

Cryptocurrency Crime and Anti-Money Laundering Report

CipherTrace
Cryptocurrency Intelligence
May 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 FATF 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

EXECUTIVE SUMMARY.....	6
<i>Sanctions Research.....</i>	7
MAJOR TRENDS AND DEVELOPMENTS.....	9
DEFI HACKS REACH RECORD HIGHS.....	9
1% OF BITCOIN TRANSACTIONS ARE “RISKY”	11
0.1% OF TRANSACTED BITCOIN VALUE IS “RISKY”	12
P2P TRANSACTIONS DOMINATE ETHEREUM NETWORK	13
MAJORITY OF TETHER TRANSACTIONS ARE P2P, BUT MAJORITY OF TETHER VOLUME INVOLVES A VASP	13
CRYPTO AND SANCTIONS—IRAN’S USE OF BITCOIN	15
SANCTIONS RESEARCH	15
CRYPTOCURRENCY AND SANCTIONS	18
BLOCKCHAIN IP DATA ENHANCES SANCTIONS COMPLIANCE	20
BITGO AND BITPAY PENALTIES FOR SANCTIONS VIOLATIONS	21
TERRORIST USE OF CRYPTOCURRENCY	23
HAWALA 2.0.....	23
MAJOR THEFTS, SCAMS, AND FRAUD	26
TURKISH EXCHANGE THODEX ACCUSED OF \$2 BILLION EXIT SCAM—64 ARRESTED	26
HOTBIT POST-HACK MAINTENANCE SPARKS FEARS OF EXIT SCAM	28
URANIUM FINANCE RUG PULLS WITH \$50 MILLION IN VARIOUS CRYPTOCURRENCIES ONE MONTH AFTER LAUNCH	28
MEERKAT FINANCE EXPLOIT RESULTS IN \$31M EXIT	29
TURTLEDEX EXITS WITH \$2.5M OF USER FUNDS	29
DEFI HEDGE FUND FORCE DAO ATTACKED	31
PAID NETWORK LOSES \$180M IN INFINITE MINT ATTACK	32
DODO CROWDPOLLS HACKED FOR \$3.8M IN FLASH LOAN	33
HACKERS STEAL \$5.7M FROM SOCIAL MONEY STARTUP ROLL	33
LIVECOIN SHUTS DOWN AFTER \$3.3M HACK	34
ENFORCEMENT ACTIONS.....	35
FORMER BITMEX CEO TO FACE TRIAL	35
UK BITCOIN SCAMMER FINED \$571 MILLION	35
IN-HOUSE TRADING SOFTWARE USED BY COINBASE RESULTS IN CFTC SETTLEMENT	36
FORMER CCO OF CRED REVEALED TO BE A UK FUGITIVE	36
AUTHORITIES INVESTIGATE CRYPTO SCAMS PROMOTED BY SOCIAL MEDIA INFLUENCERS	37
JOHN McAFFEE INDICTED FOR \$2 MILLION SECURITIES FRAUD	38
BITPAY ENTERS INTO \$507K SETTLEMENT WITH US TREASURY OVER MULTIPLE CRYPTO SANCTIONS VIOLATIONS.....	39
AUSTRALIAN MAN EMBEZZLED \$90 MILLION FROM US INVESTORS THROUGH FAKE CRYPTOCURRENCY FUNDS.....	39
ONTARIO MAN PLEADS GUILTY IN CASE OF MONEY LAUNDERER WHO OPERATED UNLICENSED MSB.....	40
CANADIAN NATIONAL CHARGED IN NETWALKER RANSOMWARE SCHEME	40
BULGARIAN CRYPTO EXCHANGE OWNER SENTENCED TO TEN YEARS’ IMPRISONMENT	41
JAPANESE AUTHORITIES ARREST 30 PEOPLE IN CONNECTION WITH 2018 COINCHECK HACK	42

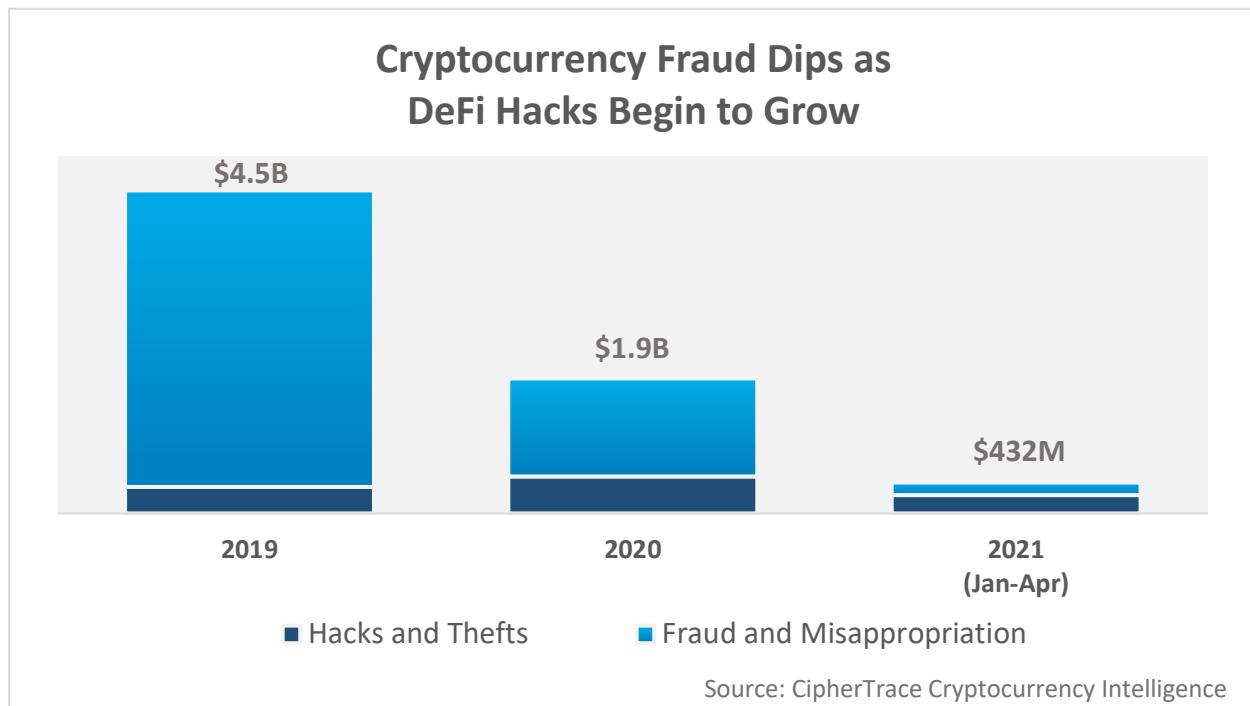
DARKNET MARKET NEWS	43
EUROPOL TAKES DOWN DARKMARKET, WORLD'S LARGEST ONLINE DARK MARKET	43
BIG BLUE MARKET EXIT SCAM	44
CORONA MARKET EXIT SCAM	46
LIME MARKET SHUTS DOWN	46
AJAX MARKET SHUTS DOWN	46
CHANGES IN GLOBAL REGULATORY REQUIREMENTS	47
PROPOSED FATF GUIDANCE FOR VIRTUAL ASSETS AND VASPs	47
UNITED STATES—FINCEN'S WALLET RULE ON ICE, BUT TRAVEL RULE MAY EMERGE	47
UNITED STATES—SEC RELEASES RISK ALERT AS A "COMPLIANCE WARNING" TO CERTAIN MARKET PARTICIPANTS	48
ARGENTINA—BCRA DEMANDS BANKS KEEP RECORD OF CLIENTS USING CRYPTOCURRENCY	49
CANADA—MSBs TO FACE NEW KYC AND TRAVEL RULE REQUIREMENTS FOR VIRTUAL CURRENCY TRANSACTIONS	49
JAPAN TAKES STEPS TO ADOPT FATF TRAVEL RULE	50
INDIA—CRYPTOCURRENCY USE TO BE BANNED THROUGHOUT INDIA	51
NIGERIA—CRYPTOCURRENCY'S NIGERIAN FUTURE UNCLEAR AFTER CENTRAL BANK PROHIBITIONS	51
SOUTH KOREA—NEW REAL-NAME CRYPTO LAWS COME INTO FORCE	51
TURKEY—BROAD BAN ON CRYPTO CLARIFIED	52
UK CRYPTO COMPANIES FACE NEW REPORTING REQUIREMENTS	52
CENTRAL BANK DIGITAL CURRENCIES (CBDCS)	53
UNITED STATES FINDS MORE SUPPORT FOR DIGITAL DOLLAR	53
<i>US Senator Sherrod Brown Says US Should Develop a CBDC</i>	54
JAMAICA'S FINANCE MINISTER WILL PILOT A CBDC IN 2021	54
RUSSIA PLANS TO PRESENT DIGITAL RUBLE PROTOTYPE BEFORE YEAR'S END	55
UAE AND ASIAN COUNTRIES JOIN CROSS BORDER PAYMENT BRIDGE	55
SOUTH KOREA STARTS FIRST PHASE OF ITS CBDC	56
BEIJING AND SUZHOU'S RESIDENTS RECEIVE DIGITAL YUAN AIRDROP FOR NEXT PHASE OF CBDC	56
INDIA MAKES MOVES TO EMBRACE CBDCS	57
IMF SAYS ONLY 40 COUNTRIES HAVE CLEAR LEGAL PATHWAY TO CBDC ISSUANCE	57
TURKEY MOVES TOWARD ESTABLISHING CENTRAL BANK DIGITAL CURRENCIES	58
UKRAINE HIRES STELLAR DEVELOPMENT FOUNDATION TO BUILD ITS CBDC	58
SANCTIONED COUNTRIES	59
NORTH KOREA	59
<i>Hackers Charged for Stealing Over \$100 Million from Crypto Firms</i>	59
RUSSIA	59
<i>US President Joe Biden Declares Russian Cyberattacks a National Emergency</i>	59
<i>Russian Anti-Money Laundering Body to Monitor Crypto-to-Fiat Transactions</i>	60

Highlights

- **Sanctions Research:** CipherTrace has detected more than 72,000 unique Iranian IP addresses linked to more than 4.5 million unique Bitcoin addresses. [pg 16]
- **DeFi-related hacks and fraud continue to grow quarter over quarter.** In just the first month of Q2 2021 the value of DeFi-related hacks and fraud has already surpassed Q1 2021's all-time high. [pg 8]
- **7 DeFi related hacks make up more than 60% of major hack and theft volume in 2021** [pg 10]. 3 DeFi related rug pulls make up 47.4% of major fraud and misappropriation in 2021. [pg 10]
- **By the end of April 2021 major crypto thefts, hacks, and frauds totaled \$432 million.** 240 million (55.4%) is related to DeFi hacks or fraud. [pg 7]
- **Report to the FATF Virtual Asset Contact Group:** 1% of Bitcoin transactions are "risky." Only 0.1% of transacted Bitcoin value is "risky." [pg 12]
- **P2P transactions dominate Ethereum network.** [pg 14]
- **While the majority of Tether transactions are P2P, the majority of Tether transaction volume involves a VASP.** [pg 15]

Executive Summary

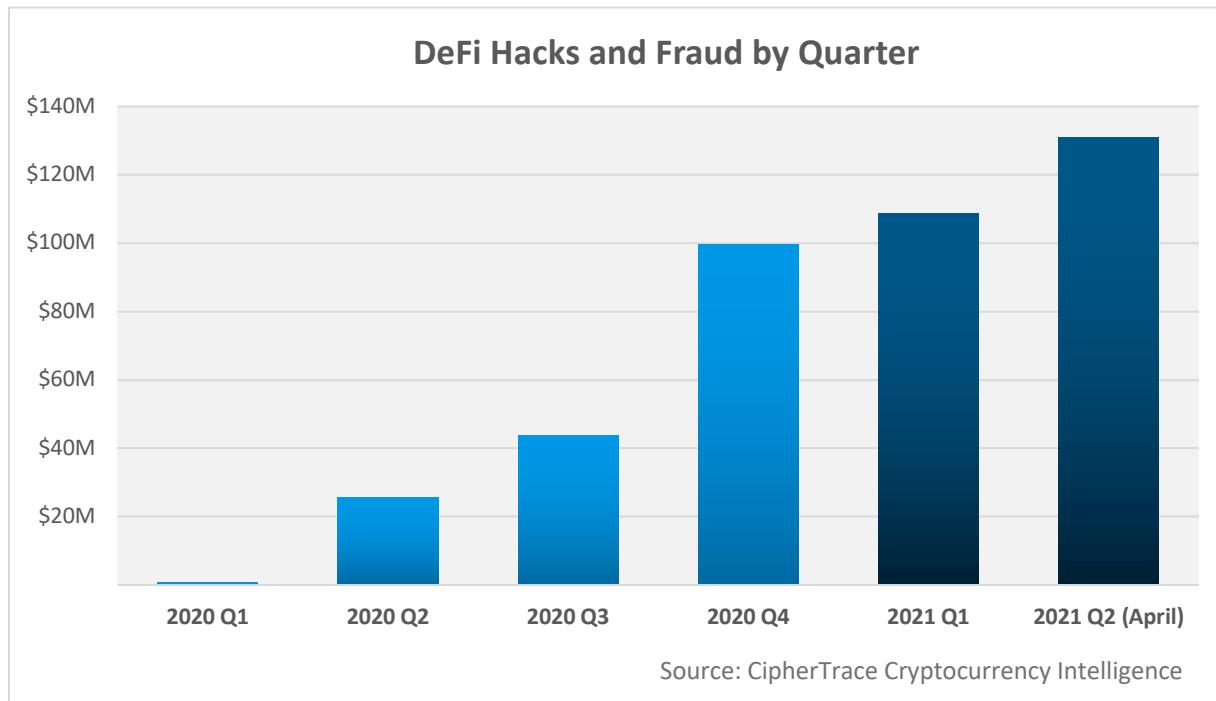
By the end of April 2021, major crypto thefts, hacks, and frauds totaled \$432 million. While this number may appear to be small when compared to previous years, a deeper look reveals an alarming new trend—DeFi-related hacks now make up more than 60% of the total hack and theft volume. This is up from only 25% in 2020; in 2019, DeFi Hacks were virtually non-existent.



