CIPHERTRACE

Cryptocurrency Crime and Anti-Money Laundering Report

CipherTrace
Cryptocurrency Intelligence
August 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

© Copyright 2021 CipherTrace. All rights reserved

© Copyright 2021 CipherTrace. All rights reserved

Highlights

- By the end of July 2021, major crypto thefts, hacks, and frauds totaled $681 million

- At $361 million, DeFi-related hacks make up 76% of major hack volume in 2021

- By the end of July 2021, DeFi hacks have already increased more than 2.8X from 2020

- At $113 million, DeFi-related fraud makes up 53% of major fraud volume in 2021

- By the end of July 2021, DeFi fraud have already increased more than 2.7X from 2020

- Ransomware actors demand highest ever reported ransom—$70 million— for universal decryption keys as the US Government sets its sights on combating ransomware the same way it combats terrorism

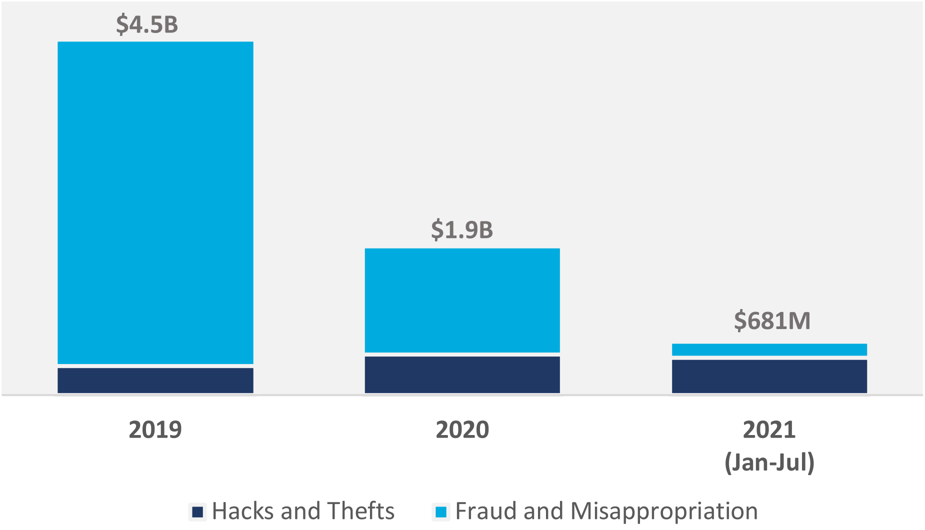
- Regulators set to accelerate the implementation of the Travel Rule as global financial crime watchdog the Financial Action Task Force (FATF) declares that no jurisdictions reported being aware of any virtual asset service providers that fully complied with all elements of the Travel Rule.

- The US State Department is offering bounties up to $10 million for information leading to the identification or location of ransomware actors that attack critical US infrastructure.

Executive Summary

By the end of July 2021, major crypto thefts, hacks, and frauds totaled $681 million. While this number continues to be dwarfed by previous years' highs, a breakdown of the types of thefts and fraud confirms a trend observed at the beginning of last quarter—DeFi-related crimes continue to grow quarter over quarter, with Q2 2021 netting criminals new highs in DeFi-related proceeds.

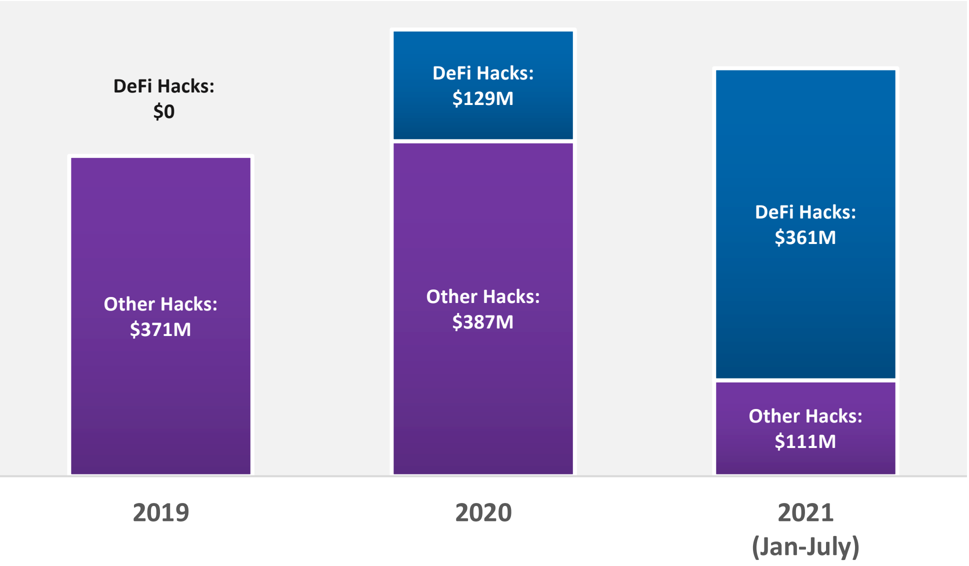
Cryptocurrency Fraud Dips as DeFi Hacks Continue to Grow



Source: CipherTrace Cryptocurrency Intelligence

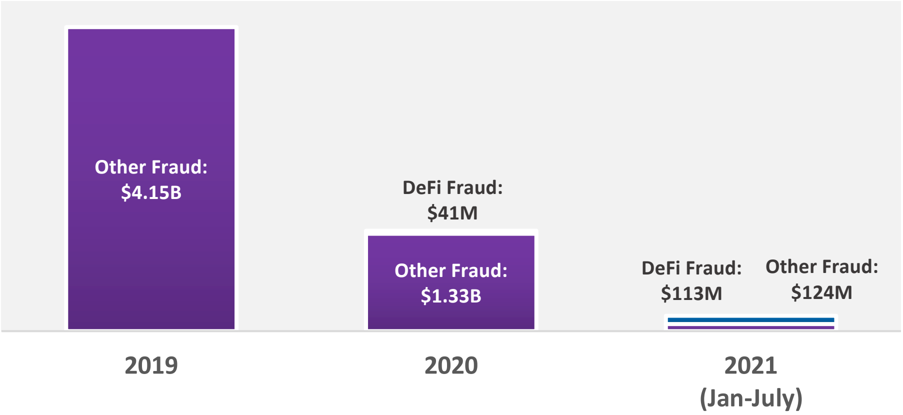
When breaking down crypto crimes by those DeFi and non-DeFi related, a clean pattern emerges. By July 2021, DeFi-related hacks total $361 million, already making up three-quarters of the total hack volume this year—a 2.7x increase from 2020. DeFi-related fraud continues to rise, as well. At the time of this report, DeFi-related fraud accounted for 54% of major crypto fraud volume, whereas last year DeFi-related fraud only made up 3% of the year's total.

DeFi related hacks already make up 76% of major hacks in 2021



Source: CipherTrace Cryptocurrency Intelligence

Overall Cryptocurrency Fraud Decreased as DeFi-related Fraud Triples



Source: CipherTrace Cryptocurrency Intelligence

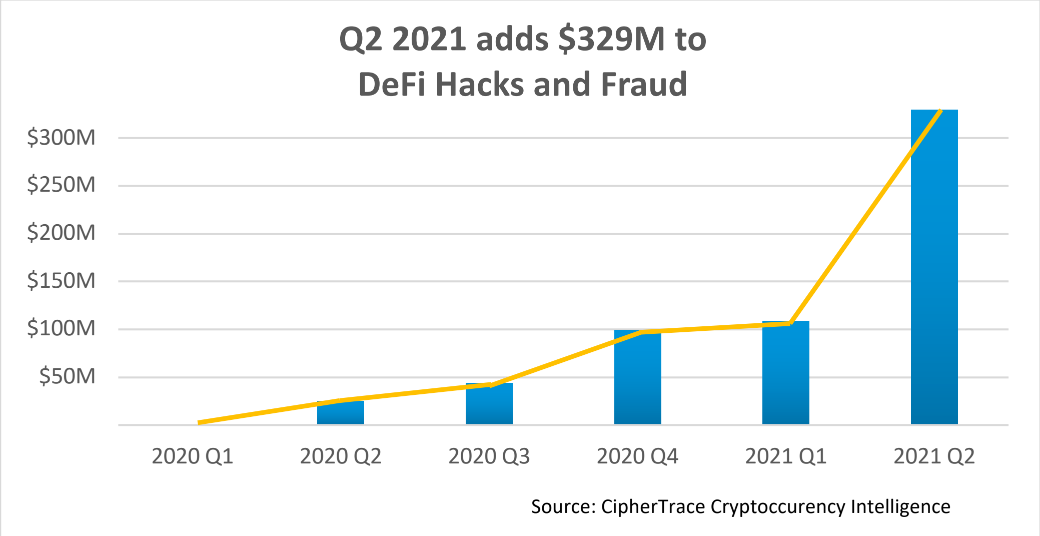
The proliferation and escalation of ransomware targeting critical infrastructure marks another disturbing trend in 2021. In July, REvil ransomware actors demanded $70 million—the highest ever reported ransom— for universal decryption keys as the US Government set its sights on combating ransomware the same way it combats terrorism globally.

