, stated Andrade “repeatedly misled investors into funding non-existent technology, falsely claiming that the technology would make digital asset transactions more secure,” adding, “Investors are entitled to truthful information so they can make fully informed investment decisions.”

SEC Orders Telegram to Return \$1.2 Billion to Investors, Pay \$18.5 Million Penalty to Settle Charges

On June 26, the SEC obtained court approval of settlements with Telegram to resolve charges that its unregistered ICO of "Grams" violated federal securities laws. According to the settlement, without admitting or denying the allegations, the defendants agreed to return more than \$1.2 billion to investors and to pay an \$18.5 million civil penalty.

Kristina Littman, Chief of the SEC Enforcement Division's Cyber Unit, noted that "new and innovative businesses are welcome to participate in our capital markets but they cannot do so in violation of the registration requirements of the federal securities laws." She added, "This settlement requires Telegram to return funds to investors, imposes a significant penalty, and requires Telegram to give notice of future digital offerings."

The SEC first filed its complaint against Telegram in October 2019, after it failed to register its early sale of \$1.7 billion in "Grams" tokens.

Chinese Authorities Arrest Over 100 People for Involvement in the PlusToken Ponzi Scheme

On July 31, Chinese authorities arrested 109 people suspected of involvement in the PlusToken cryptocurrency fraud ring. The South Korean Ponzi scheme was advertised as a high-yield investment for crypto traders, with the company claiming investors would achieve 9% to 18% monthly returns.

Members were encouraged to bring others into the fold in exchange for a commission, creating a Ponzi scheme of massive proportions. Last year, the operators of PlusToken performed a suspected exit from their scam, in which roughly \$3 billion was withdrawn from the accounts of up to four million users who suddenly found themselves unable to access their funds. The Chinese Ministry of Public Security says that they have 27 "major criminal suspects" and a further 82 "key" members of PlusToken in police custody.

As this case keeps unfolding, the real scope of the financial damage continues to come to light. The original estimate of the amount stolen was \$3 billion, but Chinese media outlet Chain News now suggests that \$6 billion was stolen from investors. This news comes after similar events have unfolded in the UK, where authorities recently closed down cryptocurrency scam platform GPay Ltd. The UK High Court ordered GPay to pay for the loss of £1.5 million (\$1.8m) in investor funds.

US Prosecutors Attempt to Return \$6.5 Million in Crypto to Victims of Ponzi Scam

US prosecutors are attempting to return \$6.5 million in cryptocurrency that was taken from the victims of the “Banana.Fund” crowdfunding project—an alleged Ponzi scheme.

The official report did not identify the operator of Banana.Fund by name. However, several victims of the alleged scam have testified that the fund was run by a British national named Richard Matthew John O’Neill aka “Jo Cook.”

Federal prosecutors have accused Banana.Fund’s administrator of admitting to investors his project had flopped, promising to return \$1.7 million, and then failing to do so. Prosecutors allege that the admin then secretly began a laundering and refund scheme that resulted in the US Secret Service’s (USSS) seizure of 482 bitcoin (BTC) and 1,721,868 tether (USDT).

The lawsuit, filed July 29 in the US District Court for the District of Columbia, aims to give the federal government ownership of the assets so they can be returned to the victims.

The way cryptocurrencies are treated in the judicial system can reveal the direction of the law’s treatment of cryptocurrencies moving forward. As governments find ways to return stolen or scammed funds to their rightful owners, the repercussions will be felt far beyond the confines of this particular case.

Centra Tech Inc. Co-Founder Implicated in \$25 Million Scam

On July 13, Sohrab “Sam” Sharma, the co-founder of Centra Tech Inc., officially changed his plea to guilty for his involvement in a scam that stole more than \$25 million from investors through an Initial Coin Offering (ICO) that his company promoted with the help of celebrities, including boxer Floyd Mayweather and musician DJ Khaled.

Robert Farkas and Raymond Trapani, Centra Tech’s other co-founders, have already pleaded guilty to the charges that they lied to investors about having developed “Centra Card”—a purported debit card that allowed customers to use crypto to make Visa- and Mastercard-backed purchases.

The trio is also accused of having falsely claimed that they had a Harvard-educated CEO with more than 20 years of business experience, partnerships with large companies including MasterCard and Visa, and licenses in more than 38 states. Prosecutors allege that they touted these falsehoods to solicit investors to pour more money into the fraudulent Centra Token scam.

\$15 Million in Crypto and Supercars Seized as Chinese Police Bust Arbitrage Scam

On July 9, China's Ministry of Public Security announced they had seized over \$15 million in crypto, and supercars worth an additional \$2 million, from the alleged operators of a novel scam that sold counterfeit tokens. This operation resulted in the arrests of ten individuals suspected of operating the fraudulent scheme.

According to the ministry, this is the first reported criminal case in China where victims were allegedly scammed using blockchain smart contracts to generate fake cryptocurrencies. The case was first reported to the police in April 2020 by a victim, identified as Li, who had joined a Telegram group called "Huobi Global Arbitrage HT Chinese Community."

According to Li, the group advertised a blockchain smart contract that supposedly generated Huobi Tokens (HT) that could yield an arbitrage opportunity with a return of 8%. Li explained how the smart contract worked: "Simply put, you send one unit of ETH to a designated address, you will receive 60 HT. And then you can sell it to gain the difference." However, after Li sent 10 ETH to the ethereum address provided by the Telegram group's administrator, the 600 HT he received in return were fake tokens which could not be deposited for selling.

Police Arrest BitGrail Boss for His Role in Largest Cyber-Financial Attack in Italy

The man who ran Italian-based cryptocurrency exchange BitGrail was arrested for allegedly defrauding more than 230,000 people of €120 million (\$146 million) collectively. In what was deemed "the biggest cyber-financial attack in Italy and one of the biggest in the world," the BitGrail boss faced charges of computer fraud, fraudulent bankruptcy, and money laundering.

In 2018, the same man alerted police of a Nano Coin hack, communicating the loss of "a huge sum." Ivano Gabrielli, who is the head of the National Centre for Cyber Crimes in Italy, said that when their team started investigating, it became clear that the man was actually the head of BitGrail "[and] it...[was]...not yet clear whether he participated actively in the theft or if he simply decided not to increase security measures after discovering it."

The police further allege that the man, a 34-year-old known as "F.F.," interfered to prevent them from halting the continuing theft.

Promoter of Australian Cryptocurrency Lending Scheme Sentenced to 20 Years

John Bigatton, an Australian man who worked as a promoter for cryptocurrency lending scheme BitConnect, was charged by the Australian Securities and Investments Commission (ASIC) and sentenced to a maximum of two ten-year terms in prison. Bigatton was found to be operating an unregistered managed investment scheme that gave unlicensed financial services and lied to customers by providing misleading financial statements. At one point during the height of ICO mania, the BitConnect pyramid scheme was valued at over \$2.5 billion.

Prior to Bigatton's sentencing, the ASIC in September banned Bigatton from providing financial services. In addition to his prison sentence, Bigatton will also have to pay restitution of at least \$80K in Australian currency (US\$58.5K).

Investment schemes like BitConnect were rampant at the height of the 2017 cryptocurrency bull market, which may hold lessons for the nascent DeFi sector. By the end of 2019, the total locked value in DeFi was less than \$1 billion. Total locked value is by the end of 2020 was over \$19.8 billion, inspiring comparisons to the 2017 cryptocurrency bubble. Those looking to "get rich quick" by launching a DeFi protocol without taking proper security audit measures shouldn't forget 2017. As the BitConnect case illustrates, the perpetrators of fraud and negligence are still being charged.

The US Department of Justice Seized \$24 Million from a Brazilian Cryptocurrency Investment Scheme

On November 4, the US Department of Justice (DOJ) announced that "Operation Egypto," the code name used for the joint U.S.-Brazilian effort to recover funds stolen from a cryptocurrency fraud scheme, resulted in the seizure of \$24 million. Brazil reached out to the United States for help in the investigation, as the scheme targeted U.S. residents, among others, by encouraging them to invest in fake investment opportunities that involved depositing either Brazilian currency or cryptocurrency in accounts controlled by the perpetrators.

According to the DOJ press release, Marcos Antonio Fagundes, the mastermind behind the scheme, was charged with "illegal operation of a financial institution, fraudulent management of a financial institution, misappropriation, violation of securities law, and money laundering." Brazilian investigators say that the money that has been recovered will be returned to the victims.

Ilya Kolochenko, the founder of Immuniweb, a Swiss AI Online Protection Program, mentioned that for crimes like these, it is of utmost importance that multiple countries get involved so that the scheme does not have a viral effect, taking off across the web.