At \$156 million, the amount netted from DeFi-related hacks in the first five months of 2021 already surpasses the \$129 million stolen in DeFi-related hacks throughout all of 2020.

DeFi-related fraud such as rug pull scams added an additional \$83.4 million to the total taken by criminals this year. These rug pulls make up 47.4% of the major fraud and misappropriation thus far this year.

The increase in DeFi-related hacks and fraud demonstrates a clear upward trend in DeFi-related crime, as illustrated in the chart below.

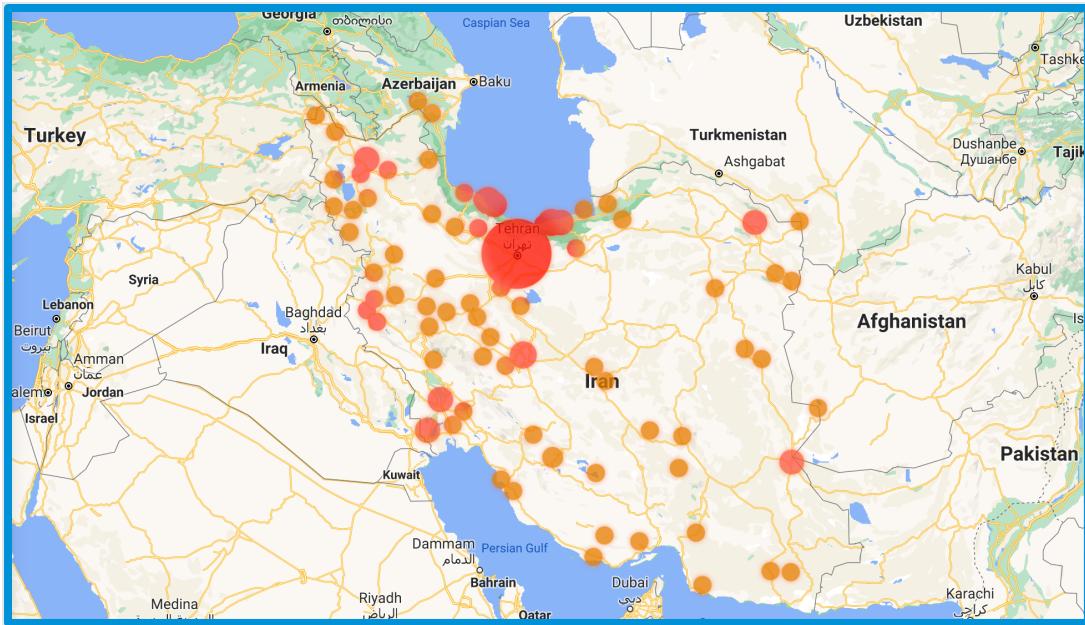


DeFi-related hacks and fraud continue to grow quarter over quarter.

Sanctions Research

Another trend detected by CipherTrace analysts is the substantial use of cryptocurrency in sanctioned geographies—most notably, Iran. As the US Treasury Office of Foreign Assets Control (OFAC) ramps up its enforcement actions against virtual asset service providers for sanctions violations related to blocked countries, it is vital that institutions screen IP data to ensure they aren't transacting with sanctioned entities and addresses.

CipherTrace detected more than 72,000 unique IP addresses linked to Iran. These addresses were either involved in direct cryptocurrency transactions or were used to query the blockchain to verify funds in cryptocurrency addresses that they control.



Location data derived from Iranian IP queries on the blockchain. Most activity centers around Tehran, Iran's capitol.

These IP addresses are not directly visible to banks, money service businesses or cryptocurrency exchanges. Because US sanctions generally prohibit the export of goods, services, or technology to Iran, if financial institutions, including exchanges, facilitate payments for an individual or company in Iran, those institutions would be exporting services to that person or entity in violation of the Iranian Transactions Regulations.

When it comes to cryptocurrency, avoiding sanctions risks should involve more than just monitoring for addresses and individuals listed in a country's designated sanctions list. IP attribution could provide critical data for a risk-based approach to anti-money laundering.

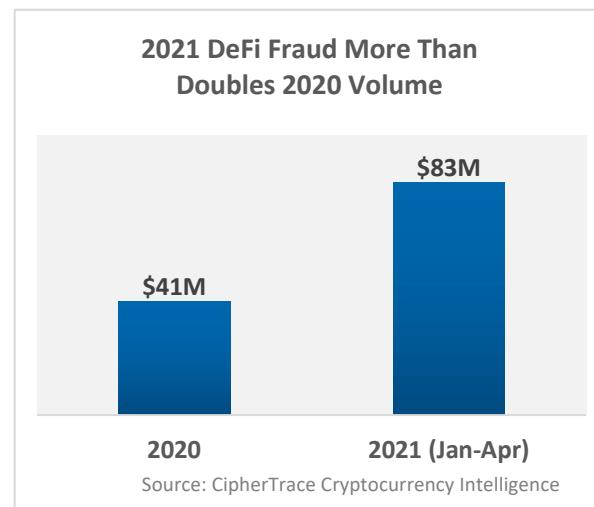
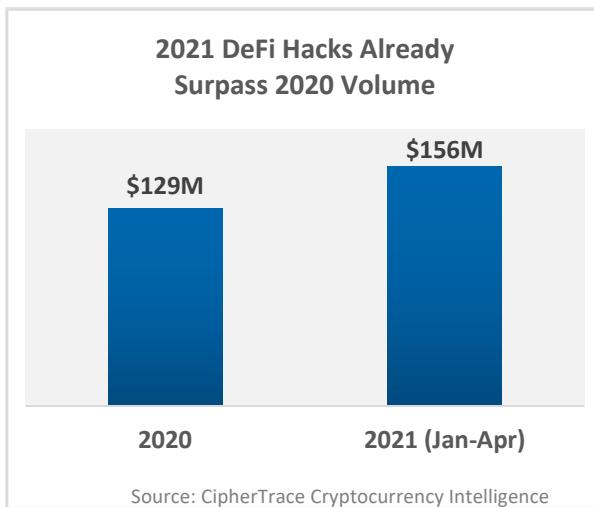
Major Trends and Developments

DeFi Hacks Reach Record Highs

By the end of 2020, DeFi locked in nearly a quarter of Ethereum's total market cap. By the end of April 2021, this total had grown to over 36%. But DeFi's explosive growth has attracted more than just new investors. Over 70% of all of 2021's major hacks and fraud thus far were DeFi related.

CipherTrace analysts found that attacks on DeFi made up more than 60% of the major hack and theft volume in 2021 and 47% of the major fraud and misappropriation. By the end of April 2021 criminals have netted nearly \$240 million from DeFi.

At \$156 million, the amount netted from DeFi-related hacks already surpasses the \$129 million stolen by hackers throughout 2020. DeFi-related fraud, such as rug pull scams, have added an additional \$83.4 million—more than 200% of 2020's DeFi fraud volume.

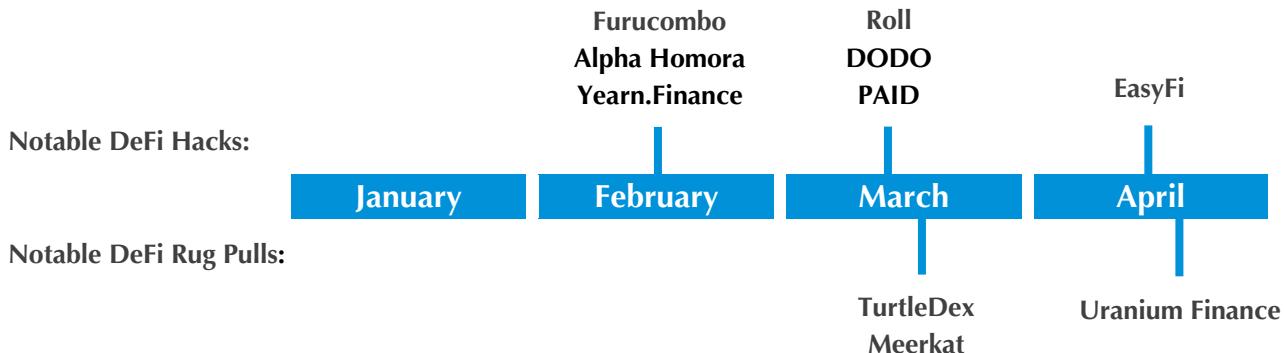


This increase in DeFi-related hacks and fraud demonstrate a clear uptrend in DeFi-related crime, as further demonstrated in the chart below.

DeFi-related hacks already make up more than 60% of major hack and theft volume in 2021



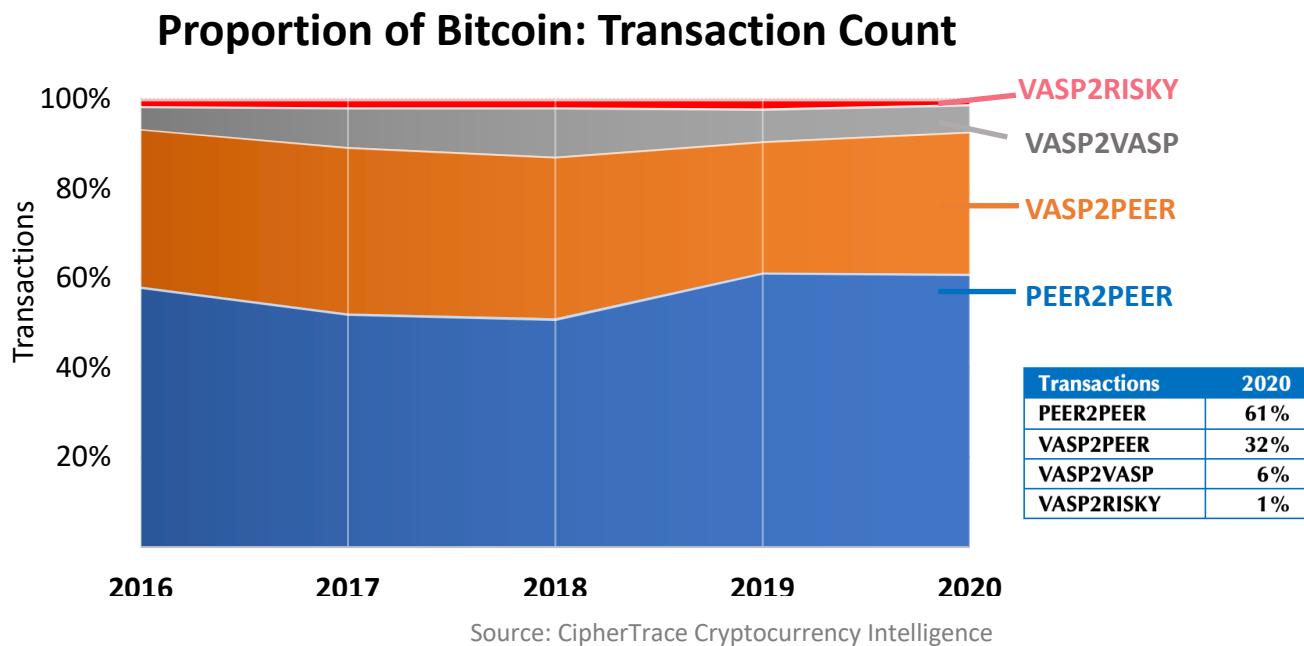
Source: CipherTrace Cryptocurrency Intelligence



1% of Bitcoin Transactions are “Risky”

In December 2020, global anti-money laundering watchdog the Financial Action Task Force (FATF) requested data from CipherTrace to help determine the proportion of virtual asset transactions that are with either a Virtual Asset Service Provider (VASP); an illicit or high-risk service provider; peer-to-peer.