© Copyright 2021 CipherTrace. All rights reserved

On the regulatory front, the world is set to accelerate the implementation of the cryptocurrency "Travel Rule" as the global financial crime watchdog the Financial Action Task Force (FATF) declares that no jurisdictions reported being aware of any virtual asset service providers (VASPs) that are fully compliant with the Travel Rule. The lack of Travel Rule implementation globally is a major obstacle to effective global AML/CFT mitigation. As such, the FATF has indicated that one of its major next steps will be to accelerate the implementation of the Travel Rule across the world. This move comes as some countries, such as Canada, have postponed Travel Rule enforcement as VASPs continue to examine possible solutions.

DeFi-Related Crime Continues to Define Major Hacks and Fraud in 2021

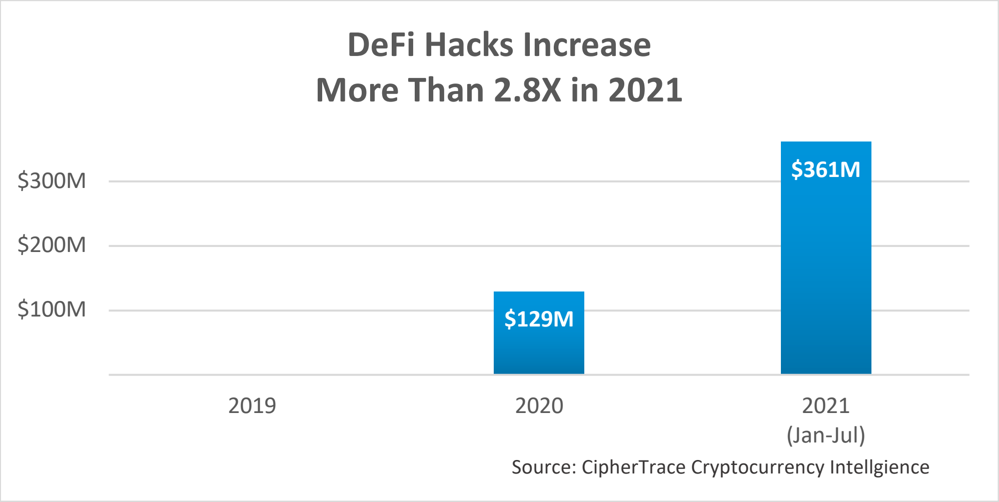
The end of Q2 2021 brought on an additional $329 million in DeFi-related hacks and fraud. With the addition of $35.6 million from the first month of Q3, 2021's year-to-date total is now nearly $474 million at the time of this report. These DeFi crimes can generally be broken down into two categories: either a hack of a DeFi protocol by outside agents, or a rugpull conducted by insiders. A majority of the DeFi volume netted by criminals in 2021 appears to have been conducted by outside agents as DeFi-related hacks make up $361 million—76% of all DeFi-related crime at the time of this report. The remaining 24% are rugpulls tallying over $113 million year-to-date.



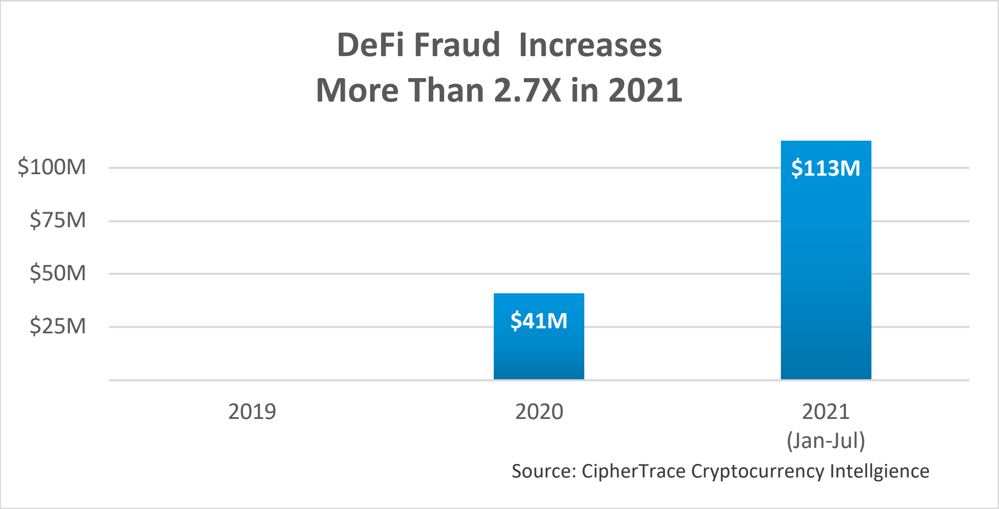
Source: CipherTrace Cryptoccurency Intelligence

While DeFi-related hacks triple fraud by volume, a look at both by quarter shows consistent—nearly identical—growth from the year prior. Both hack and fraud volumes have increased 2.7-2.8x their 2020 volume as DeFi's explosive growth over the last year continues to attract more than just new investors.

© Copyright 2021 CipherTrace. All rights reserved



Source: CipherTrace Cryptocurrency Intellgience



Source: CipherTrace Cryptocurrency Intellgience

Notable DeFi hacks and rugpulls this year are listed below. Additional coverage on DeFi-related crimes that have occurred since our last Report can be found in the *Major Scams, Thefts, and Fraud* section of this report.

Another common trend found in analyzing DeFi hacks are the use of flash loans, which have been used in a majority of DeFi protocol attacks in the past year. Because flash loans require no collateral or KYC, it is increasingly difficult to catch bad actors using them to fund their attacks. However, the crux of the problem lies not in platforms giving out the flash loans, but the unaudited smart contracts the loans are sent to and that are later exploited.

30 Confirmed DeFi Attacks in 2021 January - July

1.	2021 Q1	TurtleDex (Ape Swap and Pancake Swap)
2.	2021 Q1	Roll (WHALE, RARE and PICA)
3.	2021 Q1	DODO DEX
4.	2021 Q1	PAID Network
5.	2021 Q1	Meerkat
6.	2021 Q1	Furucombo (iouCOMBO)
7.	2021 Q1	CREAM Finance + Alpha Finance (Alpha Homora)
8.	2021 Q1	Year.Finance
9.	2021 Q2	EasyFi
10.	2021 Q2	Uranium Finance
11.	2021 Q2	Eleven.Finance
12.	2021 Q2	Alchemix
13.	2021 Q2	StableMagnet
14.	2021 Q2	Bogged Finance
15.	2021 Q2	Belt Finance
16.	2021 Q2	Rari Capital
17.	2021 Q2	Value.DeFi
18.	2021 Q2	Value. Defi
19.	2021 Q2	bEarn
20.	2021 Q2	Xtoken
21.	2021 Q2	Pancake Bunny
22.	2021 Q2	Spartan Protocol
23.	2021 Q2	WhaleFarm
24.	2021 Q2	Burger Swap
25.	2021 Q3	Chainswap
26.	2021 Q3	Chainswap
27.	2021 Q3	ThorChain
28.	2021 Q3	ThorChain
29.	2021 Q3	AnySwap
30.	2021 Q3	Bondly

Ransom Where? US Doubles Down on Finding Ransomware Actors as Demands Hit New Highs and Attacks Hit New Lows

The Kaseya hack and ransom in July 2021 marked the third large-scale attack carried out by a Russian-speaking ransomware-as-a-service (RaaS) operation REvil within the past three months. The scale and frequency of the attacks have highlighted a major security issue in American infrastructure and have drawn urgent attention from the highest levels of the US government. On June 3 the Justice Department announced it now views ransomware attacks in the same way it sees critical threats to national security such as terrorism. A few weeks later, the US State Department began offering bounties up to $10 million for information leading to the identification or location of ransomware actors that attack critical US infrastructure.

As a result of this newfound government attention on ransomware, RaaS operator REvil announced on hacker forums that it had updated its expected behavior for ransomware affiliates, deeming targets such as schools and hospitals off-limits for attacks. This updated guidance was most likely an effort to lower the REvil profile so as not to become a priority target for US DOJ. These efforts were unsuccessful as a few weeks later REvil operators were credited with one of the largest ransomware attacks to date, initially demanding a $70 million payment for a universal decryption key.

Blockchain analytics provides critical cryptocurrency intelligence needed to trace ransomware actors. Only by working together through groups like the Ransomware Task Force can cryptocurrency intelligence firms counter these transnational threat actors. It is crucial to not only trace ransomware proceeds to find and stop the operators, but also to harden systems and educate the public on how these compromises occur in order to properly mitigate disruption.

© Copyright 2021 CipherTrace. All rights reserved

Incident Response Firms have vast databases of ransom payments from their clients; identifying and tracking these funds can aid in building a full profile of the ransomware group.

Because ransomware actors use public blockchains for receiving payments, all transactions can be viewed on the chain, enabling law enforcement (or anyone) to trace the flow of funds. Utilizing a blockchain analytics tool like CipherTrace Inspector provides additional intelligence to the trace and investigation, such as identifying when the funds have been deposited into an exchange, identify choke points, and tie bitcoin addresses to real world people and locations.