IRS Calls Sentencing of Ukrainian National the First Case of Bitcoin Tax Fraud in US

On November 9, the US Department of Justice (DOJ) announced that a 26-year-old Ukrainian national residing in Washington was sentenced to nine years in prison in what the IRS calls the United States' "first Bitcoin case [with] a tax component."

Volodymyr Kvashuk is a former Microsoft employee who allegedly stole more than \$10 million from the company in currency stored value (CSV) such as digital gift cards. According to Cointelegraph, Kvashuk "used the accounts and identities of his fellow employees to steal and then sell the CSV — making it appear as though his co-workers were responsible for the fraud."

Kvashuk attempted to hide the source of the stolen value by using a Bitcoin mixing service and then communicating to the IRS that \$2.8 million in crypto assets flagged as passing through his accounts had been a gift from a relative. He filed a fake tax form to back up the false claim.

OKEx Founder "Star" Xu is Being Held in Police Custody

On October 16, Chinese news sources reported OKEx founder Mingxing "Star" Xu was being held in police custody. Xu's cryptocurrency exchange is headquartered in Hong Kong but is licensed in Malta, creating some ambiguity around where the arrest occurred.

The news followed on the heels of a report that OKEx had suspended cryptocurrency withdrawals due to the absence of one of the exchange's private key holders—presumably Xu —though a report from Mars Finance suggests otherwise. The Mars Finance report suggested that Xu may be being held by police to assist with an investigation into the backdoor listing of OK Group, completely separate from the exchange's halting of withdrawals.

OKEx CEO and co-founder Jay Hao stated that "the issue is over a personal matter and wouldn't affect the business." An OKEx statement sought to assure users of Xu's distance from OKEx, asserting that his involvement was more recently focused on the separate entities of OK Group and OK Coin.

Poor transparency and jurisdiction shopping conspire to increase risk to traders, beyond the volatility of the underlying virtual asset. OKEx appears to be in Malta, a well-regulated jurisdiction, but according to their Terms of Service, non-Maltese and non-Italian clients are serviced through a Seychelles subsidiary, Aux Cayes. Outside of Malta and Italy, Aux Cayes offers riskier financial products, including margin lending, peer-to-peer matching, spot services, and derivative products linked to VFAs or indices.

Global Cryptocurrency Money-Laundering Cartel Busted—20 Arrested

Law enforcement agencies from 16 countries collaborated on a major crackdown in October, making 33 arrests of criminals involved with cryptocurrency money laundering. Twenty of these arrests were suspected members of the QQAAZZ criminal network, which has allegedly laundered tens of millions of dollars for cybercriminals since 2016.

According to Cointelegraph, "[the] funds are allegedly transferred through international bank accounts, shell companies based in Poland and Bulgaria, and via cryptocurrency mixing services." To make the arrests, authorities searched more than 40 homes across Europe and seized bitcoin mining equipment in Bulgaria.

On the same day in a separate case, a New Zealand man was arrested for laundering \$2 million in cryptocurrencies, in part through the purchase of luxury vehicles including a Lamborghini and a Mercedes G63.

On October 15, the US Department of Justice unsealed a superseding indictment, which detailed a case against six individuals for conspiring to "launder millions of dollars of drug proceeds on behalf of foreign cartels." Casinos, front companies, cash smuggling, and bank accounts were all used to launder the funds, with one individual using cryptocurrency to bribe a US Department of State official in an attempt to acquire fraudulent US passports.

Money laundering is as old as currency itself. As criminals increasingly look to cryptocurrency to hide the origins of illicit funds, it will be that much more important for law enforcement and investigative agencies to leverage cryptocurrency tracing services and blockchain analytics. "Following the money" generally leads to the source.

Bitcoin Escrow Company CEO Pleads Guilty to Fraud and Embezzlement

On October 1, Jon Barry Thompson, the head of New York-based bitcoin escrow company Volantis, pled guilty to fraud and embezzlement of over \$7 million in investor funds. In court documents acquired by CoinDesk, Thompson admitted to misrepresenting Volantis's bitcoin custody, control, purchasing practices, and risk exposure to secure investor funds. Thompson could face a maximum 60-year prison term. His sentencing was scheduled for January 7, 2021.

Thompson also settled with the Commodity Futures Trading Commission (CFTC), agreeing to pay \$7.4 million in restitution as well as being barred from all future bitcoin trading and promising full cooperation in any future CFTC investigations.

Crypto Trader Charged with Fraud and Ordered to Repay Over \$6 Million to Investors

Thomas J. Gity, a Florida man running a digital assets day trading company, was charged with fraud and embezzlement of over \$6 million from investors. The SEC complaint, dated September 29, alleged that Gity defrauded investors of \$6.8 million from January 2018 through January 2019 by promoting the false representation that "he was a highly-profitable digital asset trader and had never lost money during a trading day."

Gity used this lie, along with promises of huge returns, to lure in over 18 investors to his operation. He also asserted that he had \$100 million under management. The SEC alleges that Gity used the majority of investor funds to perpetuate his Ponzi-like scheme, while funneling about \$1.8 million to his son.

Coincheck Hack Proceeds Seized in Japan's First Official Seizure of Cryptocurrency

On August 19, the Tokyo District Court issued an order of seizure for a portion of misappropriated funds that were stolen from the Tokyo-based crypto exchange Coincheck.

In 2018, Coincheck was hacked and over \$500 million in NEM (XEM) was stolen by the perpetrators of the attack. At the time, it was one of the biggest crypto hacks yet. However, since then, the value of XEM tokens has dropped by 93%. The original sum is now estimated to be worth around \$39 million.

Reportedly, the court issued an order of seizure from Takayoshi Doi, an Obihiro City doctor. Doi is not suspected of being involved in the 2018 hack; however, he was charged for his purchase of XEM originating from the hack.

This action marked the first time that a Japanese court ordered the seizure of cryptocurrency. The funds in question amount to roughly 4.8 million yen (\$45,000) in both XEM and bitcoin. Doi is expected to keep the funds safe until an official verdict is handed down.

Justice Department Charges Airbit Founders with Cryptocurrency Mining Fraud

On August 18, The U.S. Department of Justice released an indictment charging the operators of AirBit for international fraud, money laundering, and defrauding individuals through a purported cryptocurrency company.

The five founders of AirBit Club—Pablo Rodriguez, Gutemberg Dos Santos, Scott Hughes, Cecilia Millan and Jackie Aguilar—had been running the company since the beginning of 2015. Airbit was advertised as a cryptocurrency mining and trading company according to the Justice Department.

Victims interviewed about the scam testified that they were under the impression that they had profited when viewing their accounts on the Airbit website; however, these profits were nonexistent in reality. Instead, the operators of Airbit were using those funds to pay for their extravagant lifestyles. The Justice Department alleged that the group is also involved in the laundering of at least \$20 million of the proceeds from the scheme.

Malaysian Authorities Arrest Crypto Miners That Stole \$600K+ in Electricity

On September 1, Malaysian state officials put an end to a three-year-long crypto mining operation that had stolen more than \$600,000 worth of electricity.

“We found that illegal wiring was installed so that electricity was supplied directly and not through the TNB meter,” said Nazlin Alim Sadikhi, a regional director with the country’s Energy Commission.

Sadikhi explained that the group's largest crypto mining rigs consisted of over 100 individual mining devices and had been operating nonstop for three years. The perpetrators of this scheme only paid \$7 to \$14 monthly for electricity but consumed over \$20,000 worth of power per month.

OCC Hits New York Based Bank with First-Ever Enforcement Action for Lack of Crypto AML Compliance

On January 30, 2020, the Office of the Comptroller of the Currency (OCC) issued the first cryptocurrency-related enforcement action against New York's M.Y. Safra Bank (MYSB)—the first-ever enforcement action against a US-based bank. The OCC alleged that, for more than two years, MYSB failed to fully vet its cryptocurrency customers and transactions in high-risk jurisdictions.

The order was wholly focused on deficient anti-money laundering (AML) practices for compliance and monitoring of the bank's Digital Asset Customers (DACs). The lack of AML controls cited include opening accounts for DACs without sufficient customer due diligence (CDD) and a lack of adequate monitoring and investigating of suspicious transactions linked to these customers. The entities included cryptocurrency exchanges, bitcoin ATM operators, ICOs, incubators, and virtual OTCs as well as other crypto-related businesses.

Read more details on the CipherTrace blog: <https://ciphertrace.com/occ-hits-new-york-based-bank-with-first-ever-enforcement-action-for-lack-of-crypto-aml-compliance/>

Major Thefts, Scams, and Fraud

Massive exit scams have dominated cryptocurrency crimes in the last two years. 2020 saw WoToken, a similar scheme to 2019's PlusToken HYIP, defraud investors out of \$1.1 billion in its exit scam. As a result of these large rackets, fraud made up 73% of 2020's total crime volume. However, data also indicates that 2020's hacks were smaller than those the year prior—a sign of increasing maturity in the crypto space as entities continue to harden systems and take precautions against inside and outside threats. A summary of major thefts, scams, and fraud can be found below.