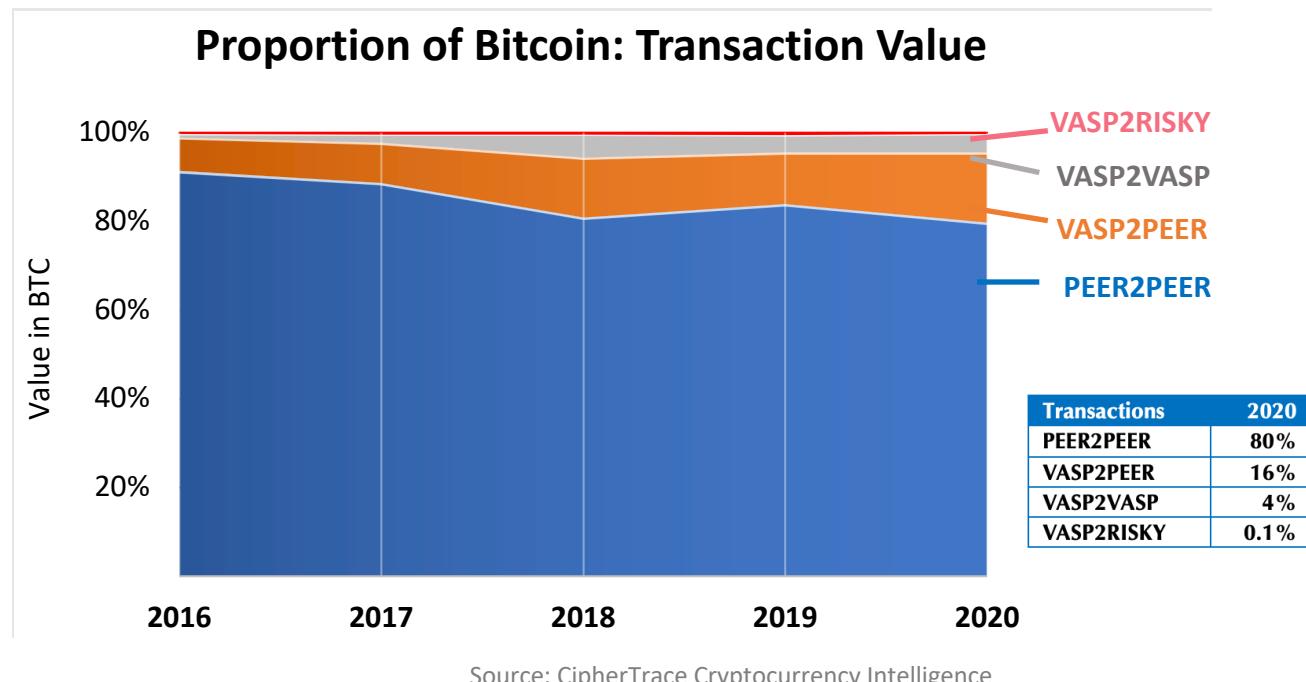
When looking the proportion of bitcoin transactions, CipherTrace analysts found that only 1.2% of transactions were between a VASP and a risky entity in 2020, 6% of transactions were between two VASPs, 32% were between a VASP and a private wallet, and 61% of transactions were P2P.



CipherTrace identifies “risky” transactions as transactions with an entity flagged as “High Risk” in any of CipherTrace’s blockchain forensic tools. Flagged entities include gambling sites, mixers, dark markets, HYIP, ransomware, malware, criminal actors, dark vendors and high-risk exchanges.

0.1% of Transacted Bitcoin Value is “Risky”

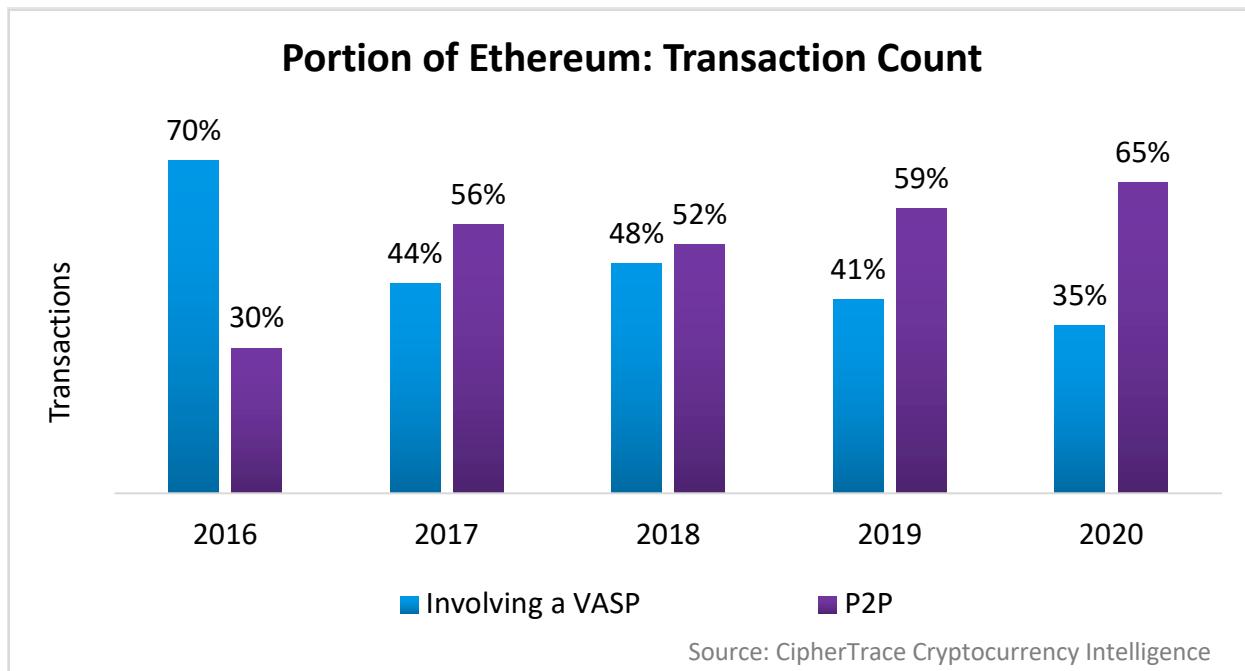
When analyzing the proportion of transacted bitcoin value in 2020, CipherTrace intelligence determined that the proportion deemed “risky” had dropped from over 1% to only 0.11%, indicating that the volume of BTC sent in these “risky” transactions is generally relatively low value transfers. This 0.1% will eventually need to be laundered before it can be cashed out. Comparatively, the United Nations Office of Drug and Crime estimates the amount of fiat money laundered globally in one year to be between 2-5% of global GDP, which would total from \$800 billion to \$2 trillion.



The proportion of risky transactions is 10 times higher than the underlying value of those transactions, indicating that larger transactions tend to be lower risk than high value transactions.

P2P Transactions Dominate Ethereum Network

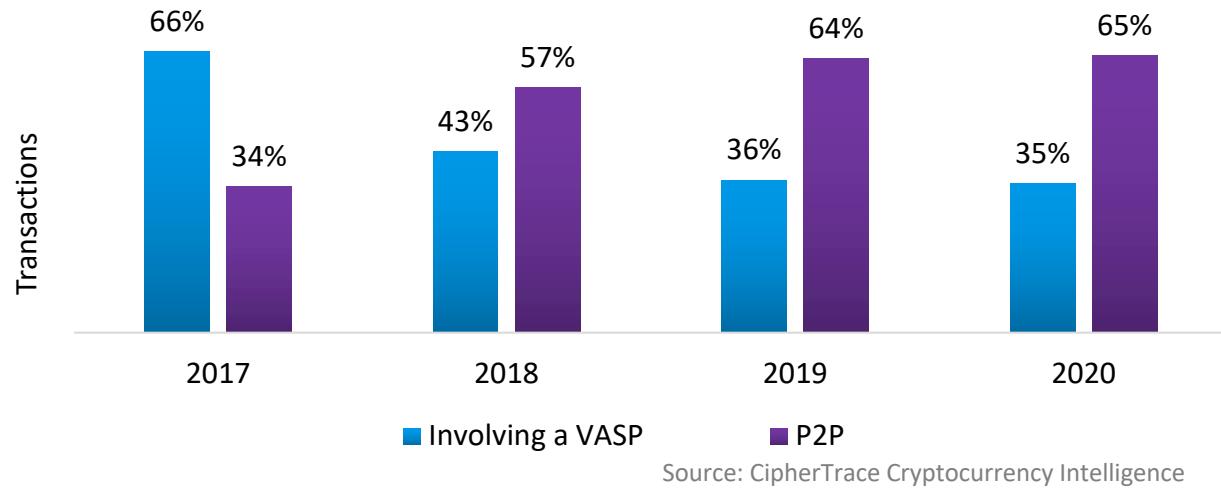
When comparing the proportion of Ethereum transactions that were P2P to those that involved a VASP, CipherTrace analysts found that the percentage of P2P transactions has been steadily climbing since 2016. This trend is likely due to the increase in DeFi protocols and DEXs that facilitate P2P transfers.



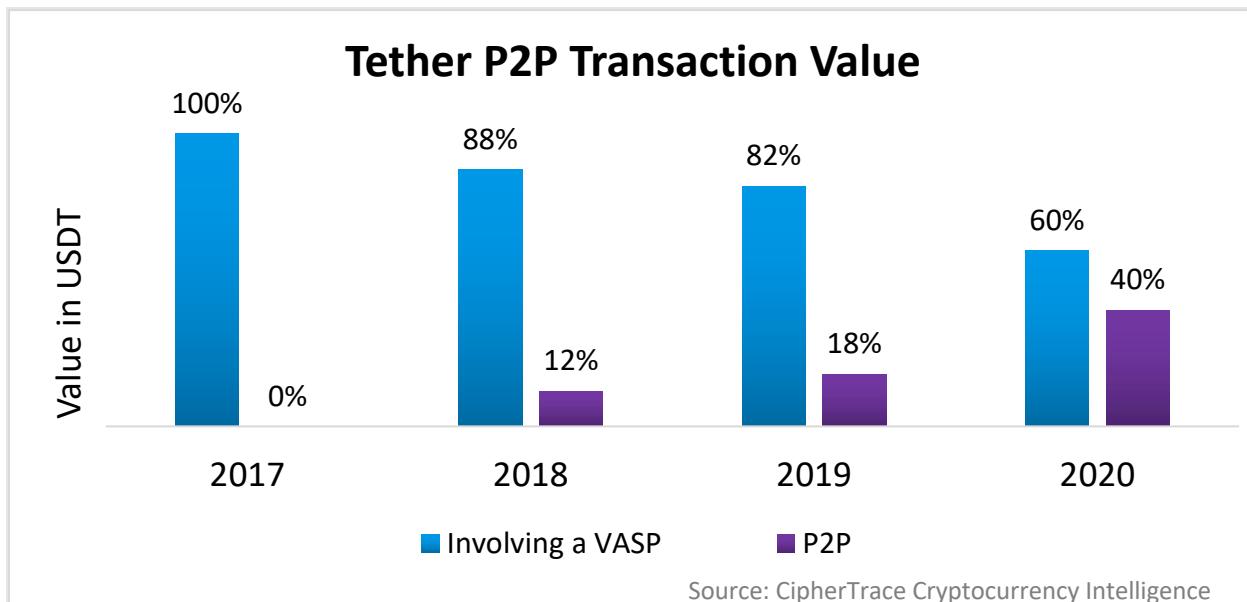
Majority of Tether Transactions are P2P, but Majority of Tether Volume Involves a VASP

Interestingly, CipherTrace analysis of the proportions of stablecoin transactions demonstrated that while a majority of Tether transactions were P2P in 2020, most of Tether's transaction volume involved an exchange.