REvil Demands $70M in Bitcoin in Kaseya Hack—Largest Ransom Ever Recorded

On July 2 Russian ransomware group REvil targeted over 200 US companies, infecting over a million machines in the process, and demanded $70 million for a universal decryption key—the largest ransomware demand ever recorded. It is believed that this attack was carried out by successfully infecting Australian software supplier Kaseya's network management systems and then spreading the malware through the cloud.

In response to the attack, US President Joe Biden urged Russian leader Vladimir Putin to "take action to disrupt ransomware groups operating in Russia." Four days after their call, on July 13, the REvil darknet site went down and has yet to resurface at the time of this report.

Nearly three weeks after the attack, on July 22, Kaseya finally obtained the universal decryption key and began working to help customers affected by the ransomware. The company claims to have received the key through a "trusted third-party" and denies paying the ransom.

© Copyright 2021 CipherTrace. All rights reserved

Colonial Pipeline Ransomware Attack

On May 7, 2021, Russia-based cybercrime group DarkSide attacked the Colonial Pipeline—part of the critical infrastructure sector of the United States. As part of the attack, DarkSide actors encrypted devices on the network and stole unencrypted files, threatening to release them to the public if the company failed to pay. According to blockchain analysis, the next day Colonial Pipeline paid the 75 BTC ransom, worth more than $4.2 million at the time. Following the attack, the White House issued an executive order on improving US cybersecurity against "persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."

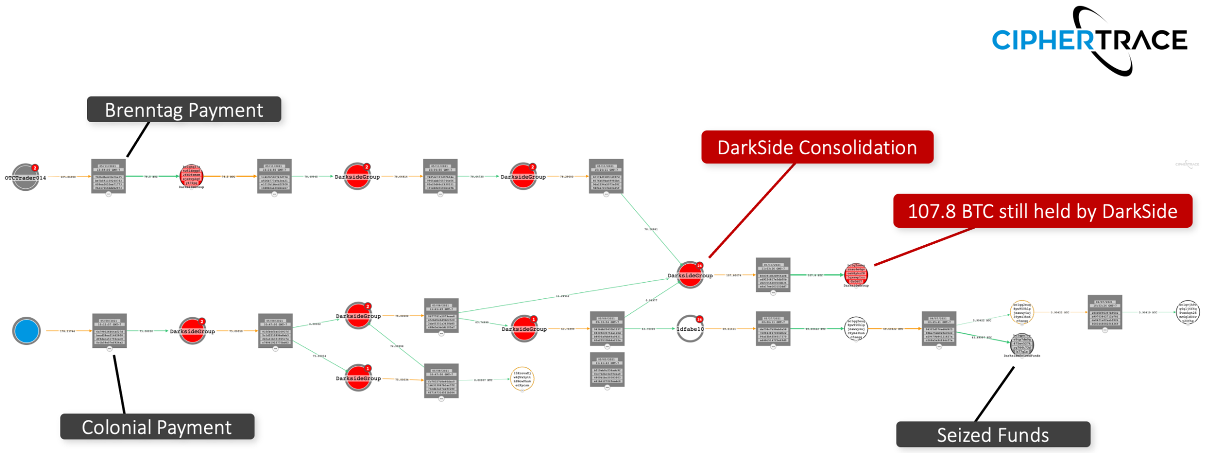
This attack crippled the eastern seaboard as the Colonial Pipeline carries gasoline and jet fuel necessary to operations in the Southeastern United States. The operational technology systems were not affected by the ransomware; rather it was the billing system that was compromised. According to CNN reporting from sources inside the company, the inability to know how much to bill customers for fuel they received was the reason for halting the pipeline operation. Colonial Pipeline claimed to have halted all of the pipeline's operations to contain the attack.

Colonial Pipeline Ransomware Recovery

On June 7, 2021, the US Department of Justice announced that they had seized 63.69 BTC of the 75 BTC ransom Colonial Pipeline had paid to DarkSide. This ransom recovery is the first undertaken by the recently created DOJ Ransomware and Digital Extortion Task Force.

While the FBI was able to recover about 85% of the bitcoin paid to DarkSide, this only accounts for roughly half of the USD equivalent initially paid due to a fall in the price of bitcoin since the ransom payment. The remaining 11.3 BTC remained in a different DarkSide or DarkSide affiliate-controlled address, as shown in the graphic below.

Based on an analysis of the flow of funds and DarkSide's operation as a Ransomware-as-a-Service (RaaS) model, the unseized funds could be held by DarkSide operators while the funds seized were those held by the RaaS affiliates that conducted the hack. It is common practice for ransomware operators to take a 15-30% cut of the ransom, leaving the RaaS affiliates (those that conduct the attack) with the remainder.



Source: CipherTrace Cryptocurrency Intelligence

The 63.69 BTC funds recovered appear to have been seized via direct access to the ransomware actor's wallet, as indicated in the seizure warrant by referencing FBI's control of the private key, and not through an Exchange which is more typical of asset recovery.

The Darkside operators consolidated the remainder of the Colonial Pipeline funds with multiple other ransom payments, including with that of global chemical distribution company Brenntag, which had been attacked just days earlier. This consolidation of 107.8 BTC of DarkSide funds have not been seized by the DOJ as of this writing, and have been dormant since May 13.

According to the DarkSide Seizure Warrant, the Cyber Crimes Squad of the FBI's San Francisco Field Division used blockchain analysis to determine the Colonial Pipeline ransom payment funds flow. In this warrant, the FBI also announced that they were in possession of the private key for the cryptocurrency address linked to 63.7 BTC directly traceable to the Colonial Pipeline ransom payment. These private keys were likely obtained as a result of the seizure of DarkSide servers on or around May 13, as reported by messages sent to affiliates of the DarkSide RaaS operation.

The seizure of cryptocurrency by direct, physical access to the wallet is not common. In order to seize crypto, law enforcement must have access to the private key, or have access to an individual who can access the private key. This is why most crypto is seized either via an exchange, since exchanges hold the private keys, or after an arrest of an individual that has a wallet on them or among their belongings.

Ransomware Attack on Chemical Distribution Company Brenntag

Four days after the Colonial Pipeline attack, global chemical distribution company Brenntag suffered a ransomware attack that targeted their North America division. On May 11 the company paid 78.5 BTC, worth roughly $4.4 million at the time, to the ransomware operators. Similar to the Colonial Pipeline attack, as part of this attack, DarkSide actors encrypted devices on the network and stole unencrypted files. However, unlike Colonial Pipeline, Brenntag funds have not yet been recovered at the time of this report.

Ransomware Attack on Largest Global Meat Supplier JBS

JBS, the world's largest meat supplier, was the victim of a May 30 cyber-attack on its North American and Australian IT systems, resulting in shutdowns at the five biggest beef plants in the US responsible for 20 percent of America's meat processing capacity. JBS paid the $11 million ransom in bitcoin on June 1. The next day JBS resumed operations and the FBI officially attributed the JBS attack to REvil.

© Copyright 2021 CipherTrace. All rights reserved

Ireland's Health Services Recover from Severe Ransomware Attack

After being the target of what some officials are calling the most significant cyber-attack in Irish history on May 14, Ireland's Health Service Executive (HSE) revealed that the hacker has demanded a $20 million ransom in order to decrypt the network. Ireland's Prime Minister Michael Martin ruled out any form of payment to the perpetrators, stating, "We're very clear we will not be paying any ransom or engaging in any of that sort of stuff." Instead, they began working with the National Cyber Security Centre (NCSC) to attempt to recover the data.

In order to protect against further damage, the HSE immediately shut down their computer systems. The impact of the shutdown varied across the country with many services delayed, such as COVID-19 test results and x-rays.

The attack has been attributed to the Conti, a ransomware-as-a-service (RaaS) group known for attacking critical infrastructure related to hospitals, 911 dispatch carriers, emergency medical services and law enforcement agencies. A week after refusing to pay, the Conti group offered the decryption keys for free so the HSE could continue critical operations but claimed on their darknet site that they would still sell or publish the stolen data if the ransom demands were not met. Health Minister Stephen Donnell responded to the threats by stating no ransom has or will ever be paid by the Irish government.

Rewards for Justice – Reward Offer for Information on Foreign Malicious Cyber Activity Against US Critical Infrastructure

The U.S. State Department announced its Rewards for Justice program on July 15, offering bounties up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, participates in ransomware attacks against critical U.S. infrastructure.

Major Thefts, Scams, and Frauds

Brothers Behind Crypto Platform Africrypt Purportedly Disappear with $3.6 Billion in Bitcoin

Ameer and Raees Cajee, two South African natives and founders of bitcoin-based company Africrypt, have gone missing along with an alleged 69,000 bitcoin (worth roughly $3.6 billion dollars at the time of their disappearance). CipherTrace has been unable to verify this total and believe the true amount taken to be an order of magnitude less. As such, we have not included Africrypt in our year-to-date total for cryptocurrency scams.

Issues first came to light when investors requested a law firm investigate an alleged hack in April. After the investigation was complete, then-CEO Ameer Cajee instructed the investigating firm to keep the info gained from the authorities. Shortly after, Africrypt employees and developers lost access to the back end of the platform. A lawyer for the two brothers has since told the BBC that they categorically deny any involvement in a "heist".