Social Media Giant Twitter Compromised by Insiders

On July 15, Twitter accounts for multiple high-profile cryptocurrency exchanges, public figures, and various entities were taken over by hackers promoting a bitcoin doubler scam. The scammers soon after began moving funds into cryptocurrency exchanges and mixing services.

On July 30, Twitter released an update on their investigation, claiming that the hack, in which over 130 verified Twitter accounts were compromised, was the result of a "phone spear-phishing attack" against its employees. Hackers were successful in tweeting a Bitcoin phishing scam from 45 out of the 130 hacked accounts, which included those of Barack Obama, Elon Musk, Bill Gates, and Joe Biden.

Phone spear phishing is a sophisticated form of phishing in which malicious actors target specific businesses or individuals using phone calls. During these calls, the Twitter hackers may have convinced victims to hand over passwords or other information used to access Twitter's internal tools.

"The attack on July 15, 2020, targeted a small number of employees through a phone spear-phishing attack," Twitter said in a tweet, adding, "This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to our internal systems."

Our research showed that the majority of Bitcoin sat in unattributed addresses after the hack—most likely private wallets. We were also able to trace portions of the bitcoin into exchanges and other wallet services, specifically those with privacy-enhanced features.

In the aftermath of the hack, the details of Twitter's lack of security protocols were harshly revealed. According to Decrypt, "over 1,000 Twitter staff and even outside contractors had access to the platform's so-called 'God Mode' administrative panel. It was revealed by Bloomberg in 2017 and 2018 that those contractors with access to the admin tool had

previously misused it to snoop on the likes of Beyonce, tracking the musician's geolocation data and viewing private information.

Read our full analysis of the hack in our blog: <https://ciphertrace.com/twitter-hacked-insiders-compromise-social-media-giant/>

Cryptocurrency Exchange KuCoin's Hot Wallets Hacked for Millions

On September 26, the Singapore-headquartered digital asset exchange KuCoin announced that it had detected large withdrawals of bitcoin (BTC) and ethereum (ETH) tokens to an unknown wallet beginning at 19:05 UTC the day prior, affecting roughly \$150 million in user funds.

In a livestream, KuCoin CEO Johnny Lyu said that the group that infiltrated their system had obtained the private keys to KuCoin's ethereum hot wallets. The hackers then sent the majority of the contents of two hot wallets to an outside ethereum address. In total, the attackers were believed to have made off with 11,480 ETH.

After the hack, KuCoin transferred the remainder of its hot wallets to new secure wallets and froze all customer deposits and withdrawals. Most of the stolen cryptocurrencies were ERC20 tokens, which can be easily laundered through DeFi protocols. This case marks the first high profile instance of a DEX, in this case Uniswap, being used as a money mixer. Unlike centralized exchanges, a DEX can't freeze funds—only specific projects can.

On October 3, Lyu announced that the exchange had identified the suspected hackers and had officially involved law enforcement in their investigation.

DeFi Hackers Use Complex Attack to Steal \$500,000 From Balancer

On June 29, Balancer, a Decentralized Finance (DeFi) liquidity providing platform, was hacked for \$500k in crypto. Following several reports online, Balancer confirmed that an incident occurred that affected two pools containing transfer fees, known as deflationary tokens.

Balancer described how the attackers took a flash loan in Ethereum (ETH) from the non-custodial exchange dYdX, converted those ETH into WETH (Wrapped Ethereum), executed a subsequent trade for STA tokens, and finally drained the STA balance from the pool. According to the platform, once the balance of the pool approached zero, "its price

relative to the other tokens [was] extremely high and the attacker [used] STA to swap for other assets in the pool extremely cheaply.”

CryptoNews pointed out that this attack bears similarity to others that happened earlier this year. Back in February, tokenized margin trading and lending platform bZx suffered two attacks, which were defined not as oracle attacks, but “a clever arbitrage execution.”

This attack is unfortunately just one in a line of many blows to the DeFi industry. In February, hackers also targeted a known vulnerability in the callback mechanism of ERC777, which allowed hackers to hijack a transaction and sell the same batch of tokens multiple times. These instances highlight the need for enhanced security mechanisms and audits to catch attacks early and, ideally, prevent them altogether.

Instagram Influencer “Hushpuppi” Hides \$14 Million of Stolen Funds in Bitcoin

The Federal Bureau of Investigation believes two Nigerian nationals may have hidden a significant amount of the \$17 million they acquired through a phishing scheme in Bitcoin. The scammers were reportedly identified as Raymond Abbas, known to his 2.4 million Instagram followers as “Hushpuppi,” and Olalekan Jakob Ponle, known as “Mr. Woodbery.”

The pair allegedly posed as the accountants of two Chicago-based companies as part of a large-scale phishing scheme. One firm reportedly lost \$15.2 million in this manner while another company’s employees transferred over \$2.3 million to the suspects.

A criminal complaint filed by the US Attorney for the Northern District of Illinois and a special agent-in-charge of the Chicago office of the FBI stated, “The emails were nearly identical to prior legitimate emails sent over the company’s email account, but the fraudulent emails instructed victims to wire funds to a bank account that was set up by money mules at the direction of Ponle.”

Brigadier Jamal Salem Al Jallaf, the director of Dubai’s Criminal Investigation Department, said the local police also confiscated “incriminating documents of a planned fraud on a global scale worth AED 1.6 billion (\$435 million).”

New Zealand Police Seize \$90 Million in Investigation of BTC-e Exchange

On June 22, the Asset Recovery Unit in New Zealand announced the freezing of \$90 million as part of a global investigation into BTC-e—the now-defunct Bitcoin exchange run by Alexander Vinnik. Police Commissioner Andrew Coster said that the “New Zealand Police has worked closely with the Internal Revenue Service of the United States to address this very serious offending.”

Vinnik is accused of facilitating the laundering of proceeds from cybercriminals, ransomware scams, identity theft schemes, actions by corrupt public officials, tax fraud, and drug rings. His notorious exchange, BTC-e, was one of the world’s largest and has traded at least \$4 billion worth of bitcoin with “high levels of anonymity,” the US Department of Justice has said. BTC-e facilitated criminal activity by not requiring users to validate their identity and has been accused of anonymizing transactions and the source of funds.

On the topic of the seized assets, NZ Police Commissioner Andrew Coster stated in a New Zealand Police Media Centre press release, “These funds are likely to reflect the profit gained from the victimization of thousands, if not hundreds of thousands, of people globally as a result of cyber-crime and organized crime.”

Nexus Mutual CEO Hacked for Over \$8 Million in NXM Tokens

On December 14, Hugh Karp, the CEO of DeFi insurer Nexus Mutual, lost the equivalent of \$8 million in NXM tokens in a targeted attack by one of the project's own members. The hacker executed the attack by completing Nexus Mutual KYC process to become a member; later, the attacker switched to a new address and gained remote access to Karp's computer and modify Karp’s MetaMask wallet extension.

Fortunately, no other members have been attacked, and, according to a Nexus Mutual tweet, “The mutual is not impacted; the pool of funds and all systems are safe.” However, after the attack was exposed, the price of Nexus Mutual wrapped tokens dropped 14% on the cryptocurrency exchange Huobi. A portion of the stolen funds were located on 1inch.exchange, a decentralized exchange aggregator.

\$2.5 Million in Crypto Stolen Through SIM Card Hacks by Irish Man

On November 17, twenty-one-year-old Conor Freeman from Dublin, Ireland was given a three-year sentence after being found guilty of stealing over \$2 million in cryptocurrency. Although his attorneys claimed that he acted alone, the prosecution found that Freeman was part of a group of six others who hacked crypto accounts during a three-day heist in 2018.

The group found their victims through social media, where they obtained victims' email addresses and phone numbers to put on SIM cards. Conor Freeman's main job was to go through victims' emails to find their cryptocurrency accounts. The \$2.5 million in stolen funds was looted from three victims.

When Ireland's National Police Force finally caught Freeman, they found that he already spent over \$130K of the stolen funds, but upon arrest he provided the digital wallet and access keys so that police could retrieve the remaining balance.

Argentina's National Immigration Agency Hacked by Ransomware Group

Argentine government officials refused to negotiate with the group responsible for an August 27 ransomware attack on its national immigration agency, Cointelegraph reported.

A group of Netwalker ransomware hackers breached Argentina's immigration agency, Dirección Nacional de Migraciones (DNM). After the hack, DNM received a ransom note stating, "your files are encrypted." The note elaborated that the only way to unlock the files was to buy the decrypter program from the hackers for US\$2 million.