Proportion of P2P Tether Transactions Double



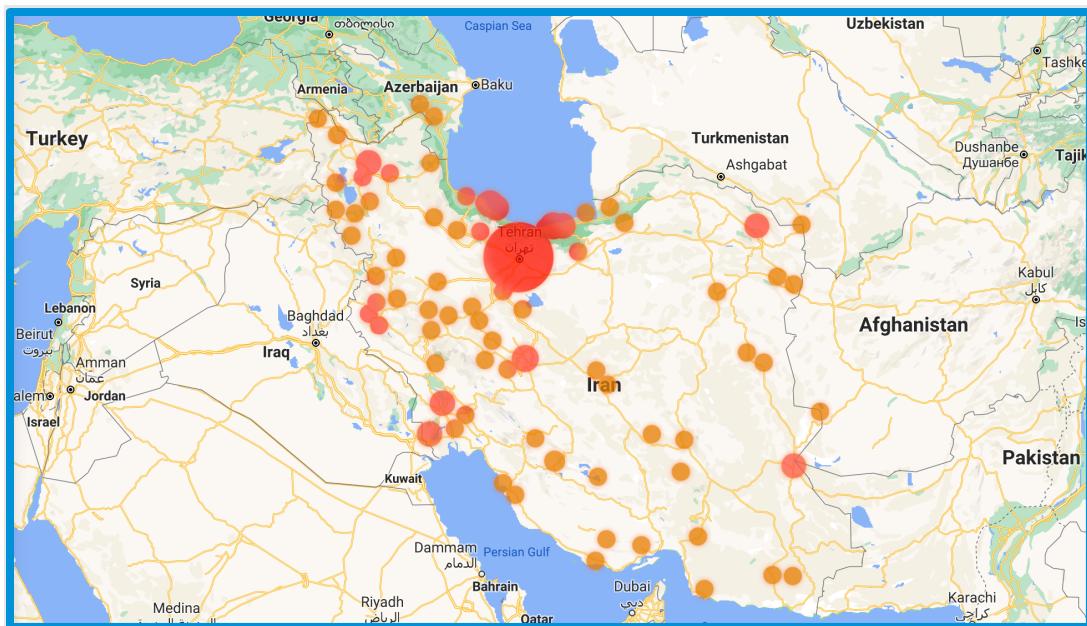
While the proportion of P2P Tether transactions has doubled since 2017, the bulk of USDT volume still involves a VASP, as noted in the chart below. This is likely because: i) USDT's prevalence in cross-exchange arbitrage operations as well as moving dollar pegged positions on and off chain and; ii) as USDT has become increasingly popular as a dollar-denominated payment rail for cross-border settlements, the number of P2P transactions continue to increase, though typically in smaller transactional value.



Crypto and Sanctions—Iran's Use of Bitcoin

Sanctions Research

Since monitoring sanctions-related IP usage across the Bitcoin blockchain, CipherTrace has detected more than 72,000 unique Iranian IP addresses linked to more than 4.5 million unique Bitcoin addresses. These Iranian IP addresses were either involved in direct cryptocurrency transactions or were used to query the blockchain to verify funds in cryptocurrency addresses that they control.



Location data derived from Iranian IP queries on the blockchain. Most activity centers around Tehran, Iran's capital.

Many of the tagged bitcoin addresses have been linked to multiple Iranian IPs, likely indicating the usage of mobile wallets connecting to multiple internet sources. IP addresses on mobile devices are constantly refreshed by service providers upon beginning new data sessions. These IP addresses are not directly visible on the blockchain, meaning

banks, money service businesses or cryptocurrency exchanges do not have direct visibility into the link between a bitcoin address and users in a sanctioned country that query it.

Iranian nationals are using Bitcoin to mine and liquidate funds as the country provides licensed mining operations with inexpensive electricity to power mining rigs. Mined funds can then be liquidated on the global market, often with no indication of which part of the world they came from if the addresses are not checked for linked IP queries.

When it comes to cryptocurrency, avoiding sanctions risks must involve more than monitoring for addresses and individuals listed in a country's designated sanctions list. These lists may include some of the cryptocurrency addresses associated with a designated person, however, they are often incomplete and only list a few addresses in the designated person's wallet. Blockchain analysis tools can fill these gaps.



"Institutions should consider reviewing blockchain ledgers for activity that may originate or terminate in Iran."

- US Financial Crimes Enforcement Network (FinCEN)¹

Financial institutions should take a risk-based approach when considering the likelihood that they may encounter sanctions issues. Financial institutions may consider additional indicators and the surrounding facts and circumstances, such as a customer's historical financial activity and the existence of other red flags, before determining that a transaction is suspicious.

IP data should supplement all sanctions risk mitigation strategies to ensure you're a financial institution isn't transacting with sanctioned countries. While the most common way to incorporate IP data is to collect it on customer logins to detect foreign persons accessing an institution, this tactic alone isn't enough to detect transactions to and from

¹ Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System:
<https://www.fincen.gov/sites/default/files/advisory/2018-10-11/Iran%20Advisory%20FINAL%20508.pdf>

sanctioned jurisdictions and is often easily thwarted by VPNs. Supplementing a financial institution's sanctions strategy with this additional IP data collected from the blockchain will help to ensure a more accurate view of the geographies in which customers transact or interact.

CipherTrace has already collected several million IP datapoints across sanctioned countries including North Korea, Syria, and Iran. Notably, CipherTrace analysts have detected an uptick in Iranian IPs querying the Bitcoin blockchain this past year compared to other sanctioned jurisdictions.

The screenshot shows a software interface for monitoring Bitcoin transactions. At the top, it displays 'ADDRESS: BITCOIN (BTC)' and 'CURRENT BALANCE BTC 1'. On the left, there's a sidebar with a green 'RISK' button labeled '2'. The main area shows a table titled 'TAGGED IP ADDRESSES' with one entry: 'IP ADDRESS 5.12 MAP IRAN DATE [redacted]'. Below this, there are filters for 'FILTER TRANSACTION' (set to 'ALL ADDRESSES') and 'DATE RANGE FIL' (set to '1/3/2009'). To the right, there are sections for 'MY CASES' and 'SHARED CASES', both currently empty. At the bottom, there's a table with two rows, each showing a redacted address, a blue 'C' icon, 'EXCHANGE', and 'UNITED STATES'.

BTC address associated with an Iranian IP accessing a large US exchange

US sanctions generally prohibit the export of goods, services, or technology to Iran. If financial institutions, including exchanges, facilitate payments for an individual or company in Iran, those institutions would be exporting services to that person or entity in violation of the Iranian Transactions Regulations.

“Institutions should consider reviewing blockchain ledgers for activity that may originate or terminate in Iran.”

- US Financial Crimes Enforcement Network (FinCEN)

One likely explanation for this uptick in Iranian IPs is the abundant increase of Bitcoin mining by Iranian actors. Many of the new Iran-associated addresses interact with mining pools.

Recommendations for Compliance Officers:

1. **In addition to screening customer IP data upon login, VASPs should screen counterparty addresses for IP data linked to sanctioned countries.**
2. **VASPs must not rely solely on sanctions lists for restricted addresses; there are often additional related addresses in the same wallet, controlled by the sanctioned party, that were not included on the sanctions list.**

Cryptocurrency and Sanctions

On November 28, 2018, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) added two bitcoin addresses to its list of Specially Designated Nationals (SDNs) for the first time ever. These two addresses belonged to two Iranian-based cryptocurrency brokers who laundered 6,000 BTC over 40 exchanges for SamSam ransomware actors and others.

Since 2018, OFAC has sanctioned 67 additional addresses, including Bitcoin, Ethereum, Litecoin, Bitcoin SV, Bitcoin Gold, Dash, Zcash, and Monero addresses. However, CipherTrace analysts have discovered that the addresses that end up on OFAC's SDN list are only a small handful of the actual addresses under the sanctioned person's control or in their "wallet." The use of blockchain analysis is necessary to uncover the additional addresses under the sanctioned person's control but not listed by OFAC or other consolidated lists of persons.

If a financial institution is unaware of these additional addresses, it runs the risk of unknowingly transacting with sanctioned persons.

"Treasury will aggressively pursue Iran and other rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards to further their nefarious objectives."

- US Treasury Under Secretary for Terrorism and Financial Intelligence,
Sigal Mandelker²

With the addition of cryptocurrency to the US sanctions list, the Department of Treasury has clarified that the cryptocurrency addresses listed in the SDN list aren't exhaustive and any additional addresses associated with designated addresses should also be blocked.³

Additional, IP data should be incorporated into all sanctions compliance programs that deal in web-based activity⁴, such as cryptocurrency transactions. The anonymity that internet-based transactions provide often increases sanctions risk exposure. Many internet-based financial service companies already have IP address blocking procedures; however, these procedures are usually limited to uncovering customer IP data upon login. While this approach can be effective initially, it does not fully address a web-based financial institution's compliance risks.

Blockchain technology allows financial institutions to gather additional IP data on counterparties that is impossible to see in traditional web-based transactions. This data

² Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses: <https://home.treasury.gov/news/press-releases/sm556>

³ How will OFAC identify digital currency-related information on the SDN List: <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626>

⁴ OFAC Compliance for Internet, Web Based Activities, and Personal Communications: <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/73>

can help inform compliance teams of whether a counterparty transaction is to or from a sanctioned country and prevent potential violations.

Blockchain IP Data Enhances Sanctions Compliance

CipherTrace has already collected over 72,000 unique Iranian IP addresses. Many of these addresses have already transacted with large exchanges domiciled in regions that could constitute a sanctions violation—such as in the US.

Unlike traditional financial institutions, Virtual Asset Service Providers (VASPs) have an increased risk of inadvertently transacting with sanctioned jurisdictions simply because of the pseudonymous, cross-border nature and global reach of cryptocurrency transactions. VASPs should use IP data derived through blockchain analytics to enhance their compliance programs and reduce sanctions risk exposure.

Transactions to and from addresses with an IP associated with a sanctioned country should be a red flag for any VASP. While IP blockchain data alone cannot guarantee that an address belongs to actors in a given region, it is enough to demonstrate significant interest from a person in the sanctioned jurisdiction and should trigger enhanced due diligence for the account holder transacting with the potentially sanctioned address.

Financial institutions should perform additional inquiries and investigations where appropriate to ensure that their assessments are in line with their internal risk profile. IP addresses can also be used by institutions to search for additional bitcoin addressees associated with a customer or counterparty IP. These additional insights can be beneficial for an institution's risk and threat assessments and suspicious transaction reporting requirements.

Sanctions Obfuscation Red Flags

Sanctioned persons will often attempt to conceal their illicit activity, making it essential for any compliance team to know how to identify red flags that could indicate an attempt to obfuscate sanctions violations. Unlike a traditional financial institution, Virtual Asset Service Providers (VASPs) can directly send funds to unhosted (private) cryptocurrency wallets anywhere in the world, increasing their sanctions risk exposure. To help mitigate these risks, financial institutions should be able to identify the following red flags:

- 🚩 **A customer sends or receives funds to or from a cryptocurrency address associated with multiple IP addresses from a sanctioned jurisdiction.**
- 🚩 **A customer's deposit address at your institution has been queried by an IP from a sanctioned jurisdiction.**
- 🚩 **A customer sends or receives funds to or from a cryptocurrency address in the same cluster (wallet) as a sanctioned address, even if the address itself has not been identified by any sanctions list.**

Bitgo and Bitpay Penalties for Sanctions Violations

At the end of 2020, OFAC levied its first enforcement action against a VASP for sanctions violations. According to OFAC, 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.

... OFAC emphasized that “sanctions compliance obligations apply to all US persons, including those involved in providing digital currency services.”

OFAC and Bitgo eventually came to a settlement of \$93,830. In the enforcement action, OFAC emphasized 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.

OFAC 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. The Enforcement Action 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.

Then, on February 18, 2021, OFAC entered into a \$507,000 settlement with cryptocurrency payment provider BitPay. The enforcement action claims BitPay allowed persons from sanctioned jurisdictions, such as North Korea, Iran, Sudan, and Syria, to transact with merchants in the United States using crypto from BitPay’s platform.

While BitPay screened its direct customers—the merchants—against OFAC’s List of Specially Designated Nationals and Blocked Persons (the “SDN List”) and conducted due diligence to ensure they were not located in sanctioned jurisdictions, OFAC claims BitPay failed to screen location data that it obtained about its merchants’ buyers. This resulted in 2,102 transactions on behalf of individuals who, based on IP addresses, were located in sanctioned jurisdictions.

This was OFACs second enforcement action in two months against a VASP for sanctions violations related to blocked geos. These two recent actions show how important it is to screen IP data to ensure VASPs aren’t facilitating sanctioned transactions.

Terrorist Use of Cryptocurrency

Hawala 2.0

Before cryptocurrency, the use of Hawaladars and their underground banking system was one of the quickest and easiest ways for immigrants and foreign workers to transmit remittances across the world without the use of the standard global financial system. Because Hawala is unregulated, with no record keeping or reporting requirements, it was also a boon for illicit activity, such as terrorism financing and money laundering. The Hawala system has been used to finance operations by ISIS, al-Qaeda, al-Shabab, and other terrorist organizations.

Modern technologies have reinvented the traditional Hawala system for bad actors, making it even easier to send funds cross-border with little oversight. In September 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. As with Hawala, the receipts for these “coupons” purchased in France were then cashed out by operatives in Syria linked to Hay'at Tahrir al-Sham (HTS), an al-Qaeda affiliate.

The arrest of these operatives, as well the Federal District of Columbia Court of the United States Complaint of Forfeiture outlining how Syrian militants used cryptocurrency to fund terrorist operations and the role blockchain analytics played in determining the flow of funds, has led many Telegram channel and group managers linked to terrorism financing to stop publicly posting deposit addresses for cryptocurrency donations; instead, interested parties are instructed to contact them in person to obtain a deposit address.