CipherTrace is currently investigating the report. More updates to follow.

TITAN Collapse After Crypto Bank Run

On June 16, 2021, Iron.Finance suffered an incident that resulted in TITAN, the governance token that backs the stablecoin IRON, crashing nearly 100% in what is being called “the world’s first large-scale crypto bank run.” As a result of TITAN’s crash, the price of the IRON stablecoin moved off peg.

This incident was the result of a design flaw—Iron.Finance lacked a proper stabilizing mechanism. Without an adequate mechanism in place, when the TITAN token started collapsing the prices provided by the Price Feed Oracle were delayed and the gap between these prices and real-time data made arbitraging unprofitable. Because Iron.Finance had relied on arbitrage users to help stabilize the price of IRON, when arbitrage was no longer profitable the issue compounded. TITAN has an infinite supply and is only supposed to be used as collateral when minting IRON. Any user in the system can issue IRON which is backed by their USDC and TITAN holdings.

As crypto markets are quite volatile, it is not uncommon for a stablecoin to lose its peg. However, due to this possibility, every stablecoin needs a mechanism of protection for such fluctuations. In IRON's sense, their only mechanism was assuming that arbitrage users would buy cheap IRON from the market when the price dips and thus redeem it for USDC+TITAN and then sell TITAN for profit.

On the day of the attack the stabilization was working as intended until the price of TITAN started dropping and eventually reached zero. At this same time IRON lost its peg and dropped to around ~$0.94, which is a massive drop for a stablecoin. In order to protect further features, Iron.Finance had to pause both minting and redeeming. In a recent report that dives into the details of TITAN and the use of arbitrage, it describes that the delay (10min. Time Weighted Average Price) from the Price Feed Oracle for TITAN, caused the prices to be higher than those on an AMM (real time automated market maker) as it couldn't keep up. Thus, the price gap caused arbitraging to become unprofitable, and thus could not protect the stabilization.

Iron.Finance published a post-mortem on the incident, which failed to mention the lack of a stabilizing mechanism. The DeFi bank run resulted in Iron.Finance losing more than $2 billion in the total value locked (TVL) in the protocol, dropping from $2.18 billion locked to less than $10.5 million.

For future developments for similar systems, there are a variety of scenarios to take into account when properly testing your environment around price fluctuations, loss of peg, and tightening the time frame between oracles or other mechanisms for determining prices.

Scammers Find New Ways to Steal Crypto

Hackers are getting more and more creative, and scams are getting harder to identify. Some may be easier to spot but still have massive amounts of cryptocurrency sent their way. During Elon Musk's Saturday Night Live appearance, scammers used his image and name to gain over $100k worth of bitcoin, Ethereum, and Dogecoin.

New malware downloads are appearing in gaming apps like Steam and Discord, waiting to steal anything related to crypto. Authorities also found a new cryptocurrency hunting malware program that has been going around the dark web being labeled as the best way to make money in 2021, alarming crypto enthusiasts as it seems to be an advanced version of an already exposed software. The scams are coming out of the virtual world too, with FBI agents marking bitcoin ATMs in Ohio with warning markers as the kiosks are often used to send funds quickly and by non-crypto users.

THORChain Loses $13M Attack in Two Attacks

In July THORChain, a cross-chain decentralized exchange, was attacked by cyber criminals who made off with roughly $8 million in various cryptocurrencies. THORChain developers announced in their official telegram that admins had the funds needed to cover the assets stolen from users but would rather solve the issue by paying the hacker a bug bounty in exchange for the funds return. After telling users that their funds would be available after the issue has been resolved, they took to Twitter to release their roadmap for recovery of the funds. Starting with patching up the vulnerability and restarting the network, Ether will then be donated to liquidity provider pools to reimburse impacted users. The developers have also promised to contact third-party blockchain security firms to audit their network.

© Copyright 2021 CipherTrace. All rights reserved

This was THORChain's second attack in a month, with hackers previously making off with roughly $5 million in user funds due to a bug in the recently updated THORChain Bifrost bridge code.

ChainSwap Attacked for the Second Time this Month

On July 11, ChainSwap's smart code was exploited by an attacker once again, resulting in $4.4M USD in potential losses for investors. The attacker took control of the platform's smart contracts and was able to mint various tokens directly to their wallet before exchanging them on PancakeSwap. The attack was noticed by a developer of one of the projects that were impacted, Wilder World, which lost 20 million WILD tokens. Other exploited tokens included Antimatter, Optionroom, Umbrellabank, Nord, Razor, Peri, Unido, Oro, Vortex, Blank, and Unifarm. ChainSwap responded by pulling liquidity and announcing an investigation while assuring investors that funds were safe.

DeFi Protocol Rari Capital Loses $10 Million in Hack

On May 8, an "evil contract" exploit in the Rari Capital ETH Pool associated with the protocol's new Alpha Homora integration led to the theft of $10 million in assets. In an "evil contract" exploit, an attacker is able to trick a smart contract into thinking its "evil contract" has the proper access or permissions.

In the case of the Rari Capital hack, the exploit caused the HomoraBank contract to make the incorrect assumption that the hacker was setting up an ibETH pool on the platform. The attacker used flash loan ETH from dYdX to repeatedly fund deposits into the pool, artificially inflate the value, and withdraw more ETH than what was initially deposited due to the inflation. While Rari's integration of Alpha was audited by Quantstamp, the exploit was not previously detected.

Following the hack, all of Rari's contributors voted to return about 2 million Rari Governance Token (RGT) that had initially been slated for developer incentives to reimburse users impacted by the hack.

PancakeBunny Suffers $45M Attack

On May 19, the PancakeBunny protocol faced a flash loan exploit that drained $45 million worth of crypto assets. 8 flash loans were used to manipulate the price on various PancakeSwap pools, resulting in the minting of 697,000 BUNNY tokens. The immediate sale of these tokens caused the price of BUNNY to drop from $146 to $6.

Defi Protocol BurgerSwap Loses $7.2 Million in Hack

On May 28, DeFi protocol BurgerSwap suffered a flash loan attack that drained $7.2 million worth of cryptocurrency in fourteen transactions, according to the protocol's post mortem. The attacker was able to execute a code that manipulated the reserve supply of trading pairs between fake tokens and $BURGER, causing the price of $BURGER to increase drastically. The attacker capitalized on the price difference through fourteen flash loans, netting $7.2 million in various tokens.

WhaleFarm Rugpulls with $2.3M, Deletes Social Media Accounts

On June 20, DeFi project WhaleFarm and its team of anonymous developers successfully stole $2.3 million from investors who were chasing outrageous returns. WhaleFarm promised over 7,000,000% APY on cryptocurrencies like BTC, BNB, ETH, ADA, DOT, LINK, and stablecoins. After running for just a few days, the developers disappeared with the funds and the project's native token plummeted, losing 99% of its value.

Since the official Twitter and Telegram accounts associated with WhaleFarm were deleted shortly after the incident, this event has all the signs of a classic rug pull. Many projects that ended up being a scam exhibited the same promises of insane and unrealistic APYs and anonymous teams - two major warning signs crypto users should keep an eye out for. Crypto users should also be wary of any influencer’s true intentions when promoting a cryptocurrency.

© Copyright 2021 CipherTrace. All rights reserved

Enforcement Actions

Crypto criminals are finding that the law is catching up with them. Many enforcement actions seen this year are from crimes that have occurred years ago when bitcoin had yet to be a household name. Cases like these set the precedents for punishment in what was once a novel, and largely unregulated, economic ecosystem.

Swedish Man Receives 15 Years in Prison, Must Pay $16 Million in Restitution

In July, Roger Nils-Jonas Karlsson, who successfully stole over $16 million in bitcoin and other payment methods from 2011-2019, was sentenced to 15 years in prison for wire fraud, securities fraud, and money laundering charges. Karlsson ran an investment fraud scheme called Eastern Metal Securities and promised investors "astronomical returns" but instead used the money to purchase real estate and other luxury items. In addition to the 15-year prison sentence, Karlsson was also ordered to forfeit a luxury Thai resort he bought with the stolen funds and pay impacted investors $16,263,820 in restitution according to the US DOJ.