Later that day, a ransomware group posted a small portion of sensitive data to prove the validity of the hack. After the government refused to pay the ransom, the group increased the ransom to US\$4 million.

The Argentine news outlet Infobae reported that the hack shut down all border crossings for more than four hours as authorities took all computer networks used by immigration officials offline. Argentine government officials responded by declaring that "they will not negotiate with hackers and are not concerned with retrieving the stolen data."

Slovakian Crypto Exchange Eterbase Loses \$1.6 Million in Hot Wallet Hack

Eterbase, a small crypto exchange in Slovakia, was hacked by a group that broke into their hot wallets and stole approximately \$1.6 million in various cryptocurrencies on the evening of September 7..

Hackers broke into Eterbase's system and stole just under \$1.6 million of bitcoin, ether, XRP, tezos, algorand, and TRON. The following morning, Eterbase announced from its Telegram channel that hot wallets for six of the cryptocurrencies listed on the exchange had been compromised.

In the announcement, Eterbase shared the wallet address to which the hackers initially routed the funds but withheld further details until its own investigation into the attack could be completed.

Wotoken Ponzi Scheme Defrauds Investors of Over \$1B Worth of Crypto

On May 14, the trial against six core operators responsible for organizing and leading multi-level marketing (MLM) activities for Wotoken began in the People's Court of Binhai County, Yancheng City. According to the public hearing, this Ponzi scheme was active from July 2018 to October 2019 and had 715,249 registered users. In its little over a year of operation, the scheme netted the Wotoken fraudsters more than 7.7 billion yuan (roughly US\$1.09 billion) worth of crypto.

You can find more details in our Spring 2020 Crypto Crime and Anti-Money Laundering Report: <https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/>

2020 Technical Hacks

While 2020 may not have been saturated in as many exchange hacks as previous years, smaller attacks against blockchain protocols and unaudited smart contracts continued to proliferate. Below is a list of notable technical hacks that occurred in 2020.

- On December 28, Cover Protocol was exploited. Hackers deposited LP tokens to its shield mining Blacksmith contract, withdrew almost all tokens to inflate “accRewardsPerToken,” deposited LP tokens again, and then claimed the COVER rewards and tricked the contract to mint a quintillion tokens. The approximately \$3 million in tokens were returned by Grap Finance with a message attached. Read our full analysis: ciphertrace.com/infinite-minting-exploit-nets-attacker-4-4m/
- On December 19, the bitcoin.org site briefly went down due to a DDoS attack. Developers quickly started sharing files regarding Bitcoin Core v0.20.1 over BitTorrent to allow others to seed the file and keep new nodes up to date.
- On December 17, an oracle manipulation vulnerability in Warp Finance was exploited, resulting in the loss of approximately \$7.8 million of USDC and DAI from the WarpVaultSC. The attack took place via a flash swap of \$180 million from Uniswap and dYdX, which then was used to empty Warp.
- On December 21, the Ledger data breach from June 2020 was dumped on RaidForum. The breach included over a million email addresses and more than 250K physical mailing addresses and phone numbers, which are now being used in active phishing campaigns.
- On December 21, EXMO alerted users of suspicious withdrawal activity and the compromise of nearly 5% of total assets on their hot wallets.
- On November 27, there was a 51% attack on BCHA. A miner known as voluntarism.dev implied that they have chained the coinbase rule so all miners would need to send at least 100% of block rewards to the IFP address. The change would invalidate the entire BCHA (ABC) chain back to its origin, November 15, 2020, and then re-grow from there.
- On November 21, Pickle Finance’s pDAI PickleJar was hacked, which resulted in a loss of 19.76 million DAI. The loss was covered by COVER.
- On November 18, NiceHash’s DNS records were taken over by attackers following the latest series of attacks on cryptocurrency projects hosted on GoDaddy.
- On November 17, two vulnerabilities were discovered in the 88mph project, resulting in an exploit that accumulated to a \$100K loss. Luckily, some funds were rescued in the Uniswap pool.

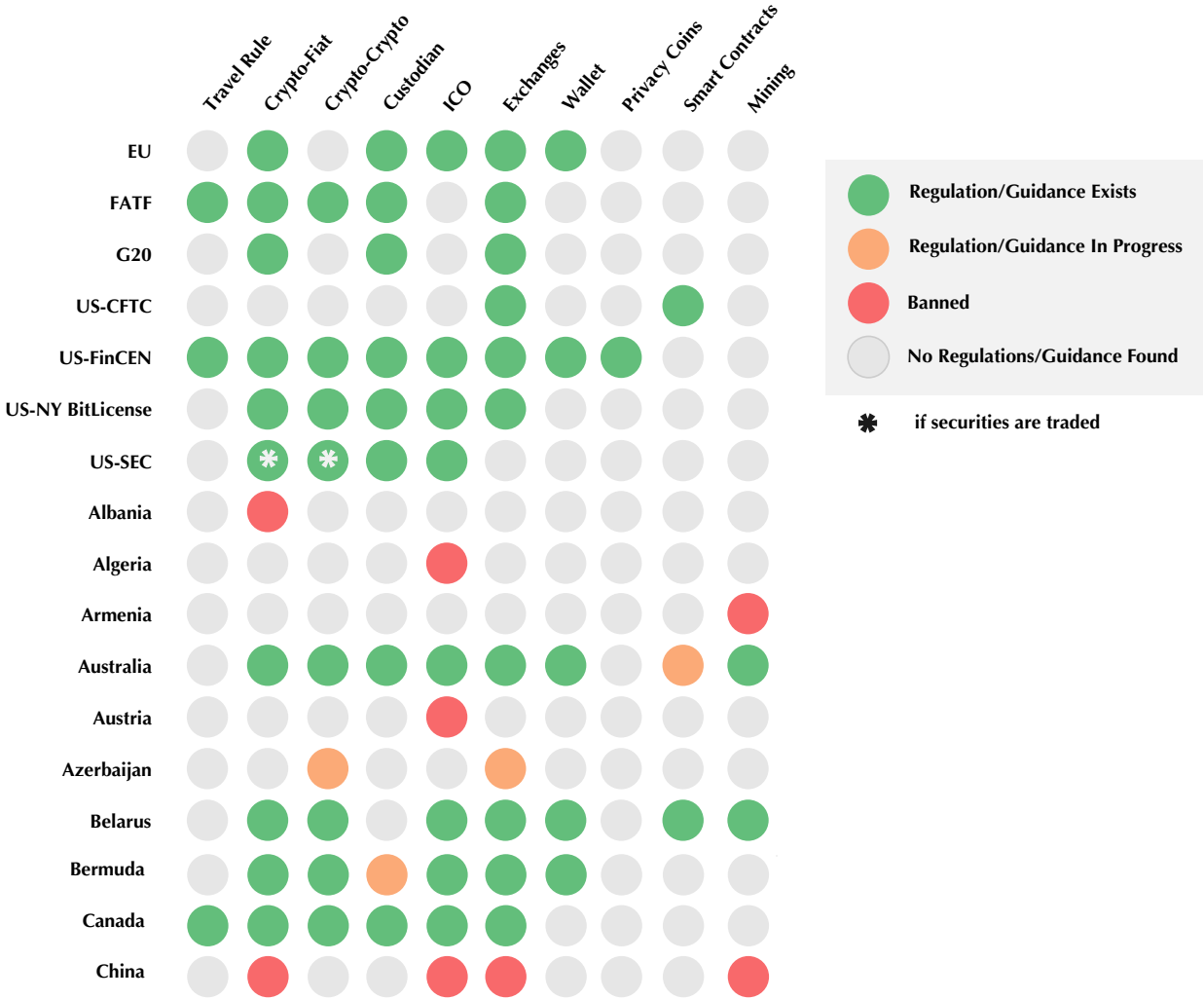
- On November 16, Origin Protocol sustained a re-entrancy attack on their Origin Dollar (OUSD), resulting in a loss of approximately \$7 million. The attack was initiated via a flash loan, followed by a few stablecoin swaps and the re-entrancy attack, which was accompanied with the redeem and further token swaps.
- On November 14, DeFi protocol Value DeFi was exploited for approximately \$6 million due to a flash loan attack via an attacker borrowing 80,000 ETH via lending platform Aave.
- On November 13, DeFi platform Akropolis suffered an approximately \$2 million loss via a re-entrancy attack utilizing a flash loan from derivatives platform dYdX. This attack followed the same steps taken in the 2016 DAO hack, but with the addition of DeFi liquidity pools.
- On November 13, a domain name hosting provider that manages one of Liquid Exchange's core domain names incorrectly transferred control of the account and domain to a malicious actor. This error resulted in the actor having the ability to change DNS records and take control over internal email accounts.
- On November 10, Riccardo Spagni (aka fluffypony), previous lead maintainer of Monero and co-Founder of Tari, shared information on an attacker who bumbled their way through a 51% attack against Monero, trying to correlate transactions to the IP address of the node that broadcast it. This fruitless effort caused no effect on Monero's on-chain mechanisms, and was mitigated by Tor, I2P, and Dandelion++.
- On November 8, GRiN—the Mimbblewimble-based blockchain—suffered a 51% attack. The attack most likely used rentable hashing power from NiceHash. The single attacking miner at the time of the event controlled 58.1% of the network.
- On November 7, a multisig bug in the BSV blockchain was exploited and approximately 600 BSV funds were stolen. This exploit originated from BSV removing the most widely used Bitcoin-based multisig script, Pay-to-Script-Hash (P2SH), and replacing it with a threshold that used the wrong inequality symbols.
- On August 29, ETC underwent another 51% attack which caused a reorganization of over 7,000 blocks, corresponding to roughly two days of mining.
- On July 31, 2gether suffered a cyberattack in which roughly €1.2 million in cryptocurrency was stolen from user accounts.
- On July 10, hackers attempted a 51% attack on the BitcoinGoldnetwork. An attacker mined 1300 blocks on Nicehash in secret starting on July 1st, then secretly supplied miners with updated node software to activate at block 640650, resulting in tons of public legit nodes blocks being dropped. The attack only cost \$297 per hour.
- On July 11, hackers stole 336 BTC, worth approximately \$3.1 million at the time, from Cashaa's over-the-counter (OTC) desk. According to the company, hackers were able to infiltrate the personal computer of an OTC transaction manager based in East Delhi, India, infecting his device with malware.