MagniFILE, an anonymous group of Syria-focused independent journalists who publish on Telegram, identified additional Telegram channels associated with extremist crowdfunding campaigns through a combination of open-source intelligence and information provided by pro-government forces that are investigating the use of cryptocurrency by extremist groups and terrorists.

According to its Telegram channel, during the course of its investigation MagniFILE uncovered more than 120 Telegram group chats and channels, such as Bitcoin Transfer, which are purportedly connected with HTS and ISIS.

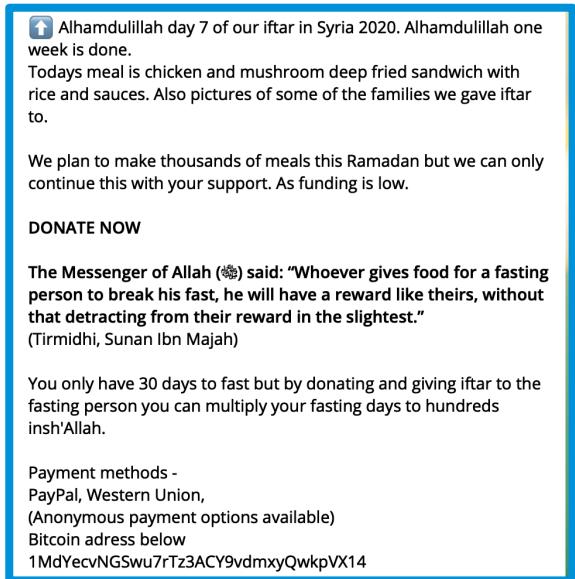
According to MagniFILE's research, HTS has accepted more than \$250,000 in donations through BitcoinTransfer since 2018 in order to fund its independent exchange offices in Idlib and other "liberated" provinces in Syria.



Source: MagniFILE Telegram page

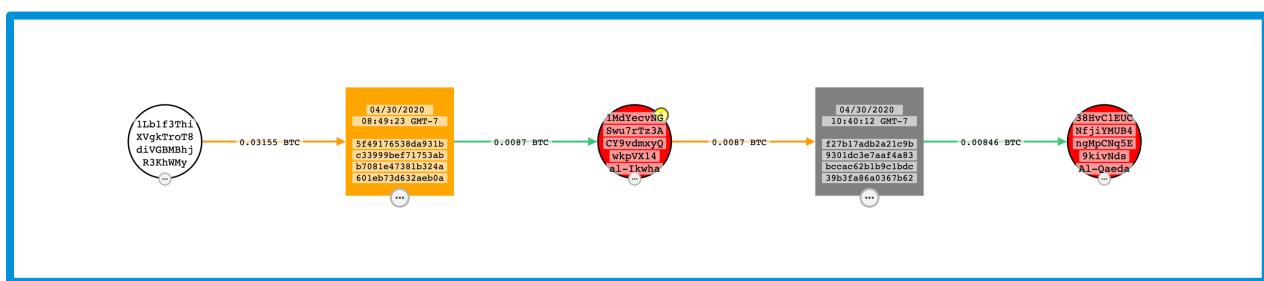


Bitcoin Transfer advertise their services in Arabic, English, Russian, Chinese, French, and Turkish



Post calling for Iftar donations on April 30, 2020

In particular, on April 30, 2020, the group posted in the channel calling for donations to support sending Iftar meals to the poor during Ramadan. CipherTrace traced the donation made on this day to al-Ikhwa's deposit address, which was then sent directly from the group to al-Qaeda.



Using CipherTrace Inspector, analysts can see donations go from al-Ikhwa directly to an al-Qaeda controlled address.

Another such channel belonging to the Syrian terrorist organization al-Ikhwa remains active and continues to solicit bitcoin donations during Ramadan to one of several published addresses. The donations purportedly go to feeding and clothing "widows, orphans, and families in need"; however, a blockchain trace of donations made in 2019 and 2020 showed that these funds were sent directly to addresses belonging to al-Qaeda.

Major Thefts, Scams, and Fraud

Turkish Exchange Thodex Accused of \$2 Billion Exit Scam—64 Arrested

On April 22, Istanbul's chief prosecutor's office announced it had opening a probe into cryptocurrency exchange Thodex amidst allegations of an exit scam affecting roughly \$2 billion in user funds after the exchange's owner left the country as user withdrawals halted.

While initially claiming the exchange was down due to "maintenance" on April 18, the exchange continues to be inaccessible. In a message on the Thodex website homepage, shown below, owner Faruk Fatih Özer confirmed that he left Turkey for Albania while denying the alleged exit scam, claiming he was visiting foreign investors in Albania. As of this writing, customers are still unable to access funds.

Distinguished Users of Thodex:

There has been a need to inform the public and dear users who use our Thodex Platform about the period we have lived.

First of all I want to indicate: publicly, my company is Koineks Teknolojileri A.Ş. and many of the claims made about the Thodex platform it owns are unfounded.

Thodex platform, where nearly 700,000 users have traded, has not victimized anyone until today and will not do so anymore. 25,000,000,00 TL, which occurred as a result of the cyber attack against our company in 2018. Without reflecting the damage to any of our users, our company tolerated it with its own means and made serious infrastructure changes in order not to experience a cyber attack again.

Considering the financial structure of the company and the number of users, it has attracted the attention of many domestic and foreign investors and received very serious partnership offers at the international level. When the financial and digital data were examined together during the partnership negotiations that have been going on for about 3 months, it was determined as of last week that there was an abnormal fluctuation in the company accounts. Thodex Platform has been temporarily closed to determine the reasons and sources of this. While our technical team of our company was conducting this research, I personally went abroad on 19.04.2021 to make final meetings with foreign investors.

In the examination of company accounts, it was determined that the cyber attack incident continued and the correct data of some account holders could not be reached.

The allegations that 391,000 people disappeared after a loss of about 2 billion USD, which was reflected to the public on 22.04.2021, are unfounded. It is necessary to make this statement in order to respond urgently to these claims that go beyond the limits of honesty and conscience.

Firstly; According to our preliminary findings, only 30,000 of our nearly 700,000 users have a suspicious situation, and the corresponding bank entry fees of these people on the platform are available in their company accounts. In this respect; I first announce to the public that no users will be victims.

ALSO; A TEAM OF PEOPLE WITH THE EXPERT INTRODUCING THEIR OWN TO THE SOCIAL MEDIA, IF NECESSARY THROUGH THE PRESS BROADCAST ORGANS, MAKES THE PUBLIC APPROACH WITH AN AMOUNT THAT DOESN'T COMPLY WITH MIND, LOGIC AND ACCOUNT. FOR; You THODEX LEAVE ALL TRADING VOLUME OF TRADING VOLUME The CRYPTO MONEY IS NOT THIS LEVEL PLATFORMS IN TURKEY.

Thus; The records of our company have been previously submitted to the information of institutions such as MASAK, CMB, the Ministry of Treasury and Finance, and it is confirmed by the records of the relevant institutions that there are no irregularities.

This process has turned into a slander campaign with inaccurate and exaggerated discourses, causing harm to both users and myself. For; According to our determinations, the payments will be made after the accounts of around 30,000 users are cleared. While our company, whose market value is approximately 40 million USD as of today, can continue its commercial life, as a result of the perception of victimization created in the public, our company is prevented from continuing its commercial life.

The important thing I ask dear users is that the statements not made by our company are not respected. We personally are making the return to Turkey in a few days in cooperation with judicial authorities led to the emergence of real and I declare I will do my best to make every effort to prevent the victimization of users. I would like to be known strongly that; I accept that even such an opinion is attributed to me as a cruelty, as I have never had an activity that would harm my state or nation in any period of my life.

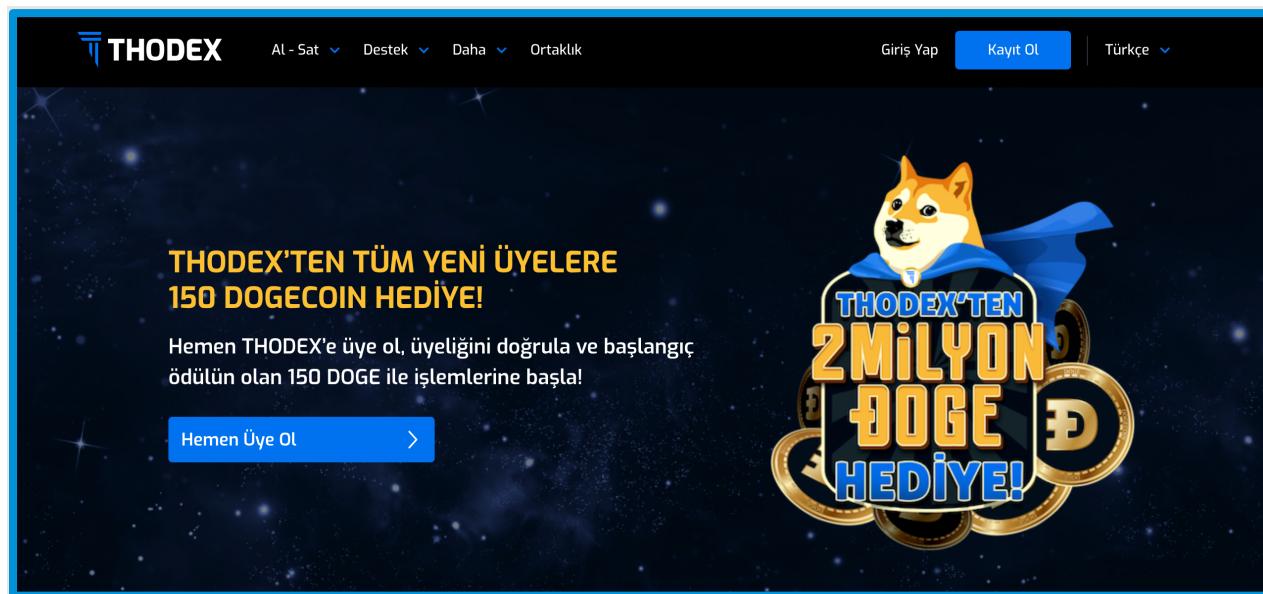
In this way; I kindly submit to the public's knowledge that the smear campaign against both myself and my company should not be respected.

Thodex homepage message (translated to English). At the time of this report, the website is still displaying this message and customers continue to be unable to login.

According to Turkey's state-run Anadolu news agency, on April 23 police raided Thodex central offices, resulting in the arrest of 62 people, including both Özer's sister and brother. On April 28 police arrested an additional two people in Albania accused of providing shelter to Özer.

There is currently an Interpol red bulletin requesting Özer's arrest.

If true, the Thodex exit scam would be the second largest exit since PlusToken, which netted admins over \$2.9 billion in 2019.

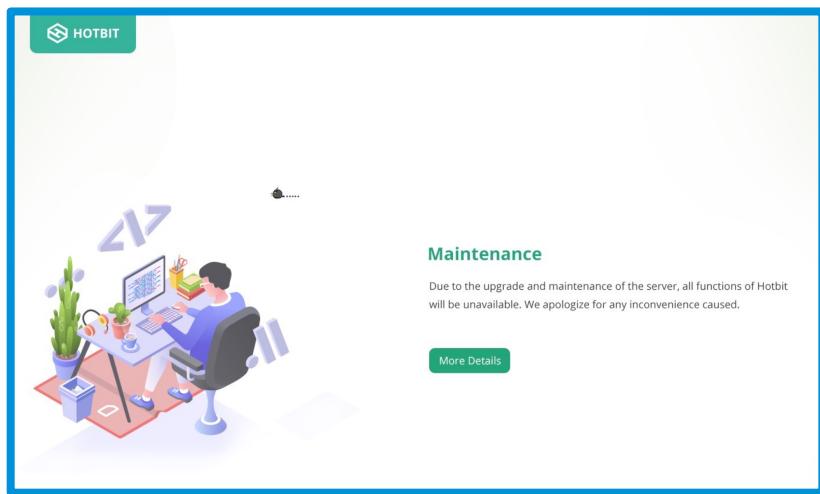


Before Thodex went dark they had just finished running a promotional campaign that gave away free Dogecoin for new customers. The exchange locked in those investments and did not allow the coins to be sold or converted into other cryptos.

This is a developing story. CipherTrace continues to investigate this alleged exit scam.

Hotbit Post-Hack Maintenance Sparks Fears of Exit Scam

On April 29, Chinese crypto exchange Hotbit shut down for an extended maintenance period after reporting a cyber-attack. While wallets were not breached, other user data was compromised, with the exchange warning users to be vigilant for phishing schemes and to ignore communications from anyone claiming to be a Hotbit representative.



While the chief security officer offered assurances via Telegram, there are fears that the hack and maintenance period could be cover for a multi-million-dollar exit scam. As of the time of this report, Hotbit was purportedly conduct various tests on their trading server. The exchange continues to leave frequent updates on its social media channels.