Members of Brazil's Bitcoin Banco Group Arrested for Alleged Embezzlement

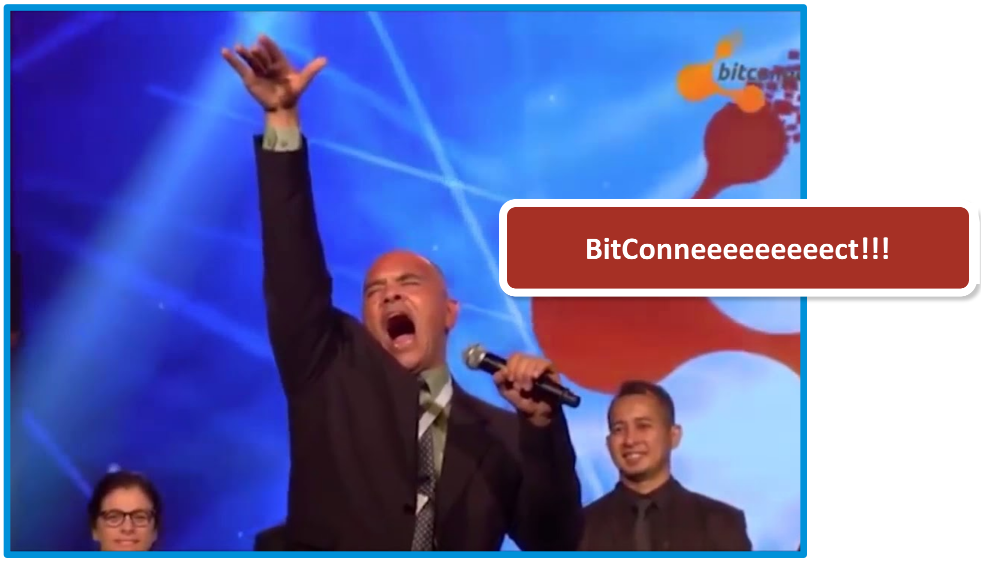
In July, Brazilian Federal Police arrested self-proclaimed "Bitcoin King" Claudio Oliveira for his role as head of "the Bitcoin Bank" where he and his group of employees worked together to steal $300 million from thousands of investors. Investigators had been looking into the case as a part of a massive three-year mission to uncover investment and embezzlement schemes, with over 90 officers involved in what was named Operation Daemon.

Oliveira reported a hack on the Bitcoin Bank back in 2019 but, according to police investigations, there was no hack—Oliveira and team had withdrawn the cryptocurrencies themselves.

SEC Sues Five BitConnect Promoters Over $2 Billion Scheme

On May 29, the Securities and Exchange Commission filed a civil lawsuit in the federal court in Manhattan against five promoters of the virtual asset BitConnect. The lawsuit alleges that the five failed to register themselves as brokers—as required by law—before promoting the sale of unregistered securities that raised over $2 billion from retail investors.

BitConnect was most notorious for the Ponzi scheme linked to an exchange that operated from 2016 through 2018 under the same name. The BitConnect platform eventually shut down when securities regulators in Texas and North Carolina ordered the platform to stop its sales after failing to register to sell securities in their states. As concerns over its similarities to a Ponzi scheme grew, many investors lost faith in the platform and the BitConnect token price crashed.



Infamous Bitconnect Promoter Carlos Mantos

© Copyright 2021 CipherTrace. All rights reserved

This is not the first time the SEC has charged virtual currency promoters for defrauding retail investors. Those looking to promote virtual currencies should proceed with caution as such actions may constitute a sale of a security. The fact that BitConnect was defunct for over three years before the SEC filed this lawsuit shows their willingness to pursue violations of the Securities Act, no matter when they were conducted.

Poloniex Faces Action from Canadian Regulators

Crypto exchange Poloniex is facing enforcement action from the Ontario Securities Commission. The move by the OSC signals the start of a more stringent era in Canadian cryptocurrency regulation, with Poloniex held to higher standards because of the crypto custody services it provides.

The Ontario Securities Commission stated, "Investors do not have possession or control of crypto assets deposited or traded on the Poloniex Platform. Rather, they see a crypto asset balance displayed in their account on the Poloniex Platform. In order to take possession of crypto assets reflected in their Poloniex account balance, an investor must request a withdrawal and is dependent on Poloniex. While Poloniex purports to facilitate trading of the crypto assets in its investors' accounts, in practice, Poloniex only provides its investors with instruments or contracts involving crypto assets. These instruments or contracts constitute securities and derivatives."

The OSC notified crypto exchanges in March that they needed to take steps to meet regulatory requirements and to contact the body for advice on getting in compliance. Poloniex allegedly did not take the first step of getting in touch and is facing expulsion from Canada.

EtherDelta Hacker Potentially Faces 47 Years in Prison Over $1.4 Million Hack

On May 20, US authorities issued a statement asking victims who were impacted by EtherDelta's 2017 hack for more information regarding the incident. EtherDelta has been no stranger to investigations, with founder Zachary Coburn charged by the SEC with running an unregistered national securities exchange in 2018, just a year after the hack. The hacker is allegedly named Tyler Nashatka and was indicted by a federal grand jury in 2019. He is believed to have launched various phishing attacks allowing him to get away with $1.4M in a matter of weeks.

China Arrests over 1,100 Suspects in Crackdown on Crypto-Related Money Laundering

In June, police in China arrested over 1,100 people suspected of using cryptocurrencies to launder illegal proceeds from telephone and Internet scams in a recent crackdown, according to the Ministry of Public Security.

Terrorism Financing and Cryptocurrency

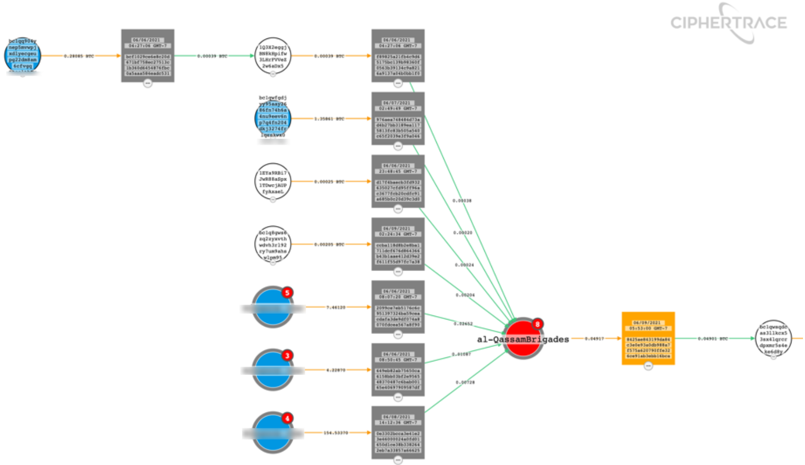
Israeli Government Orders Seizure of Several Cryptocurrency Wallets Linked to Designated Terrorist Organization Hamas

On July 1, Israel's National Bureau for Counter Terror Financing (NBCTF) released a seizure order listing several cryptocurrency addresses across several blockchains associated with donation campaigns carried out by designated terrorist organization Hamas. In addition to bitcoin and Ethereum, the seizure order demonstrates that Hamas also collected donations in Tether, TRON, Cardano, XRP, and DOGE, indicating their attempts to break out from reliance on bitcoin after the US Department of Justice announced the seizure of $2 million in cryptocurrency from prominent terrorist groups, including al-Qaeda, ISIS, and Hamas in August 2020 (*as reported in our 2020 Year End Cryptocurrency Crime and Anti-Money Laundering Report: https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/#terr*).

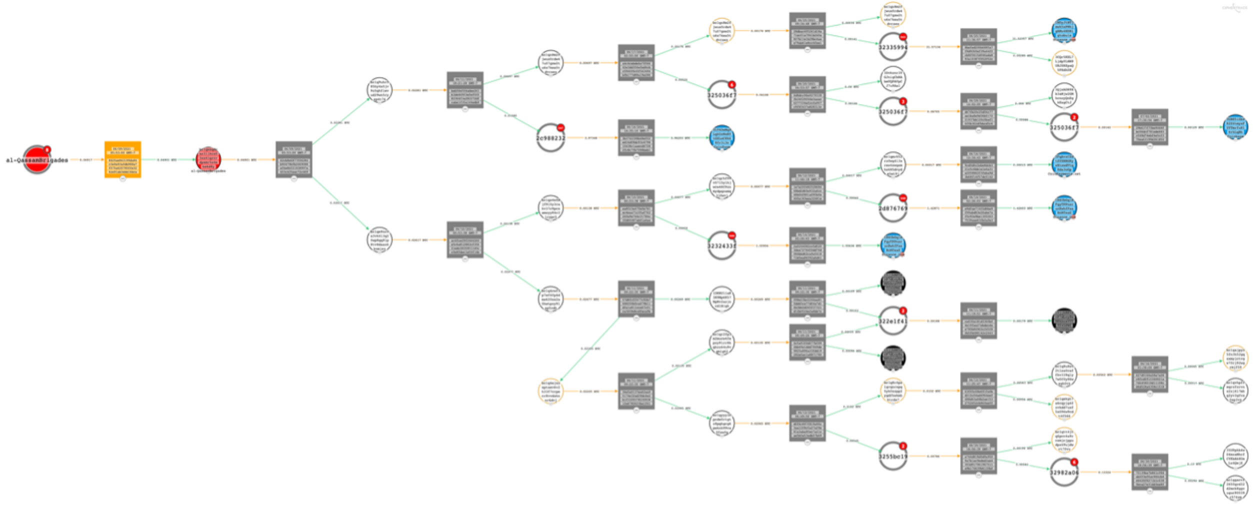
This action comes on the heels of the armed conflict between Israel and Gaza in May of this year which resulted in an uptick in reported cryptocurrency donations to Hamas. This is the first terrorism financing-related cryptocurrency seizure in Israel and highlights the importance of blockchain analysis in tracing the flow of funds to identify bad actors and counter terrorism financing.

CipherTrace analysts identified further movement of funds belonging to al Qassam Brigades—the military wing of Hamas and OFAC-sanctioned entity—that have not been previously analyzed and not yet seized by the NBCTF.