- On July 2, a Tendermint DoS vulnerability was noted regarding Tendermint v0.33.0, which would allow block proposers to include signatures for the wrong block and allow a malicious validator to halt the entire network.
- On June 30, Vether (VETH) had their entire Uniswap pool drained, about 919,299 (VETH) equivalent to US\$900K, for just 0.9 ETH (\$200).
- On June 29, hackers exploited a Ravencoin vulnerability that allowed extra (RVN) tokens to be minted outside of the 5000 RVN per block that are usually created. Ravencoin believes the vulnerability was introduced intentionally from a specific GitHub account, WindowsCryptoDev.
- On June 28, two Balancer multi-token pools were exploited resulting in a loss of about \$500K. The attacker used a flash loan to exploit a vulnerability in the way Balancer deals with deflationary tokens. Balancer noted that the bug was reported to them via their Bug Bounty program but was dismissed.
- On June 24, Palo Alto Networks released information on two new cryptojacking and DDoS hybrid malware from numerous incidents of CVE-2019-9081 exploitation. The cryptojacking malware, Lucifer, is capable of dropping XMRig for cryptojacking Monero as well as command and control C2 operation and self-propagation through the exploitation of multiple vulnerabilities and credential brute-forcing.
- On June 25, Palo Alto Networks released a report on cryptojacking within Docker containers and using Docker Hub to distribute these images. The malicious Docker Hub account "azurenql," was hosting six malicious images intended to mine Monero.
- On June 1, the Netwalker gang attacked UCSF. UCSF ended up paying the ransom, roughly \$1.14 million.
- On May 14, BlockFi suffered a data breach.
- On February 15, DeFi lending protocol bZx was exploited, netting the attacker a \$350K profit.
- After the bZx exploit, bZx announced they use Kyber as an oracle. Two days later, an attacker manipulated sUSD via Kyber. bZx ETH pool lost about \$1.8 million, while the sUSD pool gained \$1.1 million. The attacker made roughly \$640K.
- On January 23, BitcoinGold was 51% attacked. The attack was detected by two deep re-orgs on BTG which contained double spends.

Changes in Global Regulatory Environment

2020 saw a flood of new crypto regulations, as well as sweeping enforcement actions against VASPs and their executives for lack of regulatory compliance. The chart below shows the widely varying levels of maturity and sophistication in AML/CTF regimes around the globe. The gaps in these regulations present avenues that can be exploited by money launderers and terrorist organizations. Specifically, the money laundering potential of crypto-to-crypto exchanges and privacy coins are not well addressed by lawmakers attempting to regulate digital assets based on the physics of fiat currency.

Current Implementation of AML/CTF Regulations Globally



Source: CipherTrace Cryptocurrency Intelligence



Source: CipherTrace Cryptocurrency Intelligence

FATF—Revised Standards on Virtual Assets 12-Month Review

On June 24, 2020, the Financial Action Task Force met virtually to review global progress towards implementing new anti-money laundering guidance for virtual assets and VASPs. Details of the session released in FATF’s report offer a hopeful outlook for VASPs and the greater cryptocurrency community.

The scope of the review highlights three main assessment areas: emerging market trends and money laundering risks, public sector implementation and enforcement of the revised Standards, and private sector development and adoption of a Travel Rule compliance mechanism.

According to the report, out of the 54 responding FATF and FATF-Style Regional Body (FSRM) member jurisdictions, 32 jurisdictions reported having existing AML/CFT regulations for Virtual Asset Service Providers, 13 jurisdictions reported having regulations in development, and five jurisdictions indicated the prohibition or near future prohibition of VASPs.

CipherTrace's complete written brief on the report can be found here:

<https://ciphertrace.com/revised-fatf-standards-on-virtual-assets-12-month-review/>

FATF—Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing

On September 14, FATF released its report on Virtual Assets Red Flag Indicators. This report is meant to assist reporting entities, such as banks, designated non-financial businesses and professions (DNFBPs), and VASPs.

Despite the focus on VASPs, the paper does recognize the critical role that banks provide during ingress and egress of illicit funds and highlights the use of money mules at both ends.

In order for banks to comply with any of the red flags indicated in the report, it is necessary for them to be able to accurately identify and monitor all crypto-related transactions. Doing so will allow them to identify red flags such as:

- Customers converting a large amount of fiat currency into VAs with no logical business explanation.
- Customers that operate as unregistered/unlicensed VASPs on peer-to-peer (P2P) exchange websites, using bank accounts to facilitate these P2P transactions.
- Customers using one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs sourced from cash deposits into credit cards.
- Customers that are potential crypto money mule or scam victims.

EU—Crypto Businesses Faced with AMLD5 Regulation

As of January 10, 2020, the EU's 5th Anti-Money Laundering Directive, variously referred to as 5AMLD or AMLD 5, went into effect in a bid to make fiat-to-crypto transactions more transparent. Partly prompted by the terror attacks in France, the new regulations are designed to fight terrorist financing and money laundering, while making information more accessible to European financial regulators. The directive also includes tough new regulations for virtual asset service providers (VASPs) such as virtual-to-fiat exchanges and custodian wallet providers. Noncompliant crypto service providers may be subject to fines of up to €200,000.

Many European crypto asset businesses have been unable to meet the new regulatory guidelines. Already, several companies have ceased operations, citing the extensive know-your-customer (KYC) and AML requirements as AMLD 5 became a reality. However, all the technology needed to quickly and cost-effectively bring VASPs into compliance is readily available.

Not all European VASPs are making the investment in updating their compliance regimes to meet the new AMLD5 requirements. Dutch crypto derivative platform Deribit, for example, announced plans to move to Panama in early February 2020 to avoid these regulations. Despite some arguments that the costs of compliance will not be significantly higher, Deribit claimed that the new regulations would create too many barriers for the majority of traders.

US—FinCEN Releases New Proposed Rule Aimed at Closing AML Gaps from Unhosted Wallets

On December 18, the Financial Crimes Enforcement Network (FinCEN) released a proposed rule change for virtual currency transactions with unhosted wallets. Under the proposed change, banks and money services businesses (MSBs) would be required to verify the identity of their customers and submit reports for CVC transactions over \$10,000, and to keep records of CVC transactions greater than \$3,000 when a counterparty uses an unhosted or otherwise covered wallet. "Otherwise covered" wallets as those wallets that are held at a financial institution that are not subject to the BSA and are located in a foreign jurisdiction identified by FinCEN as jurisdictions of primary money laundering concern, such as Burma, Iran, and North Korea.

However, the Biden administration, which took control of the executive branch of the U.S. government in January 2021, declared a freeze on agency rule-making, which could include the recent proposed changes to lowering travel rule thresholds and new recording and reporting requirements for cryptocurrency transactions to unhosted wallets. The freeze

is only temporary, pending review by a department or agency head appointed or designated by President Biden.

Notably, there is an exception to this freeze for "financial, or national security matters," as permitted by the Director of the Office of Management and Budget (OMB). It is still unclear if these proposed crypto rules would be included under this exception. All other rules changes that have already been published in the Federal Register but have not yet taken effect—including notices of proposed rulemaking (NPRMs)—should be postponed for 60 days and opened to a new 30-day comment period for further evaluation.