Uranium Finance Rug Pulls with \$50 Million in Various Cryptocurrencies One Month After Launch

On April 27, DeFi project Uranium Finance disclosed on Twitter that hackers took advantage of various bugs in their code during their v2.1 token migration event. The platform reported a total loss of \$50 million USD in the form of BTC, ETH, DOT, ADA, USDT and their native coin u92. The breach came just one month after the platform's launch.

Shortly after the announcement, crypto Twitter was quick to call out the Uranium Finance team and question the validity of the hack. Since Uranium Finance has been around for just around one month, many users were suspect of their explanation and labeled the ordeal as a rug pull.

At the time of this report, the bug has yet to be patched and users are advised to withdraw their funds cease giving liquidity on the project.

Meerkat Finance Exploit Results in \$31M Exit

On March 6, DeFi project Meerkat Finance was drained of about 13 million BUSD and roughly 73,000 BNB, which totaled \$31 million at the time of the attack. While the project claimed on its official telegram channel that the attack was the result of hackers, on-chain data revealed that the Meerkat's smart contract that contains the project's vault business logic was altered the day before the hack. These changes were made using the original Meerkat deployer's account, suggesting that either the private key of the Meerkat deployer was compromised or the hack was in fact a rug pull.

Soon after the Meerkat website and twitter accounts were deleted, further signifying a rug pull.

TurtleDex Exits with \$2.5M of User Funds

On March 19, just days after their presale of 9,000 Binance tokens worth roughly \$2.5 million, TurtleDex, a Binance Smart Chain (BSC) DeFi project, performed a rug pull on its investors. The project's developers drained funds from trading pools on PancakeSwap and ApeSwap, converted them to Ether and send the funds to large, centralized exchanges in

an attempt to cash out. While the project had previously been audited, no critical security issues were previously identified.

The social media accounts associated with the protocol were deleted soon after the exit.

EasyFi Hacked for \$80 Million in MetaMask Attack

On April 19, EasyFi Network, a DeFi project on Polygon Network, reported that a hacker stole roughly \$80 million worth of funds from its wallet. According to the protocol's postmortem, the EasyFi smart contracts were not exploited. Instead, the private keys to the network admin MetaMask account had been compromised through EasyFi founder and CEO Ankitt Gaur's administrative computer.

This pattern deviates from the typical MetaMask attack, in which phishers obtain private keys or mnemonic phrases by tricking users into downloading a malicious version of the wallet app. At the end of last year, many users fell victim to MetaMask attacks after sponsored ads for a fraudulent version of the MetaMask site displaced the real site as the top search result on Google.

Read more about the attack on our blog: <https://ciphertrace.com/alert-malicious-crypto-browser-extension-masked-metamask/>

The postmortem can be found here: <https://medium.com/easify-network/easyfi-security-incident-pre-post-mortem-33f2942016e9>

Alpha Homora Loses \$37 million in Iron Bank Exploit

On February 13, an attacker drained \$37 million from DeFi protocol Alpha Homora by leveraging Cream's Iron Bank protocol-to-protocol lending platform. The attacker used Alpha Homora to borrow and lend repeatedly with Cream Finance's Iron Bank, which

allowed for leveraged lending. A few missing input checks in very specialized conditions allowed the hacker to abuse Alpha Homora's privilege of borrowing an unlimited amount of funds from Cream Finance's Iron Bank.

Alpha Homora had previously been audited by Quantstamp and PeckShield.

The postmortem can be found here: <https://blog.alphafinance.io/alpha-homora-v2-post-mortem/>

Furucombo Hit with \$14M “Evil Contract” Hack

On February 27, the Furucombo proxy was compromised by an attacker. The attacker used a fake contract to make Furucombo think that Aave V2 had a new implementation, resulting in all transfers being sent to an arbitrary address. This exploit netted the attacker over \$14 million in stolen funds. Furucombo has since deauthorized the relevant components.

The full postmortem can be found here: <https://medium.com/furucombo/furucombo-post-mortem-march-2021-ad19afd415e>

DeFi Hedge Fund Force DAO Attacked

DeFi hedge fund Force DAO was the victim of an attack made by five different hackers on April 4. The attack was uncovered by Polymath's blockchain team lead Mudit Gupta on Twitter, who provided each attacker's address and the amount stolen. After one attacker returned their share, Force DAO recorded a loss of \$376,000 USD worth of FORCE tokens, which also saw an 80% drop following the attack.

The postmortem can be found here: <https://blog.forcedao.com/xforce-exploit-post-mortem-7fa9dcba2ac3>

PAID Network Loses \$180M in Infinite Mint Attack

On March 5, PAID Network, a DeFi platform geared towards businesses, fell victim to an "infinite mint" hack that led to an 85% token price drop while the contract code was exploited. Though the attacker netted \$180 million in PAID tokens at the time of the attack, only a portion of the tokens were converted to wrapped ether, while the rest rapidly lost value.

The PAID Network team released a tweet explaining, "We are investigating the issue. We pulled liquidity, are creating a new smart contract, & will be restoring everyone's original balances to before the hack."

Nick Chong of Parafi Capital tweeted, "Paid Network's deployer, an EOA, transferred ownership of a contract to the attacker 30 mins before the mint," suggesting a member of EOA may have been either directly responsible for the rug pull or allowed the attack to take place through poor security oversight.

The full postmortem can be found here: <https://paidnetwork.medium.com/paid-network-attack-postmortem-march-7-2021-9e4c0fef0e07>

Yearn.Finance's DAI Vault Loses \$11M in Flash Loan Exploit

On March 4, an exploit against Yearn's v1 yDAI vault led to the project losing 11 million DAI of vault deposits. By creating exchange rate imbalances in Curve's 3pool, the hacker

was able to cause Yearn's yDAI vault to deposit and withdraw funds from 3pool at unfavorable rates across a series of transactions. By withdrawing from yDAI and from the 3pool, the attacker received rewards of Curve's DAO Tokens for providing liquidity during a time when the DAI rate strayed from the pool's other two assets. The hacker was able to net about \$2.8 million from the attack.

The full postmortem can be found here: <https://github.com/yearn/yearn-security/blob/master/disclosures/2021-02-04.md>

DODO Crowdpoools Hacked for \$3.8M in Flash Loan

On March 8, several DODO V2 Crowdpoools were attacked, including WSZO, WCRES, ETHEA, and FUSI. Hackers exploited a bug in the v2 crowdpooling smart contract which allowed a function to be called multiple times, allowing the exploiter to create a counterfeit token that would initialize the smart contract and execution of a flash loan to transfer all the real tokens from the pools. The exploit resulted in \$3.8 million being drained from the pools.

The full postmortem can be found here: <https://dodoexhelp.zendesk.com/hc/en-us/articles/900004851126-Important-update-regarding-recent-events-on-DODO>

Hackers Steal \$5.7M from Social Money Startup Roll

On March 14, hackers compromised the hot wallets of social money startup Roll to steal roughly \$5.7 million worth of ETH. As a result of the hack, a number of "social tokens"—cryptocurrencies supporting online communities—on the platform lost more than half their value. The hack was confirmed on Twitter by WHALE, a social coin on the Roll platform.

The hacker quickly sent the ETH to privacy-enhanced crypto wallet Tornado Cash in an attempt to obfuscate the flow of funds.

Livecoin Shuts Down After \$3.3M Hack

Russian crypto exchange Livecoin announced plans to shut down after being the victim of what they characterized as “a carefully planned attack” in December 2020. This attack led to users losing a total of \$3.3 million.

Livecoin users lost 106 bitcoin (BTC), 380 ether (ETH), 236 bitcoin cash (BCH), 567,000 XRP, 66.8 million DOGE, 56,000 Tether (USDT), and some other ERC-20 tokens. Livecoin told its users to contact them via email to receive their payments after going through a verification process. However, they only accepted payment claims for the next two months, which ended on March 17. There is little information available about how much value remained after the attack.

Enforcement Actions

Former BitMEX CEO to Face Trial

Arthur Hayes, the former BitMEX CEO charged with violating the Bank Secrecy Act for failure to institute money-laundering controls, flew from Singapore to Hawaii to surrender to U.S. authorities on April 6th. Hayes was released on \$10 million bail while awaiting trial. Two other BitMEX co-founders have likewise surrendered, while a fourth executive, Gregory Dwyer, remains in Bermuda at the time of this report.

UK Bitcoin Scammer Fined \$571 Million

After defrauding over 1,000 individuals of over 22,000 bitcoin (valued at about \$143 million at the time), the US District Court for the Southern District of New York entered a default judgement against a UK man at the heart of the scheme in March.

According to the Commodity Futures Trading Commission, Benjamin Reynolds of Manchester was found guilty of defrauding and misleading members of the public on social media and is required to pay \$143 million in restitution as well as \$429 million in civil penalties. He is also barred from conduct that violates the Commodity Exchange Act and CFTC regulations, and cannot trade in any CFTC regulated markets or register with the CFTC.

In-House Trading Software Used by Coinbase Results in CFTC Settlement

On March 19, popular crypto platform Coinbase was fined \$6.5 million by the Commodity Futures Trading Commission (CFTC) in response to a number of allegations surrounding their GDAX trading platform, also known as Coinbase Pro. Complaints detail that the platform misled its users by displaying inaccurate and misleading information pertaining to digital assets. The CFTC is also alleging wash trading by a former unnamed Coinbase employee.

In a statement to Decrypt, Coinbase said, "Coinbase has reached a settlement with the CFTC regarding activities that happened and ended years ago. The settlement order today does not include any finding of harm to any Coinbase customer." In an unusual move, CFTC Commissioner Dawn Stump issued a concurrent statement alleging illegal market manipulation but saying that the CFTC does not have jurisdiction over Coinbase.

Former CCO of Cred Revealed to be a UK Fugitive

Cryptocurrency lending company Cred, currently under investigation by Delaware bankruptcy court, employed UK fugitive and prison escapee James Alexander as the firm's Chief Capital Officer (CCO). March court documents shed light on Alexander's troubled past, including a three-year prison term for possessing illegal money transfers in the UK. He was later transferred to a facility where he participated in a breakout, leading to his fugitive status. Alexander allegedly funneled over \$2 million in both bitcoin and US fiat to his personal accounts.

Though there were a number of factors leading to Cred's bankruptcy filing, the platform's decision to employ UK fugitive James Alexander was a major contributor. CipherTrace supported the investigation by tracing and blocking the flow of bitcoin to James

Alexander's personal accounts, demonstrating the value of blockchain analytics in investigations involving cryptocurrencies.

Authorities Investigate Crypto Scams Promoted by Social Media Influencers

On March 24, the US DOJ charged Instagram influencer Jegara Igbara, also known as "Jay Mazini," with defrauding followers out of \$2.5M in BTC.

According to the DOJ, between January to late February Mazini offered to pay followers between 3.5% to 5% over market value for Bitcoin, claiming traditional crypto exchanges had capped how much Bitcoin he could purchase. After Mazini received Bitcoin from his fans, he sent back falsified wire transfer receipts to reflect the agreed-upon prices. In reality, he either failed to send the full amount or never sent the money.

According to the complaint filed on March 23, Mazini negotiated with one of his followers to purchase 50 BTC for \$2.56 million, with the seller sending the agreed amount of BTC to only receive \$500,000 in return.

Scams involving influencers and celebrities are not new. Sohrab Sharma, co-founder of the massive crypto scam Centra Tech, was handed an eight-year prison term by the Southern District of New York after luring investors into participating in a \$25 million scam. Sharma partnered with celebrities like Floyd Mayweather and DJ Khaled to bolster interest from investors. Mayweather and Khaled were ultimately required to pay fines to the SEC for their involvement.

John McAfee Indicted for \$2 Million Securities Fraud

Although already arrested in December for tax evasion, on March 5 John McAfee, founder of the eponymous antivirus software company, was charged with securities fraud and money laundering for his involvement in a cryptocurrency scheme. Prosecutors allege that McAfee and Jimmy Gale Watson Jr., his executive advisor and bodyguard, made \$2 million by encouraging their Twitter followers to invest in Reddcoin and Dogecoin as McAfee and Watson sold their own holdings in the tokens as prices rose. The scam ran between December 2017 and October 2018; during this period, McAfee would tweet about the "coin of the day" and "coin of the week." Aside from already being sued by the SEC for promoting fake ICOs last year and accused of murder in Brazil, McAfee faces potentially up to twenty years in prison.

McAfee is not the only the highest-profile accused fraudster to be facing charges; the US Department of Justice announced on March 4 that a Swedish citizen, Roger Nils-Jonas Karlsson, pleaded guilty to running a fraudulent crypto and gold investment scheme that defrauded victims of \$16 million. Karlsson was the founder of Eastern Metal Securities, a website used to draw investor interest. The site promised that investors could earn an eventual return of 1.15kgs in gold (equivalent to \$45K USD as of Jan 2019) for just \$100 per share paid for in bitcoin. Karlsson used a second website to communicate reasons for delayed pay-outs with such justifications used as "releasing so much money all at once could cause a negative effect on financial systems throughout the world." Karlsson was found and arrested in Thailand in 2019, where he had bought a home with the money he stole from investors.