It appears that al Qassam Brigades [Hamas] withdrew some donation funds from their accounts at a large, global exchange between June 6 – 9, consolidated and redistributed a portion of those funds back into new deposit addresses, likely linked to new accounts, at the same global exchange. One plausible explanation for this transfer pattern is to attempt to avoid additional governmental scrutiny and or further seizure of their funds.

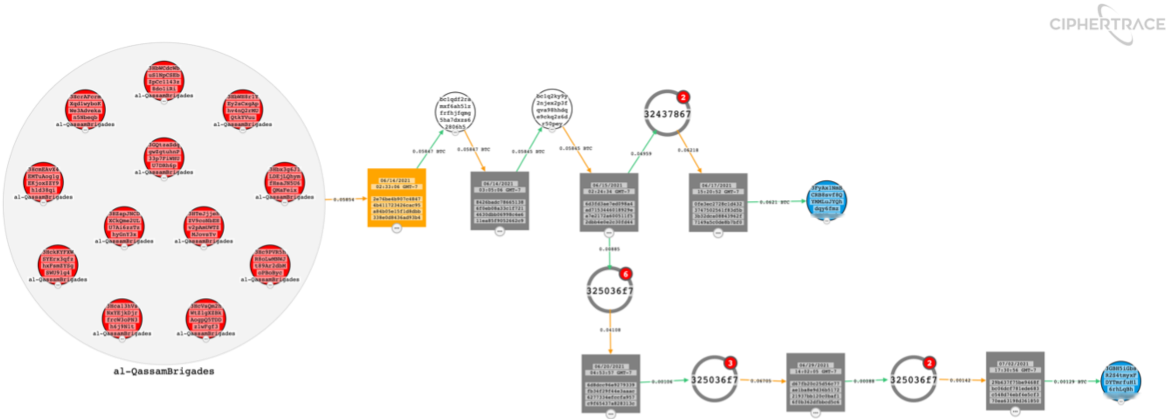


June 6 – 9 withdrawals from exchanges moved into a private wallets belonging to Hamas



Funds redistributed into exchanges, private addresses, and dark markets

Further analyses on additional Hamas clusters find that on June 14, funds moved through addresses not previously identified and then distributed into two additional identified global exchanges around July 2.


al-QassamBrigades
06/14/2021 02:33:06 GMT-7
06/14/2021 03:05:06 GMT-7
06/15/2021 02:24:34 GMT-7
06/17/2021 15:20:52 GMT-7
32437867
325036f7
06/20/2021 04:53:57 GMT-7
06/29/2021 14:02:05 GMT-7
07/02/2021 17:30:56 GMT-7

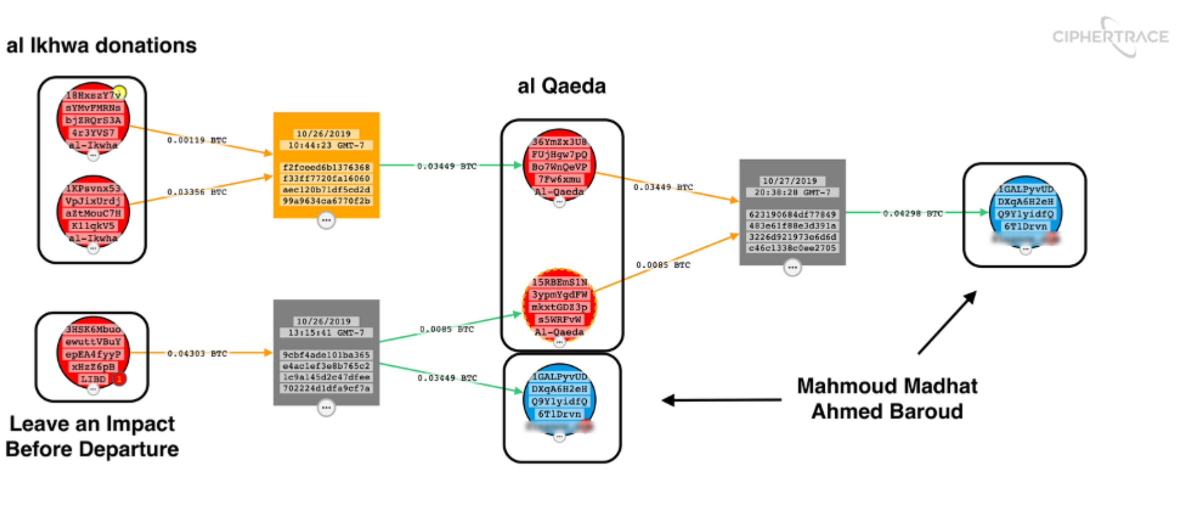
Hamas consolidation cluster and flow of funds to exchanges

This May, CipherTrace reported on donations made to Syrian terrorist organization al-Ikhwa, which were ultimately sent to al Qaeda, following intelligence gleaned from independent journalist group MagniF!le and their investigation into Syrian terrorist groups' telegram channels. According to MagniF!le's research, Hay'at Tahrir al-Sham (HTS) and other terror organizations in the region have accepted more than $250,000 in donations through BitcoinTransfer channel since 2018 in an effort to fund its independent exchange offices in Idlib and other "liberated" provinces in Syria.

CipherTrace analysts identified further movement of funds belonging to al Qassam Brigades that have not been previously analyzed and not yet seized.

CipherTrace further analyzed al-Ikhwa and other extremist group clusters to identify additional connections to the NBCTF seizures.

Donations sent to al-Ikhwa and Leave an Impact Before Departure (LIBD) in 2019 were ultimately sent to al-Qaeda controlled addresses before being deposited into an identified global exchange. The deposit address at this exchange is linked to Mahmoud Madhat Ahmed Baroud, according to the NBCTF seizure notice.


CIPHERTRACE
al Ikhwa donations
18HxszY7v sYMvFMRNs bjZRQrS3A 4r3YVS7 al-Ikwha
1KPsvnx53 VpJixUrdj aZtMouC7H K11qkV5 al-Ikwha
0.00119 BTC
0.03356 BTC
10/26/2019 10:44:23 GMT-7
f2fceed6b1376368 f33ff7720fa16060 aec120b71df5cd2d 99a9634ca6770f2b
0.03449 BTC
al Qaeda
36YmZx3U8 FUjHgw7pQ Bo7WnQeVP 7Fw6xmu Al-Qaeda
15RBEmS1N 3ypmYgdFW mkxtGDZ3p s5WRFvW Al-Qaeda
0.03449 BTC
0.0085 BTC
10/27/2019 20:38:28 GMT-7
623190684df77849 483e61f88e3d391a 3226d921973e6d6d c46c1338c0ee2705
0.04298 BTC
1GALPyvUD DXqA6H2eH Q9Y1yidfQ 6T1Drvn [redacted]
3HSK6Mbuo ewuttVBuY epEA4fyyP xHzZ6pB LIBD
1
0.04303 BTC
10/26/2019 13:15:41 GMT-7
9cbf4ade101ba365 e4ac1ef3e8b765c2 1c9a145d2c47dfee 702224d1dfa9cf7a
0.0085 BTC
0.03449 BTC
1GALPyvUD DXqA6H2eH Q9Y1yidfQ 6T1Drvn [redacted]
Mahmoud Madhat Ahmed Baroud
Leave an Impact Before Departure

2019 al-Ikhwa & LIBD donations sent to al-Qaeda, and then to Mahmoud Baroud's exchange address

CipherTrace Intelligence continues to monitor the donation funds which remained in private wallets or other addresses that had not yet moved.

Travel Rule Compliance Updates

Financial Action Task Force Release Plenary Outcomes

On July 5, 2021, the Financial Action Task Force (FATF) completed its second 12-month review of the implementation of its revised Standards on virtual assets and virtual asset service providers. This review looks at how jurisdictions and the private sector have implemented the revised Standards since the FATF's first 12-month review.

The Travel Rule was the most focused on issue in terms of VASPs' compliance with the revised FATF Standards. Yet only 10 jurisdictions reported that they are actively enforcing Travel Rule requirements for VASPs. An additional 14 jurisdictions reported that they have introduced Travel Rule regulations but were not yet enforced the requirements. No jurisdictions reported being aware of any VASP that fully complied with all elements of the Travel Rule.

There are various technologies and tools available that enable VASPs to comply with the Travel Rule, yet compliance with the Travel Rule continues to be reported as challenging due to "the lack of one unified technology to support it," according to the FATF report.

Since FATF's first 12-Month Review, there has been significant progress in Travel Rule technology development. Several standards and protocols—such as the Travel Rule Information Sharing Architecture (TRISA)—can now help enable interoperability between solutions and, when enhanced by blockchain analysis tools such as in CipherTrace Traveler, can also help identify hosted address and the VASPs to exchange Travel Rule data.

The lack of Travel Rule implementation globally is a major obstacle to effective global AML/CFT mitigation and undermines the effectiveness and impact of the revised FATF

Standards. For this, the FATF has indicated that one of its major next steps will be to accelerate the implementation of the Travel Rule globally.

Canada Extends Travel Rule Deadlines

FINTRAC had previously announced that Travel Rule obligations would come into effect on June 1, 2021. A notice issued on May 18 amended that guidance, pushing the compliance date to April 1, 2022, but FINTRAC reserved the right to assess transactional information collected by reporting entities prior to the new date.