US—FinCEN, OFAC Warn VASPs of Potential Sanctions Violations for Allowing Customers to Pay Ransomware

On October 1, the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence issued a pair of advisories to assist U.S. individuals and businesses in efforts to combat ransomware scams and attacks.

Treasury's Financial Crimes Enforcement Network (FinCEN) issued an advisory to provide information on the role of financial intermediaries in payments, ransomware trends and typologies, and related financial red flags. FinCEN's advisor highlights that detecting and reporting ransomware payments are a vital part of ransomware prevention.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory to alert companies that engage with victims of ransomware attacks of the potential sanctions risks for facilitating ransomware payments. Sanctions compliance programs of VASPs should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction.

US—National Defense Authorization Act for Fiscal Year 2021 (H.R.6395)

On December 11, the United States Congress presented the National Defense Authorization Act (NDAA) for Fiscal Year 2021 to then-President Donald Trump for final authorization. President Trump vetoed the bill on December 23, but the Senate overrode Trump's veto by a wide bipartisan margin on January 1, 2021.

Most notable to the crypto community, this year's NDAA contains language that broadens the legal definition of "value that substitutes for currency" to include emerging payment methods such as virtual currencies.

The NDAA also clarifies the definition of money transmitting businesses and services by replacing the generalized term “funds” with “currency, funds, or value that substitutes for currency.”

In an effort to strengthen Treasury's financial intelligence, anti-money laundering, and countering the financing of terrorism programs, the bill also establishes national exam and supervision priorities, increases technical assistance for international cooperation, and seeks to tackle financial crime issues related to beneficial ownership and a lack of corporate transparency.

US—OCC Issues Statement Allowing Banks to Hold Crypto Assets for Customers

On July 22, the Office of the Comptroller of the Currency (OCC) issued a statement that gave a green light to bank to hold crypto assets for their customers. The new guidance affirmed that bank custody services, which include holding digital assets, can extend to cryptographic keys and other crypto-related assets.

Jonathan Gould, senior deputy comptroller and chief counsel, wrote, "We conclude a national bank may provide these cryptocurrency custody services on behalf of customers, including by holding the unique cryptographic keys associated with cryptocurrency." He also reaffirmed the OCC's position that “national banks may provide permissible banking services to any lawful business they choose, including cryptocurrency businesses, so long as they effectively manage the risks and comply with applicable law.”

As advancements are made in the financial technology sector, banks must adapt to the changing landscape to provide the necessary services that their customers require. According to the OCC, “as the financial markets become increasingly technological, there will likely be an increasing need for banks and other service providers to leverage new technology and innovative ways to provide traditional services on behalf of customers. By providing such services, banks can continue to fulfill the financial intermediation function they have historically played in providing payment, loan, and deposit services.”

US—4th Amendment Does Not Protect Bitcoin Data, Says US Appeals Court

On June 30, a three-judge panel from the Fifth Circuit courts ruled that the American government's Fourth Amendment does not apply to bitcoin transaction data used in a crime if the data stems from virtual currency exchanges. The US court ruled against a

defendant, Richard Gratkowski, who attempted to leverage the Fourth Amendment's prohibition of unreasonable searches and seizures of private property in an appeal.

Gratkowski was charged with allegedly making payments to a child pornography website, sending bitcoin to the web portal via his Coinbase account. In the process of the investigation, the Federal Bureau of Investigation (FBI) subpoenaed Coinbase for Gratkowski's transaction records. However, Gratkowski appealed the case and said that his bitcoin transaction history deserves Fourth Amendment protection.

Judge Haynes, who voted to strike down the appeal, explained: "Coinbase is a financial institution, a virtual currency exchange, that provides Bitcoin users with a method for transferring bitcoin. The main difference between Coinbase and traditional banks, which were at issue in Miller, is that Coinbase deals with virtual currency while traditional banks deal with physical currency."

US—DOJ Publishes Cryptocurrency Enforcement Framework

On October 8, the US Department of Justice published the Cryptocurrency Enforcement Framework. The Framework is broken down into three parts: an overview of cryptocurrency-related threats, laws and regulations to combat these threats, and ongoing challenges and future strategies for cryptocurrency enforcement.

The framework distinguishes three main categories in the illicit use of cryptocurrencies: 1) using cryptocurrency directly to commit crimes or to support terrorism; 2) using cryptocurrency to hide financial activity, such as evading taxes or operating an unregistered MSB; or 3) committing crimes within the cryptocurrency marketplace itself. In discussing the DOJ's ongoing challenges in combating these threats, the framework promises that the Department of Justice will continue its aggressive investigation and prosecution of those who use cryptocurrencies to commit, facilitate, or conceal their crimes, highlighting the fact that the DOJ "has prosecuted a number of individuals operating as P2P exchangers for money laundering and for violating the BSA."

UK—FCA Becomes AML and CTF Supervisor for UK Cryptoasset Activities

On January 10, 2020, the United Kingdom's Financial Conduct Authority (FCA) became the anti-money laundering and counter terrorist financing (AML/CTF) supervisor for businesses carrying out cryptoasset activities under the amended Money Laundering, Terrorist Financing and Transfer of Funds Regulations. This amendment was a result of the implementation of AMLD5 into the UK's national legislation. Under the new regulations,

cryptoasset businesses operating in the UK are now required to register with the FCA before providing services within the country, on top of integrating traditional AML requirements such as undertaking customer due diligence, enhanced due diligence, reporting, and monitoring.

UK—FCA Issues Notice to UK Cryptoasset Businesses

According to the Financial Conduct Authority's (FCA) crypto money laundering regulations, existing businesses had until June 30, 2020, to register with the FCA and apply for priority review of their business. Companies that failed to apply by that date were warned of the potential to encounter registration processing delays. Any companies not registered with the FCA were required to cease trading on January 10, 2021.

Any new UK cryptoasset businesses that began operations after January 10, 2020, must now register with the FCA before conducting business.

UK—New National Risk Assessment of Money Laundering and Terrorist Financing

On December 17, the Treasury and the Home Office jointly published the UK's third national risk assessment of money laundering and terrorist financing (NRA). This assessment updated the findings of the previous NRA, published in 2017. Most notably, the 2020 NRA increased the money laundering and terrorist financing risk of cryptoassets from "low" to "medium." The assessment noted that the cryptoasset ecosystem has matured, developed, and expanded considerably in the last three years; however, by their analysis this maturation has also provided additional opportunities for abuse resulting in "an increased money laundering risk, with criminals increasingly using and incorporating them into their money laundering methodologies." The NRA also noted that the inclusion of VASPs into the Money Laundering Regulations (MLRs) since January 2020 would help to mitigate vulnerabilities over time.

France—Mandatory KYC Rules for All Cryptocurrency Transactions on the Horizon

On December 8, France announced its plan to implement strict KYC rules for all cryptocurrency transactions and impose harsher requirements on crypto-to-crypto exchanges. Terrorist attacks funded by cryptocurrencies were cited as the main motivating

force behind these changes, following the September arrest of 29 people suspected with involvement in cryptocurrency financing of terrorism. The event prompted France's Finance Minister, Bruno Le Maire, to declare that proposals would be made "to strengthen the control of financial funds."

The details of the decree explain that any cryptocurrency transaction worth more than €0 will go through a KYC process and require two forms of government identification. Also, all crypto-to-crypto exchanges will need to register to obtain a license in order to operate. As of now, the limit for KYC checks is capped at €1,000 and only for crypto-to-fiat. Exchanges that fail to register by the deadline could face fines or imprisonment.

These strict regulations will increase the user onboarding costs for French exchanges from approximately €1 per user to about €5. Pierre-Guy Bareges, CTO of Digital Service Group, noted that the KYC rule change "is a 'concern for all actors in France' because customers could go to foreign exchanges where constraints are much less restrictive."

These measures are currently in the ordinance stage and are expected to become a decree early 2021. Decrees do not need parliamentary approval in France before becoming a law. Once a law, all crypto firms will have six months to comply.

South Korea—New Tax Targets Crypto Traders

On July 22, the South Korean government unveiled its new crypto tax proposal. According to the proposal, traders earning over \$2,100 a year are set to pay a 20% tax on their earnings—a considerably lower threshold than what is imposed on stock market traders, who are not taxed on earnings up to \$42,000 from investments in KOSDAQ-listed companies.

Tax authorities also issued a warning to those who may attempt to bypass tax measures by trading on overseas-based exchanges. Undeclared traders will face an additional 20% tax bill on undisclosed trades.

South Korea—Plans to Ban Privacy Coins

On November 3, South Korea announced it will ban privacy coins countrywide in 2021 while enforcing stricter KYC requirements on crypto users. The new regulations, filed as updates to the country's Special Payment Act, will outlaw so-called "dark coins" that are considered hard to trace. Exchanges have six months to show compliance with the KYC elements of the law.