BitPay Enters into \$507K Settlement with US Treasury Over Multiple Crypto Sanctions Violations

On February 18, the US Treasury's Office of Foreign Assets Control (OFAC) entered into a \$507,000 settlement with cryptocurrency payment provider BitPay. The enforcement action claims BitPay allowed persons from sanctioned jurisdictions, such as North Korea, Iran, Sudan, and Syria, to transact with merchants in the United States using crypto from BitPay's platform.

While BitPay screened its direct customers—the merchants—against OFAC's SDN list and conducted due diligence to ensure they were not located in sanctioned jurisdictions, OFAC claims BitPay failed to screen location data that it obtained about its merchants' buyers. This resulted in 2,102 transactions on behalf of individuals who, based on IP addresses, were located in sanctioned jurisdictions.

This was OFACs second enforcement action in two months against a VASP for sanctions violations related to blocked geos. It is vital for VASPs to screen IP data to ensure they aren't engaging in sanctioned transactions.

Australian Man Embezzled \$90 Million from US Investors through Fake Cryptocurrency Funds

On February 4, an Australian citizen living in the United States pleaded guilty to falsely leading investors to put a total of \$90 million into two of his fraudulent cryptocurrency firms. Twenty-four-year-old Stefan He Qin committed this crime over a period of three years from 2017-2020, during which time he created the fake funds known as "Virgil Sigma" and "VQR Multistrategy Fund." Qin faces 20 years in prison.

The Department of Homeland Security Special Agent in charge said, "Qin orchestrated this reprehensible criminal scheme for many years, making misrepresentations and false promises that coaxed investors into pouring millions of dollars into fraudulent cryptocurrency firms, all the while stealing the hard-earned money of his investors." The Virgil Sigma fund used an algorithm that took advantage of price differences of crypto assets across over 40 exchanges throughout the globe.

Ontario Man Pleads Guilty in Case of Money Launderer Who Operated Unlicensed MSB

On January 29, a 49-year-old man by the name of Hugo Sergio Mejia from Ontario, California pled guilty to running an unlicensed money service business for two years that saw \$13 million worth of bitcoin exchanged illegally. Mejia advertised his company on a couple of different websites, posted on encrypted messaging apps, and met with clients in-person.

Mejia was caught when a member of law enforcement posed as a potential client and made five transactions, totaling \$250,000, exchanging bitcoin for cash. After his arrest, Mejia agreed to forfeit all the assets that he received through his illegal activities, which included crypto, cash, and silver coins and bars. He faces a maximum of 25 years in prison.

Canadian National Charged in NetWalker Ransomware Scheme

On January 27, the Department of Justice announced a series of actions against the NetWalker ransomware group, in coordination with international law enforcement partners. NetWalker was first detected in August 2019 and has victimized local

governments, educational institutions, corporations and more; even the healthcare sector has been attacked in the midst of the continuing COVID-19 crisis.

Sebastien Vachon-Desjardins, a Canadian man, is facing charges after allegedly obtaining more than \$27 million from NetWalker victims. The DOJ also seized more than \$450,000 worth of cryptocurrency paid as ransom by victims in three separate attacks.

Bulgarian Crypto Exchange Owner Sentenced to Ten Years' Imprisonment

On January 12, the owner of RG Coins was sentenced by a federal jury in Kentucky to ten years' imprisonment. Rossen Iossifov was earlier found guilty of money laundering and conspiracy to commit racketeering. RG Coins defrauded over 900 Americans and conducted money laundering operations for an eastern European cybercrime syndicate; 17 of the 20 principal actors in the scheme have been arrested, charged, and found guilty to date. Iossifov's associates used advertisements for expensive (and non-existent) cars and other luxury goods on auction sites to lure unwary buyers; Iossifov then laundered the ill-gotten cash into crypto.

Europol Arrests Ten Hackers for \$100M SIM Swapping Attacks Against Celebrities

On February 10, European law enforcement agency Europol arrested 10 people for their role in a series of SIM swapping attacks targeting thousands of victims throughout 2020, including famous internet influencers, sport stars, musicians and their families. The attackers are estimated to have stolen \$100 million worth of cryptocurrencies.

Japanese Authorities Arrest 30 People in Connection with 2018 Coincheck Hack

Back in 2018, Japanese exchange Coincheck was the victim of a hack that saw over \$500 million worth of NEM lost in what is still the largest exchange hack. In January, the Japanese police were able to arrest 30 people connected to the hack by tracing the accounts at crypto exchanges where the hacked funds were converted. There is a suspicion that Russian hackers are to blame for infecting the computers of Coincheck employees with a virus that allowed for the remote takeovers.

Previous to these arrests, authorities had only identified two men as having bought stolen NEM through dark net sellers at the time the hack happened. When the men were questioned by the police, they admitted that they knew where the funds had originated from and did not seem to care as they were able to buy those funds at a discounted rate.

Darknet Market News

Europol Takes Down DarkMarket, World's Largest Online Dark Market

On January 12, DarkMarket, the world's largest online marketplace on the dark web, was officially taken down through an operation that included six European countries and the United States. Before it was taken offline, DarkMarket had about 500,000 users who collectively sent an estimated 4,650 bitcoin transfers and made 12,800 Monero transactions. In total, about €140 million worth of cryptocurrency passed through its payment network. The vendors on this marketplace mostly sold drugs, malware, SIM cards, and stolen credit card details.



An Australian man living in Germany, suspected to be the head of DarkMarket, was arrested. The German Cybercrime Unit was able to switch off the site's servers, some of which were located in Moldova and Ukraine. The police hoped that the information

stored on these servers would provide more insight into who else was involved, including vendors and buyers.

Europol was able to provide the German authorities with analytics and coordination with other countries. Through their European Cybercrime Centre, Europol established a Dark Web team so countries across Europe could be better equipped to investigate and later prosecute those involved in Dark Web crimes. Europol plans to provide training initiatives as well as awareness campaigns as an educational tool.

Big Blue Market Exit Scam

Big Blue Market, a darknet market known for its coin swapping service and an embedded lottery, exit scammed in April 2021. The market admins attempted to target the exit scam at users of the popular darkmarket forum Dred, only allowing users they believe not to use the forum to withdraw funds. Their final announcement has been transcribed below.

Big Blue's Final Announcement

Hello all. I just wanted to state that Big Blue admin has left the building as the blue admin. Big Blue has stopped all operations since yesterday, given how our other markets are listed and got banners on dread and passed threw un-detected by the gate keepers of this whole industry (/u/hugbunter ,/u/paris ,/u/darkdotfail ,/u/darknetlive) Big blue is no longer needed.. its just a pile of evidence at this point. Given the sheer amount of abuse we have received, due to being overtly vocal on the power structure that currently rules this industry and saying the quite part out loud. Blowing the whistle on how the (dread , ddf, darknetlive) takes a percentage of an exit scam's in order to push the market visibility. You can see why blue marching to the beat of our own drum has made many enemies.. its affects how the top makes there money.

Some users where able to make withdrawals yesterday , If they met certain conditions. Conditions are as follows. If you have a dread account that corresponds user/vendor account you where disqualified from from a withdrawal. Also if you vend on monopoly market and also have a blue account .. that money is gone you where disqualified. So only a handful where able to get there money back, the rest have to take there lumps along with the other hundreds and thousands of people that lost there money due to using dread, this is no different if a dread market was to exit scam (Olympus , pax romana , invictus , imypaire , soon darkn0de) these are just recent examples. If they can do it so can we.

I understand there will be a few smiles on there faces because of this message , so i want to just leave one more thing. I just want to drive home one more lesson bout this game and sticking it dread and the rest. I have taken the liberty to unencrypt the whole db including pass's ,convos ,tracking address, etc etc . In 12 hours time we are going to shoot this db to the 3 letter agency's for maximum damage to the dread community. Maybe this should be a lesson to Hb and paris that they just cant treat people like shit. If they cared , they could buy the db from us ..but don't hold your breath, they are very hardheaded. Anyways Just wanted to put this out let everyone know

See ya on the next market

666

Corona Market Exit Scam

Corona Market links went offline in March of 2021. The market admin released the following statement:

Greetings, friends.

This is Corona Market's admin.

If you read this message it means I'm dead or in a prison which means the same for me.

I have lethal sickness and market was my try to collect money for surgery.

Probably it was not enough time.

This message was set up to show up if I don't turn it off for 7 days.

All escrow money was automatically sent to my family to support them.

I'm sorry for your lost and hope you won't curse me.

Thanks to everyone who supported me. Stay safe. Peace.

Lime Market Shuts Down

Lime Market is estimated to have gone offline between December 2020 and February 2021. Due to its small size, it's likely the market never saw much business and eventually decided to go offline, stealing any funds that may have been on the market. Lime Market claims to have been created and run by the admins of Darkbay, a previous darknet market that was shut down in a similar exit scam.

Ajax Market Shuts Down

Ajax Market appears to have gone offline in March 2021, less than three months after its launch. No real listings had been seen on Ajax, but it had been announced on Dread. It's likely the market didn't see much business and shut down quietly.

Changes in Global Regulatory Requirements

Proposed FATF Guidance for Virtual Assets and VASPs

On March 19, 2021, global anti-money laundering watchdog the Financial Action Task Force (FATF) released a public consultation for its updated Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Key changes in the draft guidance include:

- DEXs and crypto escrow
- services are considered Virtual Asset Service Providers (VASPs)
- Stablecoins are virtual asset (VAs) and FATF Standards apply to them
- Only NFTs that can facilitate money laundering and terrorism financing are VAs
- VASPs should assess and mitigate proliferation financing (PF) risks
- Best practices for counterparty VASP due diligence
- Options for mitigating peer-to-peer transaction risks
- New Travel Rule clarifications and guidance

Read our full analysis of the draft guidance on our blog: <https://ciphertrace.com/analysis-proposed-fatf-guidance-for-virtual-assets-and-vasp/>

United States—FinCEN's Wallet Rule on Ice, but Travel Rule May Emerge

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

While the comment period for the NPRM on transactions involving unhosted wallets was re-opened and extended, the Travel Rule NPRM was not.

If approved, the new Travel Rule proposal would require financial institutions to collect and store transfer information on international payments—including crypto transfers—at a much lower threshold. Currently, US financial intuitions 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.

As of the time of this report there have been no updates on the status of the NPRM, however, it is likely that some form of the new travel rule requirements are soon to become law.

United States—SEC Releases Risk Alert as a "Compliance Warning" to Certain Market Participants

On February 26, the Securities and Exchange Commission's (SEC) Division of Examinations released a risk alert detailing the compliance risks facing certain market participants, including investment advisors, broker-dealers, securities exchanges, and transfer agents.

Market participants should expect SEC examiners to review books and records as well as custody practices. Broker Dealers should expect examiners to focus on regulatory compliance with AML and CTF laws as well as sanctions. The alert warns of the hurdles to comply with AML laws when dealing with pseudonymous cryptocurrencies. Challenges aside, it is the responsibility of all market participants to file suspicious activity reports when appropriate.

Argentina—BCRA Demands Banks Keep Record of Clients Using Cryptocurrency

According to an April 2021 leaked internal memo, the Central Bank of the Argentine Republic (BCRA) has asked banks within their authority to keep a record of every user who makes a transaction in cryptocurrency. Details such as each user's address, account number, type of account, names, and their Unique Tax Identification Code are being recorded and shared with the BCRA, who claim they need this information to "monitor the functions of payment systems." Argentina's crypto community has reacted with alarm, suggesting that this move could be the first step towards the central bank blocking customers with crypto accounts.

Canada—MSBs to Face New KYC and Travel Rule Requirements for Virtual Currency Transactions

In March, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Canada's Financial Intelligence Unit, issued new guidance for MSBs operating in the country. Under the new rules, MSBs and foreign MSBs will be required to identify clients from which they are receiving virtual currency equivalent to \$10,000. The transfer, exchange, or remittance of virtual currency equivalent to \$1,000 CAD will likewise trigger KYC verification requirements.

VASPs that initiate virtual currency transfers worth \$1,000 or more must send the following information to abide by Canada's Travel Rule regulations:

- the date of the transfer;
- the type and amount of each VC that is involved in the transfer;
- if the client is a person, their name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the client is an entity, its name, address and the nature of its principal business;
- the name and address of each beneficiary;
- for every account affected by the transfer:
- the account number and account type; and
- the name of each account holder;
- every reference number connected to the transaction that is meant to be similar to an account number;
- every transaction identifier including transaction hashes or similar identifiers (if applicable) and every sending and receiving address;
- and the exchange rates used and their source.