EU Embraces Travel Rule

On June 20, 2021, the European Commission published a regulatory proposal covering the Travel Rule for crypto-asset transfers. The proposal updates the AML/CFT framework within the EU and brings crypto-assets into the regulatory folds. Under the proposal, all transfers of crypto-assets over EUR 1000 would be treated as cross-border wire transfers and subject to Travel Rule regulations.

Originating institutions should ensure that transfers are accompanied by:

- the name of the originator,
- the originator's account number, where such an account exists and is used to process the transaction,
- the originator's address, official personal document number, customer identification number or date and place of birth.
- name of the beneficiary
- the beneficiary's account number, where such an account exists and is used to process the transaction

In the EU, Directive like AMLD5 allow each Member State to transpose the rules into their national laws as they each see fit. Because this proposal is a regulation and not a Directive, it will automatically have binding legal force throughout every Member State and go into force at the same time across each jurisdiction. If approved, the regulation is set to enter into force on the 20th day after publication in the official journal.

The complete proposal can be found at: https://ec.europa.eu/finance/docs/law/210720-proposal-funds-transfers_en.pdf

Current Travel Rule Regulations by Country

As more countries choose how to adopt the FATF guidance into their national AML regime, Travel Rule laws continue to develop across the globe. While many share similarities to the FATF guidance, no two are the same. Below is a brief overview of the few countries that have Travel Rule regulations in place with clear enforcement plans. For a complete guide on Travel Rule regulations by country, please visit www.ciphertrace.com/travel-rule

United States

In the US, the rule has technically already been in place, though until now seldom enforced. In the last year, the FinCEN has decidedly refocused on the regulation by proposing several new rules for crypto payments to explicitly apply the Travel Rule to US exchanges, trading desks, crypto kiosks, and custody providers.

Canada

Canada has been forward-thinking in proposing regulations in line with FATF's Travel Rule guidelines. Starting in June 2021, Canada's financial regulator FinTRAC begun treating crypto business as money service businesses (MSBs). Crypto businesses in Canada are now required to report transaction details for amounts of 1,000 CAD or more.

Japan

Since 2017 Japan has had regulation in place under their Payment Services Act. The Japan Financial Service Agency (JFSA) requires VASPs to register for licenses and works with its self-regulatory organization (JVCEA) to ensure compliance with AML regulations—including the Travel Rule.

Singapore

This small but influential country has been an early adopter of blockchain technology and cryptocurrency. As such, they are avid supporters of FATF's Travel Rule recommendation. The reporting threshold for Singapore's Travel Rule is $1,000 USD which is 1,500 SG.

South Korea

South Korea has been strict in enforcing their Travel Rule regulations and enforcing anti-money laundering rules for cryptocurrency businesses and exchanges. The Korea Financial Services Commission (FSC) issued a regulatory proposal for cryptocurrencies in late 2020. Travel Rule requirement are set to come into effect March 25, 2022.

Switzerland

A long-time hub for financial transactions and private bank accounts, Switzerland has taken steps to go above and beyond the adoption of the FATF's guidance. The Swiss Financial Market Supervisory Authority (FINMA) requires VASPs to identify the beneficial owner of all external wallets or addresses prior to engaging in crypto transaction and has recently lowered its country's monetary threshold for unidentified crypto exchanges to comply with FATF's guidance from $5,000 to $1,000.

FATF Review of Cryptocurrency AML Compliance Globally

Financial Action Task Force Releases Second 12-Month Review

On July 5, 2021, the Financial Action Task Force (FATF) completed its second 12-month review of the implementation of its revised Standards on virtual assets and virtual asset service providers. This review looks at how jurisdictions and the private sector have implemented the revised Standards since the FATF's first 12-month review.

The FATF's first 12-month review report found that, overall, both the public and private sectors had made progress in implementing the revised FATF Standards, however, substantial work remained for the revised FATF Standards to be effectively implemented globally. As such, this second 12-month review focuses on the continued implementation of the FATF Standards.

While the second 12-month review reveals progress has been made in the implementation of the Revised FATF Standards, after two years many jurisdictions still do not have the basic regulatory framework for VASPs. The FATF covers more than 200 countries and jurisdictions, however, less than half (45%) of the 128 reporting jurisdictions reported that they have passed the necessary laws/regulations to permit or prohibit VASPs.

The number of jurisdictions whose AML/CFT regime for VASPs is actually operational is even lower. Most jurisdictions and most VASPs are not complying with the travel rule with only 10 jurisdictions reporting that they have implemented and are enforcing Travel Rule requirements for VASPs.

It is assumed that the majority of jurisdictions that did not provide a response to the FATF in this report have made even less progress in the implementation of the Revised FATF Standards.

How Jurisdictions Have Implemented the Revised FATF Standards

The report finds that many jurisdictions have continued to make progress in implementing the revised FATF Standards. Out of the 128 reporting jurisdictions that responded to the FATF's questionnaire—triple the number that responded to the first 12-month review—52 jurisdictions claimed to now regulate VASPs, 6 jurisdictions prohibit the operation of VASPs, and the other 70 jurisdictions have not yet implemented the revised Standards in their national law. These gaps in implementation mean that there is not yet a global regime to prevent the misuse of virtual assets and VASPs for money laundering or terrorist financing.

For context, in the last 12-month review, 32 jurisdictions reported having existing regulations for Virtual Asset Service Providers, 13 jurisdictions reported having regulations in development, and 5 jurisdictions indicated the prohibition or potential near future prohibition of VASPs. The increase in jurisdictions that now regulate VASPs suggests that significant progress has been made, however global implementation still has very large gaps that need to be addressed.

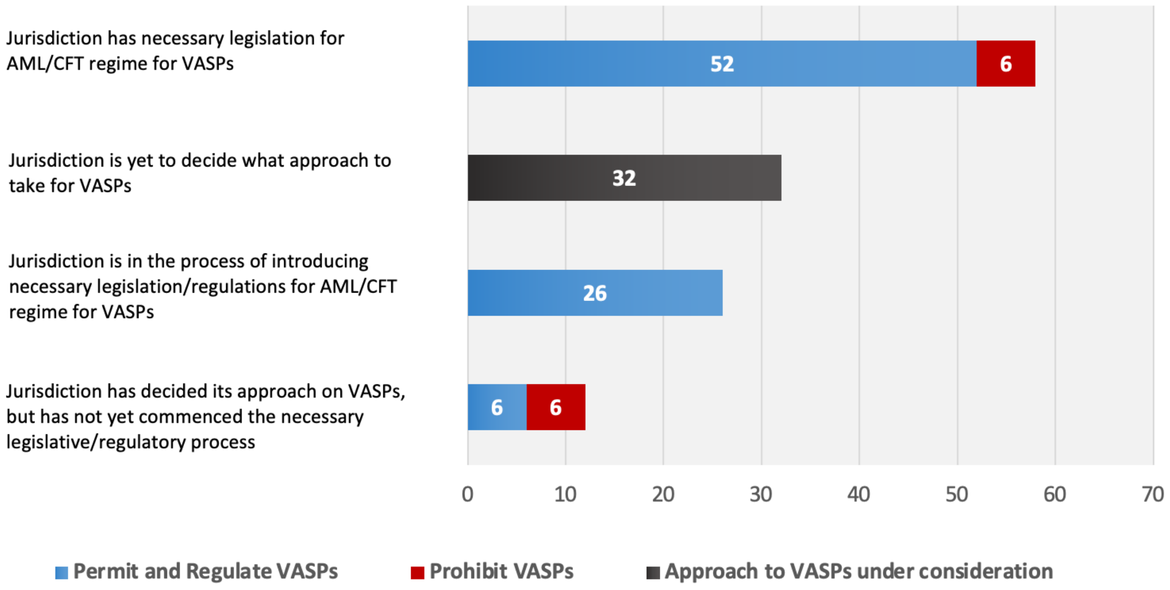
Only 35 of the 58 jurisdictions that claimed to now regulate or prohibit VASPs reported that their regime was currently operational.

For jurisdictions that have yet to prohibit or regulate VASPs, 26 jurisdictions reported that they were in the process of passing the necessary legislation in order to regulate or prohibit VASPs;

12 jurisdictions reported that they had already decided which approach they intended to take on VASPs but had not yet commenced the necessary legislative/regulatory process; and 32 jurisdictions reported that they had not yet decided what approach to take for VASPs.

© Copyright 2021 CipherTrace. All rights reserved

Progress in implementing AML/CFT regulatory regimes for VASPs



CipherTrace Cryptocurrency Intelligence
Source: The Financial Action Task Force (FATF)

Of the 52 jurisdictions that reported that they have established regulatory regimes permitting VASPs, only 36 of these jurisdictions advised that they have commenced licensing and registering of VASPs. Only 32 reported jurisdictions have extended their regime to included VASPs incorporated overseas but which offer products/services to customers in their jurisdiction. In total, these jurisdictions have reported that they have so far licensed or registered 2,374 VASPs—more than double the reported number of registered/licensed VASPs recorded in the first 12-month review.