The Singapore branch of OKEx and the Singaporean exchange Upbit delisted privacy coins based on their interpretation of FATF guidelines in September 2019. In November 2020, Colorado-based ShapeShift also delisted privacy coins Zcash, Dash, and Monero.

Kyrgyzstan—National Bank Developing New Cryptocurrency Laws

On November 13, the National Bank of the Kyrgyz Republic announced that is developing a draft law that would give them the jurisdiction to regulate crypto sales and purchases in order to better track fraud and protect consumer rights.

Pakistan—Creation of Crypto Framework in the Works

On November 6, Pakistan’s Security and Exchanges Commission (SECP) announced it is working on creating a framework for cryptocurrency regulation in the country. Pakistan sees the adoption of digital currency as a chance to present a “robust regulatory regime at par with the World for regulating Digital Assets.” The country hopes to have its own central bank.

Central Bank Digital Currencies

As central bank digital currencies (CBDCs) transition from pilot stages to retail use, prioritizing compliance with AML and CFT regulations will be of paramount importance. Just as fiat currencies are frequently transferred across borders, we should expect the same will be true for CBDCs, and so Travel Rule regulations should also be taken into account.

The jury is still out on the ultimate impact CBDCs will have on the global economy. The development of CBDCs by different countries at varying rates poses questions about global adoption and interoperability. While the countries listed below have made strides in CBDC development in 2020, many countries still lack the legal structures to allow for CBDCs.

BIS—Central Banks Reject Popular Narrative Regarding CBDC Issuance Motives

On June 24, the Bank for International Settlements (BIS) released a statement in which they rejected the supposition that private-sector stablecoin proposals—such as Libra—have spurred the issuance of central bank digital currencies (CBDCs).

BIS explained the newfound interest in CBDCs as a realization that digital currencies present a vessel through which they can shape the future of payments. The report states, “CBDC issuance is not so much a reaction to cryptocurrencies and private sector ‘stablecoin’ proposals, but rather a focused technological effort by central banks to pursue several public policy objectives at once.”

The report provides an alternative explanation to the sudden increase in CBDC tests, hirings, and studies that have occurred in the past year. Regardless of the reasons behind the boom in CBDC interest, the BIS made it clear that digital currencies are likely transformative, and that “CBDCs have the potential to be the next step in the evolution of money.”

US—National Banks Can Use Stablecoins to Facilitate Payments, OCC Says

On January 4, the US Office of the Comptroller of the Currency (OCC) issued an interpretive letter permitting national banks and Federal savings associations to use stablecoins and independent node verification to engage in and facilitate payment activities as settlement infrastructure within the US financial system.

According to the letter, banks can now validate, store, and record payments transactions by serving as a node on an independent node verification network (INVN). Likewise, a bank can use INVNs and related stablecoins to carry out other permissible payment activities. However, any stablecoin arrangements “should have the capability to obtain and verify the identity of all transacting parties, including for those using unhosted wallets.”

The OCC’s guidance is a critical first step towards enabling US banks to provide financial services through stablecoin networks. However, the letter warns that banks thinking of engaging in INVN-related activities must also be aware of the potential risks posed to their institutions, including operational risks, compliance risk, and fraud. New technologies require enough technological expertise to ensure banks can manage these risks in a safe and sound manner.

The interpretative letter also stated that while banks should conduct due diligence and ensure they assess the AML and compliance risks associated with banking any stablecoin issuers, they should also ensure an understanding of the risks of cryptocurrency in general.

The US Securities and Exchange Commission (SEC) responded to the OCC Interpretation, stating that certain stablecoins might not constitute securities under federal law. According to the statement, the SEC is willing to provide a “no-action” position regarding whether or not activities with respect to certain stablecoins invoke the application of the federal securities laws.

US—Federal Reserve Board Governor Announces Co-Op with MIT to Research Digital Currency

On August 13, the Federal Reserve Board Governor Lael Brainard said the U.S.’s central bank has been testing digital ledger technology to understand the impacts of a digital currency on the existing payments ecosystem, monetary policy, financial stability, and the banking sector. Brainard said, “With these important issues in mind, the Federal Reserve is active in conducting research and experimentation related to distributed ledger technologies and the potential use cases for digital currencies.”

Brainard explained that the COVID-19 pandemic has advanced the need for “immediate and trusted access to funds.” She observed that the recipients of COVID-19 stimulus funds spent them quickly, indicating the level of urgency needed.

“To enhance the Federal Reserve’s understanding of digital currencies, the Federal Reserve Bank of Boston is collaborating with researchers at the Massachusetts Institute of

Technology in a multiyear effort to build and test a hypothetical digital currency oriented to central bank uses,” Brainard said.

In her speech, Brainard mentioned that the rise of other CBDCs and private cryptocurrencies underscores the need for the US to seriously pursue a digital currency solution. According to Brainard, the US government needs to “remain on the frontier of research and policy development,” given the dollar’s role in the global economy.

The Bahamas—Sand Dollar Sees Retail Use

On October 20, the Bahamas officially became the first nation to roll out a central bank digital currency (CBDC). The “Sand Dollar” is available to transfer via cellular phone for the country’s almost 400,000 residents and is accepted by merchants into Central Bank-approved e-wallets.

By December, the Bahamian Sand Dollar was in retail use—a world’s-first for a Central Bank Digital Currency (CBDC) outside of pilot programs. A health-foods cafe was one of the first establishments to accept payments in the Sand Dollar; \$130,000 of the currency is currently in circulation.

What was that first transaction? A green smoothie and a snapper fish burger, according to a report in Reuters.

China—Central Bank Digital Currencies Make Big Strides Forward

On October 12, Fan Yifei, deputy governor of the People’s Bank of China, announced the results of the digital yuan pilot. He shared that “the bank opened 113,300 consumer digital wallets and 8,859 corporate digital wallets.” Most impressive was that the “digital wallets processed RMB 1.1 billion (\$162 million) across 3.1 million digital yuan transactions between April and August when the pilots launched and ended.” These numbers make the digital yuan the most-used CBDC in a commercial setting.

Sweden—Taking Next Step on CBDC Development

In February 2020, Sweden announced the launch of the test phase of its CBDC, the e-krona, developed using blockchain technology by Sweden’s national bank Riksbank and Accenture. Now, almost a year later, it has moved onto the next step, a feasibility review led by Anna Kinberg Batra, the ex-chairwoman of the Riksbank’s finance committee. It’s estimated the review will be completed around November of 2021.

Even though the governor of Riksbank, Stefan Ingves, is enthusiastic about making the transition towards issuing digital currency, he still needs to convince Swedish parliament to make the move permanent. That should not be too difficult, as Sweden was named the world's most cashless region in 2018 by the Bank of International Settlements. That said, there remains some concern that elderly citizens and those who live in rural areas who still rely on cash for basic transactions will be left behind by the switch.

Australia—The CBDC Race Heats Up Down Under

On November 1, the Reserve Bank of Australia announced its intention of exploring a central bank digital currency. The Reserve Bank is partnering with Commonwealth Bank, National Australia Bank, Perpetual, and ConsenSys Software on the project.

Brazil—President of Central Bank Sees CBDCs as the Future of Finance

On September 2, Roberto Campos Neto, president of Brazil's central bank, said that his country could be ready to issue a central bank digital currency as early as 2022.

"To have a digital currency, you need an instant payment system that is efficient and interoperable; an open system, where you can create competition; and a currency that has credibility, is convertible and international," said Neto.

The central bank introduced PIX, an instant payment system, in November 2020 soft launch. Brazil's parliament is expected to vote on a proposal to modernize the country's exchange rate system before month's end.

Brazil's CBDC working group is studying the potential impacts of a national digital currency, and will present its findings in six to twelve months.

Private Sector—Citigroup Working with World Governments to Build CBDCs

Michael Corbat, the Chief Executive of Citigroup, was quoted at a December 2020 Bloomberg event saying that Citigroup is working with various governments around the world to assist them with building their own CBDCs. Although Corbat did not mention which specific governments the company is working with, he did say that they are working on both the development and commercialization of these CBDCs.

It was just three years ago when Corbat made the prediction that governments would launch CBDC initiatives in response to bitcoin; his bank has been researching cryptocurrencies since 2014.

Citigroup is just the latest addition from the private financial sector to join in on CBDC development, as Visa and Mastercard have also launched CBDC programs. As Corbat said at the Bloomberg event, CBDCs are an “inevitable” development in the future of money.