MSBs are expected to comply with the updated guidance by June 1, 2021.

Japan Takes Steps to Adopt FATF Travel Rule

Japan's Financial Services Agency has announced its intention to adopt FATF's Travel Rule recommendations by April of 2022. The FSA asked that the Japanese Virtual Currency Exchange Association prepares for the regulation, saying, "From the perspective of ensuring the proper and reliable execution of the crypto asset exchange business, we will examine the accurate implementation of the travel rule in terms of technology and operation. We would like the JVCEA to establish a necessary system, so please inform the members of the association."

The country has yet to release the final text of the proposed regulations.

India—Cryptocurrency Use to be Banned Throughout India

The Indian government has announced in March that they will enact a blanket ban against cryptocurrency use, causing panic among cryptocurrency holders in the country. Mining, selling, holding, issuing, and transferring cryptocurrency in India will all be illegal in 3-6 months. Holders are now left with three options: liquidate their holdings, transfer their cryptocurrency to a trusted friend or relative, or send their cryptocurrency to a self-hosted wallet.

At the time of this report, there have yet to be any set deadlines for the proposed ban.

Nigeria—Cryptocurrency's Nigerian Future Unclear After Central Bank Prohibitions

On February 9 the Nigerian Central issued a circular to prohibit financial institutions from providing services to crypto exchanges. In response, the Nigerian SEC put a hold on planned regulations for cryptocurrencies; the Senate plans to summon the governor of the central bank to appear before relevant committees to further discuss the future of cryptocurrency regulations in the country.

South Korea—New Real-Name Crypto Laws Come into Force

In March 2020, the South Korean government passed an AML measure requiring real-name accounts be used by crypto exchanges. The Act on Reporting and Using Specified Financial Transaction Information, also known by the acronym FTRA, puts significant new administrative requirements in place for exchanges, including registration with the Financial Intelligence Unit. On March 25, 2021, the law officially entered into force with a six-month grace period for VASPs to comply.

Turkey—Broad Ban on Crypto Clarified

The Turkish government clarified plans to restrict the exchange of cryptocurrency after announcing a general ban which was to take effect April 30. According to Bloomberg, “The government is planning to establish a central custodian bank to eliminate counterparty risk.”⁵ The Turkish central bank had previously stated that payment providers will no longer be allowed to offer fiat-to-crypto onramps. Crypto users have been barred from using their digital assets as payments. Banks are excluded from the regulation and will be able to be used as lira on-ramps via wire transfer to exchanges.

UK Crypto Companies Face New Reporting Requirements

In March, the UK’s Financial Conduct Authority (FCA) added crypto companies to the list of firm types required to submit financial crimes reporting. The new policy nearly triples the number of firms required to report annually to the FCA and was characterized as a response to money-laundering threats.

Full policy: <https://www.fca.org.uk/publication/policy/ps21-4.pdf>

⁵ <https://news.bitcoin.com/turkey-crypto-regulation-central-bank-no-intention-to-ban-cryptocurrencies/>

Central Bank Digital Currencies (CBDCs)

Central Bank Digital Currency (CBDC) projects from all over the world are gaining traction. The Bank of Japan announced that they have officially launched their first proof of concept CBDC, with a targeted completion date of March 2022. They are currently undergoing technical feasibility testing around payments, distribution and other basic functions. Though their plans have been pushed out from their original timeframe of October 2021, and the bank states that they have no issuance plans as yet.

China's digital yuan or Digital Currency Electronic Payment (DCEP) continues to spark conversation amongst global leaders. US President Joe Biden stated that his administration would be keeping a close eye on the project, stressing the importance of understanding the impending political and economic implications. Even though some officials believe that a digital yuan could be used to topple the US dollar's dominance as the world's global reserve currency, the Biden administration's primary focus will be on understanding the DCEPs functions and uses. Galaxy Digital CEO Mike Novogratz forecasted an "existential crisis" if the US is unsuccessful in creating its own digital dollar. (add sentence on DCEP in context of Beijing's emerging sanctions regime and US strategic competitor)

United States Finds More Support for Digital Dollar

The United States continues to discuss the digital dollar but finds itself behind many countries around the world in the development of a central bank digital currency. At a March 2021 payments conference in Basel, Switzerland, Federal Reserve Chair Jerome Powell stated that "digital currencies would need to be integrated into existing payment systems alongside cash and other forms of money."

Though Powell's statement was taken as supportive of traditional finance by many banks harboring concerns about cryptocurrencies, Treasury Secretary Janet Yellen has been somewhat bullish on a digital dollar, remarking last month that a CBDC could help Americans lacking access to traditional financial systems. The Boston Fed and MIT are working in concert on a digital dollar project and hope to unveil a prototype in Q3 of 2021.

US Senator Sherrod Brown Says US Should Develop a CBDC

US Senator Sherrod Brown (D-OH), the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs, wrote a letter to the Federal Reserve Chair on how the United States should jump-start development on a CBDC or risk falling further behind China, the EU, and others. This is not the first time Senator Brown brought up the idea of token-based digital dollars. Last year, he introduced a bill to create a digital dollar and enable access to "FedAccounts" for every US resident.

Senator Brown also emphasized that, should the US move forward with a CBDC, it must protect consumer privacy and provide financial data security. Compliance with AML, CTF, and sanctions will be crucial to the successful deployment of CBDCs.

Jamaica's finance minister will pilot a CBDC in 2021

On March 9, Jamaica's Minister of Finance, Nigel Clarke, announced his plan to launch a central bank digital currency (CBDC) by 2022 in an annual National Budget Debate address before the national.

Russia plans to present digital ruble prototype before year's end

Russia's central bank is developing a digital ruble, but citizens and banks are not completely on board with making a full transition to the digital currency. The digital ruble would deploy tools like QR codes and contact-free interfaces. It would also be much easier to transfer to those who need essential services like welfare and child benefit payments, but there is concern that local banks will close if the digital ruble is more widely adopted.

UAE and Asian Countries Join Cross Border Payment Bridge

In a move to forge stronger economic ties between their nations, the United Arab Emirates, China, Hong Kong, and Thailand are working on building a payment bridge to make cross-border CBDC transactions more efficient. This development will be the second phase of the original Project Inthanon-LionRock CBDC, which started as a collaboration between the Hong Kong Monetary Authority and the Bank of Thailand in 2019. Usually, cross-border payments involve overcoming a lot of hurdles and can be very expensive; however, Forkast News reported that “[through] the m-CBDC Bridge project, the participating central banks say they hope to overcome those pain points and facilitate faster, more efficient and less costly cross-border fund transfers for international trade settlement and capital market transactions.” The initiative aims for the bridge to allow for real-time 24/7 payments and settlement.

South Korea Starts First Phase of its CBDC

On February 9, the central Bank of Korea (BoK) announced it will be testing a CBDC. A spokesperson said that the testing phase will occur within a controlled environment to ensure safety. The bank has also released a supplemental book that goes into detail about legal roadblocks that could impact a CBDC release. Bank officials predicted that issuing a CBDC would likely cause Korea's GDP to increase by 3%. Other positive results would be the elimination of printing needs and associated cash transfer fees and delays.

Beijing and Suzhou's Residents Receive Digital Yuan Airdrop for Next Phase of CBDC

China has continued to cement its lead in developing its central bank digital currency (CBDC), the digital yuan. On February 5, the cities of Beijing and Suzhou airdropped 10 million digital yuan (US\$1.55 million) and 30 million digital yuan (US\$5 million), respectively, to citizens as part of the next testing phase for China's CBDC. This rollout was as part of a Lunar New Year initiative that includes the distribution of red envelopes containing 200 yuan (US\$31) to citizens around those cities.

In order to receive the digital yuan, recipients had to download specific digital wallet apps to be put in a lottery with a Chinese ID number. The winners had a little over two weeks to spend the digital yuan at approved e-commerce and offline merchants.

Soon after the airdrop, however, Chinese police warned citizens to be aware of scammers trying to trick them into participating in CBDC-related scams. An example? The fraudulent "Central Bank's International Wallet," which told victims that they would be given access to a secret and government-run CBDC promotion fund, saying there was a chance of earning up to \$24,800. These criminals ended up stealing user data, which included names, phone numbers, and banking details.

India Makes Moves to Embrace CBDCs

After studying digital currencies back in 2018, the Reserve Bank of India (RBI) acknowledged interest in exploring a central bank digital currency (CBDC) in a booklet on payment systems published January 26. The bank created a department to study the “desirability” of a CBDC to see if it would reduce the cost of printing banknotes. In a booklet the bank published last week, RBI found that although digital payments are gaining popularity because of smartphones in metropolitan areas, the remote parts of India would need an offline option for digital payments. A pilot of an offline payments program will be underway through March of 2021.

IMF Says Only 40 Countries Have Clear Legal Pathway to CBDC Issuance

There have been many countries jumping on the CBDC bandwagon, but on January 14 the International Monetary Fund (IMF) reported that only 40 member-countries have legal structures in place allowing them to deploy CBDCs. According to the IMF blog, the group estimates that 80% of the world’s central banks are either not allowed to issue a digital currency under their existing laws, or the legal framework is not clear. In addition, the IMF said that if a country chooses to provide a digital currency, every citizen in that country should be given the ability to easily access it. The IMF reiterated that there remain many people around the globe who lack access to the devices needed to use digital currencies and reminded governments that they cannot force citizens to use CBDCs.

Turkey Moves Toward Establishing Central Bank Digital Currencies

Just as the new year began, Turkey announced a trial period of its CBDC, the digital lira, with plans for a pilot launch set for the second half of 2021. The Bank of International Settlements, an organization that amongst other functions tracks which countries are developing CBDCs, received no proposals from Turkey, making this development a surprise to them and to the international community.

Ukraine Hires Stellar Development Foundation to Build its CBDC

On January 4, Ukraine took an important step toward developing its CBDC by hiring the Stellar Development Foundation to build it. The country's National Bank announced in 2017 that they were starting to think about creating a digital currency and even spoke with other countries about what precautions to take and other important details to consider. Ukraine's Digital Transformation and IT Deputy Minister Oleksandr Bornyakov is very hopeful that the partnership with Stellar will improve the country's standing in the global digital economy.

Sanctioned Countries

North Korea

Hackers Charged for Stealing Over \$100 Million from Crypto Firms

On February 17, the DOJ charged three North Korean computer programmers with participating in a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than \$1.3 billion of money and cryptocurrency from financial institutions and companies between 2017 and 2020.

According to Assistant Attorney General John Demers, the three North Korean actors charged were the world's leading bank robbers, stealing upwards of \$100 million from a number of different crypto merchants. The three men were allegedly tied to the Lazarus Group, a notorious cybercrime ring accused of stealing over \$1.3 billion as a part of a broader financial conspiracy that included the hack on Sony Pictures Entertainment in 2014. Following the indictment, the FBI, Cybersecurity and Infrastructure Security Agency (CISA) and Department of Treasury published a joint advisory about crypto malware produced by North Korea called AppleJeus.

Russia

US President Joe Biden Declares Russian Cyberattacks a National Emergency

On April 14th, President Biden ordered an expansion of sanctions against the Russian state for meddling in the 2020 election. In response, OFAC added 28 cryptocurrency addresses to its sanctions list.

The sanctions list includes Russian officials, proxies, and intelligence agencies linked to the Internet Research Agency (IRA)—a Russian “troll farm” known to use crypto to fund influence operations around the world on behalf of Russian political interests. Many of

these sanctioned addresses are attributed to deposit addresses at regulated exchanges, including two popular off-shore exchanges and one US-based exchange.

Read our full analysis: <https://ciphertrace.com/sanctions-alert-russian-crypto-related-designations-for-us-election-interference/>

Russian Anti-Money Laundering Body to Monitor Crypto-to-Fiat Transactions

During a March 23 meeting of the State Duma Committee on the Financial Market, Deputy Head of Russia's Federal Financial Monitoring Service (Rosfinmonitoring) Herman Neglyad announced that the AML body has begun monitoring crypto-to-fiat transactions. Based on Neglyad's statements, it appears Rosfinmonitoring is collecting data from Russian banks, which are monitoring for transactions to and from virtual asset service providers (VASPs) and reporting these transactions to the Federal Financial Monitoring Service.

As more mainstream consumer and institutional investors embrace cryptocurrencies, it becomes increasingly difficult, if not impossible, for traditional financial institutions to avoid entanglements with the crypto economy. As such, it's important for banks to understand how best to detect and monitor transactions to and from VASPs. CipherTrace research has found that a typical name-based monitoring system may entirely miss up to 70% or more of the crypto exchanges out there, and up to 90% of the actual transaction volume.

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, VP of Financial Investigations

Dave Jevans, Chief Executive Officer

Editor-in-Chief

John Jefferies, Chief Financial Analyst

Lead Analysts

Julio Barragan, Director of Cryptocurrency Intelligence

Jonelle Still, Cryptocurrency Forensics Analyst