Non-Compliance with FATF Standards

The FATF calculates implementation of FATF Standards through a self-assessment by participating jurisdictions and is not an official assessment of the level of actual compliance with the FATF Standards. By assessing jurisdictions through the Mutual Evaluation and Follow-Up Report (MER/FUR) process, the FATF found that no jurisdictions with published reports have received a compliant (C) rating. Most jurisdictions have received a partially compliant

© Copyright 2021 CipherTrace. All rights reserved

(PC) rating or above. Two jurisdictions have been assessed as having a non-compliant (NC) rating.

According to the FATF, the main barrier to compliance appears to be a lack of action by jurisdictions. A third of jurisdictions with FURs/MERs assessing Recommendation 15 have taken no or minimal action to implement the requirements. The other two thirds of jurisdictions have taken action, but have not implemented the requirements fully—such as omitting Travel Rule regulations.

Suspicious Transaction Reporting (STR)/Suspicious Activity Reporting (SAR) and VASPs
In the FATF Report, 36 jurisdictions provided Suspicious Transaction Report (STR) data from VASPs. According to these 36 jurisdictions, VASPs had filed 146,704 STRs between 2019 and 2020. Some jurisdictions noted that they had noted an increasing number of STRs in 2020 as more VASPs entered the market, knowledge of AML/CFT grew in the sector, and VASPs developed their reporting systems. Of the 146,704 STRs reported, 55,118 were from 2019 and 91,586 were from 2020.

Market Metrics on Peer-to-Peer Transactions

Data collected by the FATF from several blockchain analysis companies, including CipherTrace, indicates the share of illicit transactions appears higher for peer-to-peer transactions than in transactions with VASPs. There were substantial differences in the data provided by the different blockchain analytic companies resulting in the FATF being unable to assess with certainty the size of the peer-to-peer sector and its associated ML/TF risk. The report therefore does not find clear evidence of a shift towards peer-to-peer transactions.

The inconsistency of results from blockchain analytics companies is indicative of inconsistent definitions, double counting and data quality issues.

FATF Next Steps for Crypto AML/CFT Compliance

All jurisdictions need to implement the revised FATF Standards, including Travel Rule requirements, as quickly as possible. The FATF will undertake the following actions focused on virtual assets and VASPs. According to the Second 12-Month Review, the FATF's next steps will be to:

- accelerate the implementation of the Travel Rule;
- finalizing the revised FATF Guidance on virtual assets and VASPs by November 2021;
- monitor the virtual asset and VASP sector, but not further revise the FATF Standards at this point in time (except to make a technical amendment regarding proliferation financing).

FATF's full report can be accessed here:
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html

© Copyright 2021 CipherTrace. All rights reserved

Changes in Global Regulatory Requirements

FinCEN Issues First National AML/CFT Priorities with Crypto at Top of the List

On June 30, FinCEN issued its first ever list of priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) policy. These Priorities are intended to assist financial institutions in their efforts to meet their AML/CFT obligations. The final revised regulations are set to come out within the next 180 days, as required by the Anti-Money Laundering Act of 2020 (AML Act). Most notable in FinCEN's list were that:

- The new priorities explicitly include the use of cryptocurrency for ML/TF and ransomware payments
- Banks are not required to incorporate the AML/CFT Priorities into their risk-based BSA compliance programs until the effective date of the final revised regulations
- Nevertheless, in preparation for any new requirements when those final rules are published, banks may wish to start considering how they will incorporate the priorities
- While virtual assets are only listed in the second point, cryptocurrency touches each and every one of the eight priorities highlighted by FinCEN.

The full press release can be found here: https://www.fincen.gov/news/news-releases/fincen-issues-first-national-amlcft-priorities-and-accompanying-statements

UK Crypto Companies' Inability to Meet AML Rules Attracts Attention from Regulators Who Call for New Regulatory Measures

London Metro police detectives have asked officials to grant them the ability to freeze digital assets belonging to individuals believed to be participating in criminal activity. In addition to the freeze, detectives also want legislation in place that makes it more difficult for criminals to transfer crypto and digital assets. This news comes just as the UK Financial Conduct Authority (FCA) made a statement claiming that an “unprecedented number” of crypto firms have withdrawn applications to register with the FCA due to a significant number of them failing to meet AML standards.

Only five companies are currently registered and approved to conduct business with UK citizens, with others on the temporary license list. In response to the lag in applications, the FCA pushed back the deadline to apply for the Temporary Registration Regime from July 9, 2021, to March 31, 2022, allowing crypto companies to continue operating while working out how to comply with the country's AML laws.

OCC Set to Take a New Direction Regarding Crypto

Acting Comptroller of the Currency Michael Hsu has signaled the intention to review several of the actions undertaken by his predecessor, including those related to cryptocurrency. “At the OCC, the focus has been on encouraging responsible innovation,” Hsu stated. He has asked staff to review actions such as the creation of the Office of Innovation, the updated framework for chartering national banks, and the addition of crypto custody to the purview of banks.

© Copyright 2021 CipherTrace. All rights reserved

FDIC Seeks Information on Cryptocurrency Banking

Per a May 17 announcement, the FDIC announced they were "gathering information and soliciting comments from interested parties regarding insured depository institutions' (IDIs') current and potential activities related to digital assets. The FDIC is interested in receiving input on current and potential digital asset use cases involving IDIs and their affiliates." Comments were due by July 16.

El Salvador Will Accept Bitcoin as Legal Tender

On June 8, El Salvador voted to accept bitcoin as legal tender. The official currency of the country is the U.S. dollar. President Bukele also suggested that the nation's volcanoes could be used as a source of sustainable energy for bitcoin mining.

State Chartered Banks in Texas Granted Approval to Work with Crypto Companies

After a June 10 notice from the Texas Department of Banking, state chartered banks have been cleared to custody cryptocurrency for their customers. While the notice isn't a law, it states that as long as there are protocols in place and banks comply with legal frameworks, they can offer crypto holdings. Marcus Adams, assistant general counsel at the Texas Department of Banking, also stated that Texas will not be taking any guidance from the federal government.

South Korea Enforces New Rules for Crypto Exchanges and Operators

On June 13, South Korea's Financial Services Committee (FSC) announced new rules that are expected to impact nearly 60 unauthorized crypto exchanges, in addition to a law that states banks must label any crypto clients as "high risk."

The new guidelines include measures that help strengthen the security of platforms through ID requirements and verification. Currently, only four exchanges in the country utilize ID verification and have real name accounts. The FSC is justifying these new rules by saying the demand for safeguards at smaller crypto exchanges is growing at a rapid pace, allowing exchanges to place systems in order before their proposed deadline of September 24.

Due to these rules, banks will have to deny service to all customers failing to comply. Banks have appealed the decision and have asked for a lowered level of liability when dealing with exchanges, something many believe will expand if more regulations are to come. Crypto exchanges have also stood firm against the rules, citing lack of trust from customers and the costly bank fees that will severely impact small exchanges' ability to operate.

Financial Regulators Developing Rules to Protect Korean Banks

According to regulations that went into effect in March, Korean crypto exchanges are required to partner with banks to issue real-name accounts to exchange users. However, the compliance burden on banks has made the traditional financial sector hesitant to partner with exchanges out of fear of sanctions. In order to encourage more exchange partnerships with banks, the Financial Services Commission is discussing issuance of updated guidelines to ease the accountability burden banks are faced with. According to an unidentified South Korean official, the revision could come as soon as next month.

Central Bank Digital Currencies (CBDCs)

China's Digital Yuan Smart Card to Diminishes Privacy with Biometrics and Fingerprint Scanning

In early May, China announced that their Digital Currency Electronic Payment (DCEP) will feature a digital yuan card fitted with IDEX Biometrics and fingerprint scanning. Created by the People's Bank of China, the project is getting ready to launch with officials hoping for a fully functional DCEP system by the 2022 Winter Olympics in Beijing.

While Chinese officials say that biometrics and fingerprint scanning technology are necessary for the DCEP network to thrive, critics have raised the issue of privacy and note that the cards will most likely indicate a lack of anonymity. Regardless of the public's concern, China's aggressive approach and adoption of cryptocurrency and blockchain-based technology must be noted as the world races to figure out the best way to implement the new technology.

Sanctioned Countries

As the Country Becomes a Bitcoin Mining Hotspot, Iran Energy Ministry Announces Fines for Home Miners

On May 16, the Iranian Energy Ministry’s spokesman announced the agency was set to impose “heavy fines” on cryptocurrency miners who use household electricity as a power source, claiming that crypto mining is one of the greatest threats to Iran’s energy supply. In addition to fines, those found illegally mining will also have to repay the Energy Ministry for any damage done to the main power grid. Iran legalized industrial cryptocurrency mining in 2019, thereby giving birth to a booming industry; however, the nation continues to struggle with power supply issues.

After reaching its peak in October, the cryptocurrency mining industry in Iran was slapped with regulations, funneling profits to the government to cover for economic losses due to sanctions. Iran has struggled to find a balance between encouraging an industry that can boost the Iranian economy while safeguarding the country's electricity supply.

Explore CipherTrace’s Iranian 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. https://ciphertrace.com/sanctions-research-more-than-72000-unique-iranian-ip-addresses-linked-to-more-than-4-5-million-unique-bitcoin-addresses/

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