IOSCO—Global Stablecoins May Be Subject to Securities Regulation

On March 23, the Board of the International Organization of Securities Commissions (IOSCO) published Global Stablecoin Initiatives—a report examining the possible implications of global stablecoin initiatives on securities markets regulators and how existing IOSCO Principles and Standards could apply. The report features a hypothetical case study of a stablecoin set to be used for domestic and cross-border payments, using a reserve fund and a governance board. The Report concludes that, depending on its structure, global stablecoins could and would likely fall within securities market regulatory frameworks.

Sanctioned Countries

Russia

Russian Court Rules Theft of Bitcoin is Not a Crime

On June 30, a Russian court denied a motion to demand restitution for the victim of kidnapping and bitcoin larceny. The judge ruled that the larceny was not a felony because bitcoin, a virtual currency, does not enjoy the same property protection as real assets.

The case goes back to 2018 when two men impersonating Federal Security Service (FSB) agents kidnapped the victim and forced him into giving them 5 million rubles (approximately \$90,000 in US currency) in cash and 99.7 BTC — worth about \$900,000 at the time. The kidnappers were sentenced to eight- and ten-year prison sentences.

As part of the criminal proceedings, the victim requested the court rule to force the thieves to repay the funds that they stole from him. The court ruled partially in the victim's favor, asserting the thieves must repay the cash sum. However, when it comes to the cryptocurrency, the court declared that it is unable to satisfy the claim since virtual currencies are not recognized by Russia's laws as legal tender or its surrogate.

New Russian Crypto-Related Designations

On September 10, four individuals were added to OFAC's SDN List for attempting to influence the US electoral process. Three of the designated individuals were linked to supporting the cryptocurrency accounts of the Internet Research Agency (IRA)—a Russian "troll farm" tied to influence operations abroad on behalf of Russian political interests. According to OFAC, "the IRA uses cryptocurrency to fund activities in furtherance of their ongoing malign influence operations around the world." These designations include BTC, LTC, ZEC, and BSV addresses.

On September 16, two Russian nationals were added to OFAC's SDN List for their involvement in a sophisticated phishing campaign that targeted customers of two US-based and one foreign-based virtual asset service providers (VASPs) in 2017 and 2018. This attack resulted in combined losses of at least \$16.8 million. The designation includes Bitcoin, Bitcoin Gold, Litecoin, Ethereum, Ethereum Classic, DASH and ZCash virtual currency addresses and one Monero payment ID. This is the first time OFAC has listed Monero (XMR) in their designations.

To perpetrate their scheme, one of the fraudsters—Potekhin—spoofed the websites of numerous legitimate virtual currency exchanges to collect users' login credentials and gain access to their real accounts. According to OFAC, the duo employed a variety of methods to move the legitimate funds out of users' accounts, including the creation of exchange accounts with fake or stolen IDs; swaps to different virtual currencies, such as Monero; and moving the virtual currency through multiple intermediary addresses.

Once they had access to the funds, the second fraudster—Karasavidi—laundered all the proceeds of the attacks into an account under his name. Despite attempting to obfuscate the true nature of the funds by layering deposits through multiple accounts and multiple virtual currency blockchains, blockchain analytics were still able to trace the stolen funds to his account. The US Secret Service seized millions of dollars in virtual currency and US dollars from Karasavidi's accounts in a forfeiture action.

Iran

Amid a Struggling Economy, Iran Amends Regulations to Allow for Cryptocurrency-Funded Imports

On October 25, Iran Daily reported that the Iranian government has amended previously-enacted cryptocurrency regulations to allow for legally-mined cryptocurrencies to be exchangeable when used to finance imports from other countries. A CoinDesk report on the news suggested that this amendment was made in reaction to the country's need for an influx of international currencies to help its economy.

Iran Daily cited a report by IRNA, saying, "The miners are supposed to supply the original cryptocurrency directly and within the authorized limit to the channels introduced by the [Central Bank of Iran]." Iran Daily suggested that "[u]sing cryptocurrencies to fund imports could help the CBI evade restrictions imposed by the United States on Iran's use of the dollar system."

North Korea

6,000+ North Korean Hackers Hack for their Country, According to US Army Memo

A July 2020 US Army report on North Korean tactics revealed information on the hermit kingdom's infamous network of government-sanctioned hackers. According to the report, the DPRK has more than 6,000 hackers stationed in countries all over the world, including Belarus, China, India, Malaysia and Russia.

The report suggested that the group is overseen by Bureau 121, the cyber warfare guidance unit of North Korea. It is thought that the hackers generally do not launch cyberattacks directly from North Korea, as the country lacks the IT infrastructure necessary to enable such an undertaking.

North Korean hackers have conducted numerous high-profile hacks of financial institutions and international business. The notorious Lazarus Group has successfully stolen millions from several cryptocurrency exchanges, unleashed the WannaCry ransomware on the web, and broke into Sony Pictures and leaked unreleased content and other private info. According to the U.S. Army memo, the group's mission is to "create social chaos by weaponizing enemy network vulnerabilities and delivering a payload if directed to do so by the regime." It's also thought that the hackers use privacy coins to cover their tracks when converting funds into cash. This revelation highlights the need to continue developing methodologies for tracing illicit money flows via privacy coins.

Chinese Nationals Added to OFAC SDN List and Charged by DOJ for Laundering \$100 Million in Cryptocurrency Stolen by North Korea

On March 2, the U.S Treasury's Office of Foreign Assets Control (OFAC) added two Chinese nationals to the Specially Designated Nationals List (SDN) for their roles in laundering stolen cryptocurrency from a 2018 exchange hack. The two, Tian Yinyin and Li Jiadong, are purportedly associated with the Lazarus Group—North Korean state-sponsored cybercriminals believed to have been behind the Sony breach and WannaCry malware attacks, and \$2 billion in thefts from banks and crypto exchanges.

According to the Treasury press release, Tian and Li received approximately \$100.5 million worth of stolen crypto from North Korean controlled accounts. Tian ultimately moved more than \$34 million worth of these illicit funds through a bank account linked to his crypto exchange account. Li moved an additional \$33 million through linked accounts at nine different banks.

As a result of these sanctions, all property belonging to Tian and Li in the US or in the possession or control of US persons and entities must be blocked and reported to OFAC. In addition, persons that transact with Tian or Li, or with their sanctioned addresses, may find themselves penalized for sanctions violations or placed on the SDN list.

In parallel, the US Attorney for the District of Columbia has brought a Verified Complaint for Forfeiture in Rem against 113 virtual currency accounts linked to the theft and money laundering process. "Today's actions underscore that the Department will pierce the veil of anonymity provided by cryptocurrencies to hold criminals accountable, no matter where they are located," said Assistant Attorney General Benczkowski of the Justice Department's Criminal Division.

While the identities of virtual currency address owners are pseudonymous, these sanctions demonstrate how law enforcement can identify the owner of a particular cryptocurrency address by applying advanced blockchain analytics such as CipherTrace cryptocurrency intelligence. The use of accurate tools with high-quality attribution can not only reveal additional addresses controlled by the same individual or entity but also ensure that a financial institution or its customers are not transacting with sanctioned entities. Tian and Li's use of bank accounts linked to their crypto exchange accounts also demonstrates the importance of banks being able to detect crypto-related transactions in their payment networks.

Read our full analysis here: <https://ciphertrace.com/chinese-linked-dprk-laundering-analysis/>

Venezuela

U.S. Accuses Venezuelan President of Using Crypto to Conceal Illicit Drug-Running

On March 26, the Department of Justice indicted Venezuelan President Nicolás Maduro and 14 other officials for operating a narcotics ring involving drug runners, Colombian revolutionaries, and narco-terrorism. In a related press release, Homeland Security Investigations (HSI) alleged the conspirators used crypto to conceal their crimes.

At a press conference, then-United States Attorney General William Barr, along with the head of the Drug Enforcement Administration and the top federal prosecutors in Manhattan and Miami, accused Maduro of conspiring with a faction of the Colombian Revolutionary Armed Forces (FARC) rebel group “to flood the United States with cocaine,” and “devastate American communities.”

HSI Acting Executive Associate Director Alys D. Erichs alleged the conspirators used crypto to conceal their crimes. “Today’s announcement highlights HSI’s global reach and commitment to aggressively identify, target and investigate individuals who violate U.S. laws, exploit financial systems and hide behind cryptocurrency to further their illicit criminal activity,” explained Erichs. “Let this indictment be a reminder that no one is above the law — not even powerful political officials.”

Follow this code to read all of CipherTrace's quarterly reporting and learn more.



<https://ciphertrace.com/resources/>

CipherTrace protects financial institutions from cryptocurrency laundering risks and helps grow the blockchain economy by making it safe for consumers, trusted by investors and, accepted by governments.

Editorial Board, **Pamela Clegg and Dave Jevans**

Editor-in-Chief, **John Jefferies**

Financial Crime Analyst, **Julio Barragan**